University of Zurich[UZH]

Burkhard Stiller, Alberto Huertas, Bruno Rodrigues, Chao Feng, Christian Killer, Eder John Scheid, Eryk Schiller, Jan von der Assen, Katharina O. E. Müeller, Krzysztof Gogol, Muriel Franco (Edts).

Internet Economics XVI

TECHNICAL REPORT – No. IFI-2022.08

January 2023

University of Zurich
Department of Informatics (IFI)
Binzmühlestrasse 14, CH-8050 Zürich, Switzerland

ifi

B. Stiller et al. (Eds.): Internet Economics XVI: IntEco Seminar
Technical Report No. IFI-2022.08, January 2023
Communication Systems Group (CSG)
Department of Informatics (IFI)
University of Zurich
Binzmühlestrasse 14, CH-8050 Zürich, Switzerland
URL: http://www.csg.uzh.ch/

Introduction

The Department of Informatics (IFI) of the University of Zurich, Switzerland works on research and teaching in the area of computer networks and communication systems. Communication systems include a wide range of topics and drive many research and development activities. Therefore, during the autumn term HS 2022 a new instance of the Internet Economics seminar has been prepared and students as well as supervisors worked on this topic.
Even today, Internet Economics are run rarely as a teaching unit. This observation seems to be a little in contrast to the fact that research on Internet Economics has been established as an important area in the center of technology and economics on networked environments. After some careful investigations it can be found that during the last ten years, the underlying communication technology applied for the Internet and the way electronic business transactions are performed on top of the network have changed. Although,a variety of support functionality has been developed for the Internet case, the core functionality of delivering data, bits, and bytes remained unchanged. Nevertheless, changes and updates occur with respect to the use, the application area, and the technology itself. Therefore, another review of a selected number of topics has been undertaken.

Content

This new edition of the seminar entitled "Internet Economics XVI" discusses a number of selected topics in the area of Internet Economics.
The first talk, Talk 1, provides an overview of the future of digital user-to-user communication techniques, highlighting its economic aspects and market potential. Talk 3 discusses Ransomware from an economic and technical point of view, analyzing whether companies should pay the ransom to the attackers. Talk 5 presents an overview of crypto-related scams and their key properties. Furthermore, it shows the detection techniques of cryptocurrency scams. Talk 6 introduces the Business Process Compromise (BPC) attacks, elaborating on the reasons for their success and the consequences they caused. Besides, it suggests countermeasures which could help to prevent becoming a victim. Talk 8 explores, on the one hand, the technical aspects of pulse-wave Distributed denial of service (DDoS) attacks and, on the other side, the economic aspects related to the actors involved in such an attack. Finally, Talk 9 investigates the relationship between consumer trust and Internet of Things (IoT) products by diving deeper into the privacy concerns IoT product categories display, analyzing consumers' attitudes toward IoT devices and reviewing public policy and economic implications regarding the privacy concerns for IoT products.

Seminar Operation

Based on well-developed experiences of former seminars, held in different academic environments, all interested students worked on an initially offered set of papers and book chapters. Those relate to the topic titles as presented in the Table of Content below. They prepared a written essay as a clearly focused presentation, an evaluation, and a summary of those topics. Each of these essays is included in this technical report as a separate section and allows for an overview on important areas of concern, sometimes business models in operation, and problems encountered.
In addition, every group of students prepared a slide presentation of approximately 45 minutes to present its findings and summaries to the audience of students attending the seminar and other interested students, research assistants, and professors. Following a general question and answer phase, a student-lead discussion debated open issues and critical statements with the audience.
Local IFI support for preparing talks, reports, and their preparation by students had been granted by Alberto Huertas, Bruno Rodrigues, Chao Feng, Christian Killer, Eder John Scheid, Eryk Schiller, Jan von der Assen, Katharina O. E. Müeller, Krzysztof Gogol, Muriel Franco, and Burkhard Stiller. In particular, many thanks are addressed to Chao Feng and Bruno Rodrigues for organizing the seminar and for their strong commitment on getting this technical report ready and quickly published. A larger number of pre-presentation discussions have provided valuable insights in the emerging and moving field of communication systems, both for all groups of students and supervisors. Many thanks to all people contributing to the success of this event, which has happened in a lively group of highly motivated and technically qualified students and people.

Zurich, January 2023

Contents

1 New Means of Communication - Sending Emotions through the Air? 7
Jordi Küffer

3 An Economic Analysis of Ransomware Attacks: Should Companies Pay or Not? 22
Mark Rueetschi

5 Cryptocurrency Scams: Overview and Classification 36
Dominic Vogel

6 On the Security of Processes: An Overview of Business Process Compromise (BPC) Attacks 55
Jasmin Hochuli

8 An Overview into Pulse-Wave DDoS Attacks 68
Aleksandar Ristic

9 How does Public Trust Affect the Economic Value of IoT Products 85
Tram Vo

Chapter 1

New Means of Communication - Sending Emotions through the Air?

Jordi Küffer

Mobile communication has long become irreplaceable for our daily lives. Just a few years ago we were not able to access the internet on our mobile devices. Today we are doing this hundreds of times a day with enormous speeds. 5G networks that are being deployed right now are once again bringing new specifications and opportunities to mobile. But researchers are already wondering what the next generation networks will be like.
To date, each generation has brought new innovations and means of communication with it. In this paper we present a look back at the technology and repercussions of previous generation as well as a look ahead on 6G network visions. We are also evaluating new means of communication that could be stimulated by 6G. For each major user-to-user communication technology, we present our views for its future market potential.

Contents

1.1 Introduction 9
1.2 Methodology 9
1.3 Previous Mobile Communication Generations 10
1.4 6G: The Next Generation 12
1.4.1 Vision of 6G Networks 12
1.5 Visionary Mobile Communication stimulated by 6G 13
1.5.1 Virtual Reality (VR) 13
1.5.2 Holographic-type communication (HTC) 14
1.5.3 Brain Interfaces 15
1.5.4 Emotion Detection 15
1.6 Evaluations and Discussions 17
1.7 Conclusion 18

1.1 Introduction

Mobile communication is gaining popularity every year. In Switzerland alone, the number of landline subscriptions has dropped to less than 40 per 100 inhabitants while mobile subscriptions have been steadily increasing [2]. The different generations of mobile communication each stimulated new technologies in user-to-user communication.
1G, for example, has brought voice calls among mobile phones and landlines. 2G enabled Short Message Service (SMS) communication, 3G brought the internet to the palms of our hands, 4G stimulated the internet of applications and 5G is said to stimulate the internet of things [23]. Although most users have just become accustomed to mobile broadband provided by 4G, like on-the-go video calls or sharing snap videos of day-to-day lives on the internet, 5G is now being deployed, and society has yet to fully benefit from the 5G repercussions. Certainly, new mobile communication generations carry a lot of potential for emerging communication technology businesses and markets.
But what will the potential brought forward by the next generation be? Current research suggests that 6G could enable terabit-per-second links [34]. This could make science-fiction technology feasible as for instance holographs would require a data rate of approximately 4.32 Tb/s. The idea to further digitize the human senses and transfer them across networks [23] expands the concept of digital communication even more. We might even be able to send emotions through the air soon enough...
The goal of this paper is to understand the previous mobile communication generation in terms of technology and innovations to then analyze the current research on 6G and future means of communication stimulated by 6G. Furthermore, it should discuss the economical aspects and market potential of these new communication technologies.

1.2 Methodology

To understand the mobile communication generations, the author gathered relevant literature by searching publication databases such as ACM, IEEE, Elsevier, Springer, and MDPI for literature on previous mobile network generations. The author then summarized the most relevant findings in his paper. To achieve this the keywords ”mobile networks evolution”, ”1G to 5G”, ”communication technologies”, and similar were used.
The same approach was taken to understand the current opinions in the field of 6G research. Finally, the author presented published research on visionary means of communication and their market potential and feasibility with 6G mobile communication as well as his own opinions on these topics.

1.3 Previous Mobile Communication Generations

The evolution of mobile communication has profoundly changed our everyday lives generation after generation. Every new generation introduces new innovations and capabilities to mobile users. In this chapter, we want to take a look at the evolution of these generations and understand technical aspects, applications & innovations as well as challenges and the need for the next generation.

1G

The first mobile generation was introduced in the 1980s and was still an analog system [28]. Its main use case was voice communication and was implemented by using frequencies around 900MHz [29]. It used frequency division multiple access(FDMA) for modulation and provided up to 2.4 kbps [22].
Even though the voice quality was good, the capabilities were still very limited. Fax communication was only available partly and communication across borders, unlike with existing landline networks, was basically impossible as the systems were incompatible and often completely different equipment was needed. [20]

2G

With the introduction of digital modulation schemes such as Time Division Multiple Access (TDMA) [22] the systems progressed noticeably. In the beginning, speeds up to 64kbps were possible and new means of communication like the short messaging service (SMS) or multimedia message service (MMS) were developed [22].
The regulation also moved from state-owned monopoly operators to an open competition for multiple operators chosen by regulators [20]. Despite many new technologies, "Global System for Mobile Communications" (GSM) became the standard and was the first one to support international roaming to enable users to use their mobile phone connections in different countries [22]. This was enabled by the need for standardization. Organizations like the 3rd generation partnership project (3GPP) were formed to continuously work on standardizations for cellular networks in the future [7].
During the second generation, mobile phones became progressively smaller, lighter, and also smarter [20]. Along with the progression of the internet the desire to interconnect was fueled, and for that much higher speeds were needed.

3G

The third generation introduced much higher speeds, in local coverage areas up to 2Mbps. This really enabled users to connect to the internet on the go. For the first time, users were able to check their emails or open a website with their mobile phones [20; 22].
In 3G the main technology was Universal Mobile Telecommunication System (UMTS), which used Code Division Multiple Access (CDMA). It was this technology that promised a never seen 2Mbps connection. But it seemed like the technology was not able to live up to that promise in most cases. Additionally, UMTS faced competition by rising WLAN technology that provided cheap and high bit rates. It was clear that the next generation was in need of different technology to further progress data transmission speeds. [20]

4G

While 3G introduced higher data transmissions over cellular networks and connected our phones to the internet, the fourth generation improved the user experience by a multiple.

Only with speeds of hundreds of Mbps or even 1Gbps [22] it became feasible to really enjoy videos on the go, browse the internet, or use intensive communication technologies like video calls.
[20] describe 4G as a "cleverly modified copy of WLAN, which has proven to be an ideal technology for high-speed wireless communications." They also state that it is based on orthogonal frequency division multiplexing (OFDM) which allows for combating the delay spread challenge.
During the past years, data transmission has seemingly exploded. Especially video streaming has and will further increase the amount of handled data by wireless networks. Additionally, the number of mobile devices has been rapidly growing. [14] 4G could not keep up with these rising demands for mobile network capabilities.

5G

With millimeter-wave (mmWave) communications, 5G is already able to achieve a maximum of 20Gbps peak data transmission [35]. Today 5G is still in its early stages but it is said to support massive machine-to-machine communication and highly stimulate the platform of the Internet of Things (IoT) [20].
With these specifications, 5G cellular networks are enabling industry applications [15] and extend their capabilities beyond individual cellular usage.
Although some industry applications like telesurgery in e-health might already be limited by the capabilities of 5G networks [26].

1.4 6G: The Next Generation

During the past four decades, mobile communications have advanced over four generations, beginning the fifth right now. Each of the generations introduces new technology and new innovations. The exploration of higher frequency spectrum has led to increasing channel capacity and speeds. These advancements also had a tremendous economic impact. The number of mobile subscriptions amounted to 8.335 billion in 2020 [9]. Each subscription is connected to a mobile device, presumably most being smartphones but also laptops, tablets, smartwatches, and IoT devices. Which are in turn all connected to a wide range of digital applications.
Research for the sixth generation has already started and visions and requirements for 6G mobile networks are being formulated.

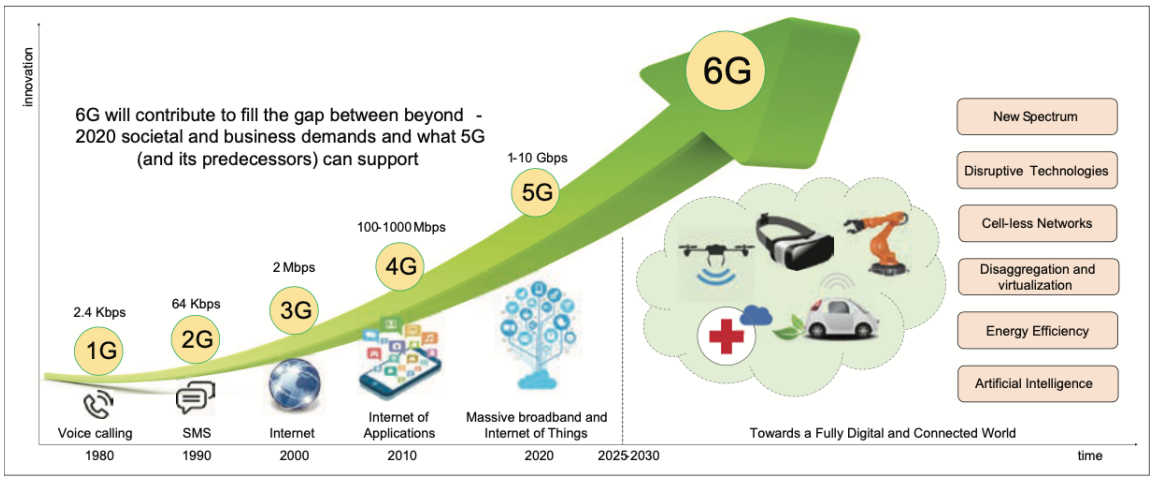

Figure 1.1: Evolution of cellular networks, from 1G to 6G, with a representative application for each generation [23].

1.4.1 Vision of 6G Networks

The visions of 6G networks focus on a highly digitized, fully connected, and data-driven information society. The Annual mobile data usage is expected to more than threefold by 2024 [3]. With these assumptions, researchers (most notably [35; 23] envision:

- underwater and space communication
- massive IoT connectivity
- fully autonomous vehicles supported by 6G Networks
- extremely low power communications
- ultra high definition video streaming

To allow these use cases 6G networks should be able to deliver a much higher data rate ($>$ 1 Tbps) by using TerraHertz Communications. With decreasing wavelength the energy and bandwidth increase [23]. To provide ubiquitous access effective integration of satellites in non-terrestrial networks as well as underwater networks will be needed [30]. A selection of important key performance indicators (KPIs), applications, and characteristics of 6G networks and the comparison to their predecessors are listed in Figure 1.2.

		4G	5G	6G
Applications		• High-Definition Videos • Voice • Mobile TV • Mobile Internet • Mobile Pay	• VR/AR/360° Videos • UHD Videos • IoT • Smart City/Factory/Home • Telemedicine • Wearable Devices	• Tactile/Haptic Internet • Full-Sensory Digital Sensing and Reality • Fully Automated Driving • Industrial Internet • Space Travel • Deep-Sea Sightseeing • Internet of Bio-Nano-Things
Network Characteristics		Flat and All-IP	• Cloudization • Softwarization • Virtualization • Slicing	• Intelligentization • Cloudization • Softwarization • Virtualization • Slicing
Service Objects		People	Connection (People and Things)	Interaction (People and World)
KPI	Peak Data Rate	100 Mb/s	20 Gb/s	≥1 Tb/s
	Experienced Data Rate	10 Mb/s	0.1 Gb/s	1 Gb/s
	Spectrum Efficiency	1×	3× that of 4G	5–10× that of 5G
	Network Energy Efficiency	1×	10–100× that of 4G	10–100× that of 5G
	Area Traffic Capacity	0.1 Mb/s/m^2	10 Mb/s/m^2	1 Gb/s/m^2
	Connectivity Density	10^5 Devices/km^2	10^6 Devices/km^2	10^7 Devices/km^2
	Latency	10 ms	1 ms	10–100 μs
	Mobility	350 km/h	500 km/h	≥1,000 km/h

Figure 1.2: Network features of 4G to 6G simplified from [35]

1.5 Visionary Mobile Communication stimulated by 6G

The current visions of sixth-generation mobile networks indicate another massive technological advancement. With the increasing need for remote communication and interaction, we are expected to see many new innovations in the upcoming years following the deployment of 6G networks.
Will it be groundbreaking technologies like communication involving all five senses or will the current means of communication mainly increase in quality and user experience? In this chapter, we want to analyze which means of communication could be possible with the 6G specifications.

1.5.1 Virtual Reality (VR)

The technology and idea for virtual reality have been around since the 1960s [33]. But it has been very recently that the hardware and software are affordable and of high quality. The worldwide market revenue for consumer and enterprise Virtual Reality currently (2022) is 11.97 billion US dollars and is expected to grow by around 17 billion dollars until 2026 [1].

1.5.1.1 Metaverse

With the rising interest in virtual reality and virtual worlds, the term metaverse has been gaining popularity. It describes a post-reality universe, an interconnected web of social, networked immersive environments in persistent multi-user platforms [16]. The most notable brand associated with the metaverse according to a survey published by Ipsos [12] is Meta (formerly known as Facebook), which is investing massively in a future driven by virtual reality.

(a) Meta Horizon Worlds [6]

(b) The Sandbox [11]

Figure 1.3: Example of metaverse avatars

Facial expressions are very important when it comes to nonverbal communication. They play an important role in conveying emotions. [13] We are already used to reading the feelings and emotions of our communication partner(s) in real life. This is likely why difficulties with collaboration and communication have been one of the main struggles when working remotely [10].
Meta's newest headset (Quest Pro) now also introduces face tracking to mimic facial expressions to your virtual avatar [8]. With technology like this, it might be possible to better communicate emotions in VR meetings or when participating in the metaverse.
However, there are still some limitations to this. The visual quality of avatars is still very low (Figure 1.3). Increasing the resolution would currently overload available network bandwidth and further increase computation overhead and latency [18]. Even though 5G is said to make advancements in mobile VR, it will not be possible to introduce a truly immersive mobile experience with current networks. 6G on the other hand could be able to provide the required specifications. [23]

1.5.1.2 Market Potential

The innovations in the VR space will continue to reshape our digital lives. As previously mentioned the VR market is growing rapidly. 5G networks will push the potential even further and might cause the technology to become more mainstream.
Let's assume 6G will be able to provide a fully immersive VR experience wherever you go. Accompanied by a headset that is lightweight and portable, more like glasses, it could have the potential to replace our smartphones as personal devices. The current global smartphone market revenue is estimated to be almost 500 Billion US dollars [5].

1.5.2 Holographic-type communication (HTC)

After introducing the possibilities to enhance communication through virtual reality, we can introduce extended reality (XR) with an example of holograms.
HTC describes the transmission and interaction with a holographic. Holographs, not to be confused with 3D graphics, add parallax which allows the user to look at the holographic from different angles. [19]
The advantages of HTC are quite similar to those of VR communication. Increasing the presence of the communication partner by allowing non-verbal communication and increased interaction possibilities. [23] suggest that "a raw hologram, without any compression, with colors, full parallax, and 30 fps, would require 4.32 Tb/s." This requirement would already be very demanding for 6G visions but may still be possible.

1.5.2.1 Market Potential

Assuming 6G networks will be able to support HTC, with the current visions it will most likely only be the early adoption of this type of communication. It might not be able to provide a high-quality standard, possibly like the quality we are seeing across VR platforms today.
In this scenario, we will most likely not see HTC replace our daily communication. Instead, it could be focused on very important business meetings or applications in e-Health like remotely diagnosing patients or telesurgery [26]. It would still be a huge technological advancement with many parties willing to invest and push the technology further in the mainstream direction.

1.5.3 Brain Interfaces

Traditional means of communication present certain limitations when it comes to expressing abstract constructs or emotions. This is why neural engineers have already spent years developing new technology to overcome these limitations [31]. Brain-computer interfaces already allow humans to control prosthetic limbs [32]. More recently researchers were able to create the first non-invasive multi-person direct brain-to-brain interface (BBI) called BrainNet [24]. Brain activity is recorded and decoded using electroencephalography (EEG) and then transmitted over the internet to a receiver whose brain is in turn magnetically stimulated. [24] suggest that using a cloud-based BBI server could make BrainNet globally operable and potentially open new frontiers in human communication and collaboration.
With continuous research in this field, the technology might be much more advanced by the deployment of 6G networks. 6G networks could make this technology mobile which could increase availability and interest. Currently, there is limited research linking 6G networks with brain-to-brain interfaces, thus making assumptions purely hypothetical. The combination of using BBIs and VR technology seems particularly interesting. A truly immersive VR experience combined with the possibility to control your avatar with your thoughts on top of communicating with other users through tech-boosted telepathy really paints the picture of how far we could get.
There have also been studies with invasive devices, meaning implants. Yet these methods carry risks associated with surgical procedures, which decreases the potential of future commercial applications [25].

1.5.3.1 Market Potential

Because the widespread application of brain-to-brain communication interfaces still is a futuristic vision, only hypotheses about future market potential are possible. However brain-computer interfaces (BCI) are already more advanced and the global market revenue is expected to grow to 283 million US dollars until 2025 [4]. After the adoption of BCIs, we could expect BBIs to gain more traction. As of now concerns about safety and long-term effects might decrease consumer interest in brain-to-brain interfaces.

1.5.4 Emotion Detection

While instant messaging still is a very popular form of communication, we have long surpassed the sole usage of letters and numbers when texting. Emojis and their emoticon ancestors deal with the lack of opportunity to share non-verbal cues [27]. The usage of such emojis has gained a lot of popularity as almost half of all verbal messages shared on digital platforms include emojis [17]. Still, users have to pick and choose which ones represent their current emotional state often leaving room for interpretation.

[21] presents a variety of technologies that could be used to automatically detect emotions. They conclude that emotion detection is a thriving field of research and expect more advancements to be made in the coming years. Visions include that emotions could be detected automatically by a multi-modal system and shared instantly, opening a bunch of creative doors for communication applications.
6G could provide the necessary foundation to be able to process the input information in real-time and mobile, assuming detection algorithms will be computationally intensive and done remotely.

1.5.4.1 Market Potential

As [21] pointed out, the interest of companies in collecting affective information about their clients has created a new market for established firms or startups to enter. The economical incentive behind collecting and interpreting this data seems to bring large potential. Microsoft for example is developing the Emotion API which can detect emotions from facial expressions in pictures or videos [21]. Although the current focus is not in user-to-user communication, as the technology advances application programming interfaces like the mentioned Emotion API can be used to build user-to-user focused applications.

1.6 Evaluations and Discussions

Understanding the evolution of mobile networks helped us to identify trends in user-to-user communication. Each generation revolutionizes mobile communication in some areas. Most recently 4G networks brought higher speeds to mobile devices, enabling video streaming and user-friendly internet surfing. The communication method brought forward by 4G is video calling. 5G is currently being deployed, and using mmWaves introduces a much lower latency and larger data rate. With 5G networks, we will see the connection between people and things rather than only people.
Researchers are now wondering which technology 6G is stimulating. Visions include a fully digitized society with 6G networks facilitating the interaction of people and the world. We discovered four major means of communication that are gaining momentum and where 6G could provide further stimulation.

Communication Technologies

Virtual Reality is forecasted to gain popularity with large companies like Meta heavily investing in the space. The metaverse provides a virtual world where users can meet and interact digitally. New headsets like the Quest Pro continue to make the experience more immersive and user-friendly for example by introducing face tracking to bring the user's facial expressions to the avatar. Facial expressions have been shown to be important when it comes to communicating emotions. 6G networks could be able to provide the necessary specifications to introduce higher quality and a truly immersive experience to VR users. So that user-to-user communication can be experienced almost like in real life.
Another technology often connected to 6G visions is Holographic-type communication. We compared the effects of HTC in terms of emotional communication to communication in a truly immersive metaverse and concluded that the same advantages of enabling non-verbal communication apply to HTC.
We also discussed current research on brain-to-brain interfaces and discovered BrainNet as the first non-invasive multi-person direct brain-to-brain interface. Due to limited literature connecting 6G and brain interfaces we were only able to hypothesize about the advancements in BBI technology and their potential to utilize mobile internet connections to transmit thoughts.
Finally, we discussed automatic emotion detection and the possibility of using multi-modal systems to capture body signals and translate them into emotions. This technology could stimulate a variety of creative communication applications in the future. 6G networks could provide the necessary data rate and latency to perform emotion detection online and enable this technology on our phones.

Economical Aspects

In terms of economical potential, we realize that HTC as well as BBI technology is still in a very early stage and possibly will not be consumer ready with the first deployments of 6G networks. The market for these types of communication could be very large as soon as the technology is sophisticated enough to provide a safe and user-friendly experience.
VR on the other hand is a very relevant industry that is projected to grow very quickly in the coming years. Companies like Meta are heavily investing to be the key player in this space. With the increasing quality of hardware and software, VR devices have the potential to become our day-to-day devices.
Emotion detection is another growing field of research and companies are starting to generate value by monetizing APIs that afford to detect emotions from different inputs. We see potential in utilizing this technology to integrate it into communication applications.

Future Research

This paper focused on a few communication methods that are currently discussed in relation to 6G networks. However, with researchers closing in on the vision and requirements of 6G networks, there are more technologies available that could be brought in connection with 6G and show how 6G could improve or evolve these systems. It could also be interesting to investigate which means of communication will be eradicated with 6G networks.

1.7 Conclusion

The future of digital user-to-user communication is closing in on the real-life experience. In the past video calling has introduced a visual component to digital communication, making the users feel more involved in the conversation. New technologies expand on this idea and introduce 3D visual components to communication. We have seen that by transmitting more and more non-verbal signals to the communication partner, we are able to understand them beyond their words. Understanding emotional signals thus becomes more and more possible. Technologies that are still early in the development phase have shown means of communication that even go beyond the real-life experience enabling users to share and receive thoughts. With these technologies in mind and the advancements to be made until 6G deployments we conclude that new means of communication really could be able to send emotions through the air and even enabling this experience on mobile devices with 6G networks. We have also shown the market potential behind these technologies to be promising, some markets being worth billions of dollars already.

Bibliography

[1] "Consumer and enterprise VR revenue worldwide 2026 | Statista." [Online]. Available: https://www.statista.com/statistics/1221522/virtual-reality-market-size-worldwide . Date accessed: 30/10/2022

[2] "Digitale Gesellschaft in der Schweiz | Bundesamt für Statistik." [Online]. Available: https://www.bfs.admin.ch/bfs/de/home/statistiken/kultur-medien-informationsgesellschaft-sport/informationsgesellschaft.assetdetail.22686430.html . Date accessed: 12/10/2022

[3] "Global annual mobile data usage 2025 | Statista." [Online]. Available: https://www.statista.com/statistics/1222698/worldwide-annual-mobile-data-usage . Date accessed: 01/11/2022

[4] "Global brain computer interface market size 2018 and 2025 | Statista." [Online]. Available: https://www.statista.com/statistics/1015013/worldwide-brain-computer-interface-market-value . Date accessed: 05/11/2022

[5] "Global: smartphone market revenue 2013-2026 | Statista." [Online]. Available: https://www.statista.com/forecasts/1286699/worldwide-smartphone-market-revenue . Date accessed: 01/11/2022

[6] "Virtual-Reality Welten und Communities | Horizon Worlds ." [Online]. Available: https://www.oculus.com/horizon-worlds . Date accessed: 01/11/2022

[7] "Introducing 3GPP." [Online]. Available: https://www.3gpp.org/about-us/introducing-3gpp . Date accessed: 22/11/2022

[8] "Meta Quest Pro | Meta Store." [Online]. Available: https://www.meta.com/ch/quest/quest-pro . Date accessed: 30/10/2022

[9] "Mobile subscriptions worldwide 1993-2021 | Statista." [Online]. Available: https://www.statista.com/statistics/262950/global-mobile-subscriptions-since-1993 . Date accessed: 24/10/2022

[10] "Struggles with working remotely 2022 | Statista." [Online]. Available: https://www.statista.com/statistics/1111316/biggest-struggles-to-remote-work . Date accessed: 30/10/2022

[11] "The Sandbox Game." [Online]. Available: https://www.sandbox.game/en/me/avatar . Date accessed: 01/11/2022

[12] "U.S. adults brands associated with metaverse 2022 | Statista." [Online]. Available: https://www.statista.com/statistics/1290674/united-states-adults-brands-associated-with-the-metaverse . Date accessed: 30/10/2022

[13] N. Ambady, R. Rosenthal, "Nonverbal communication," *stanford.edu*. [Online]. Available: http://web.stanford.edu/group/ipc/pubs/1998Ambady.pdf

[14] J. G. Andrews, S. Buzzi, W. Choi, S. V. Hanly, A. Lozano, A. C. K. Soong, and J. C. Zhang, "What Will 5G Be?" *IEEE Journal on Selected Areas in Communications*, vol. 32, no. 6, pp. 1065–1082, 2014.

[15] J. Ansari, C. Andersson, P. de Bruin, J. Farkas, L. Grosjean, J. Sachs, J. Torsner, B. Varga, D. Harutyunyan, N. König, and R. H. Schmitt, "Performance of 5G Trials for Industrial Automation," *Electronics 2022, Vol. 11, Page 412*, vol. 11, no. 3, p. 412, 1 2022. [Online]. Available: https://www.mdpi.com/2079-9292/11/3/412

[16] T. Azar, R. Barretta, and S. Mystakidis, "Metaverse," *Encyclopedia 2022, Vol. 2, Pages 486-497*, vol. 2, no. 1, pp. 486–497, 2 2022. [Online]. Available: https://www.mdpi.com/2673-8392/2/1/31

[17] I. Boutet, M. LeBlanc, J. A. Chamberland, and C. A. Collin, "Emojis influence emotional communication, social attributions, and information processing," *Computers in Human Behavior*, vol. 119, p. 106722, 6 2021.

[18] R. Cheng, N. Wu, M. Varvello, S. Chen, B. Han, "Are We Ready for Metaverse? A Measurement Study of Social Virtual Reality Platforms," *felixshing.github.io*, vol. 15, no. 22, p. 2022. [Online]. Available: https://felixshing.github.io/papers/IMC_2022_Metaverse.pdf

[19] A. Clemm, M. T. Vega, H. K. Ravuri, T. Wauters, and F. D. Turck, "Toward Truly Immersive Holographic-Type Communication: Challenges and Solutions," *IEEE Communications Magazine*, vol. 58, no. 1, pp. 93–99, 1 2020.

[20] K. David and H. Berndt, "6G Vision and Requirements: Is There Any Need for Beyond 5G?" *IEEE Vehicular Technology Magazine*, vol. 13, no. 3, 2018. [Online]. Available: https://ieeexplore.ieee.org/document/8412482

[21] J. M. Garcia-Garcia, V. M. R. Penichet, and M. D. Lozano, "Emotion Detection: A Technology review," *Proceedings of the XVIII International Conference on Human Computer Interaction*, 2017. [Online]. Available: https://doi.org/10.1145/3123818.3123852

[22] Gawas Anju Uttam, "An Overview on Evolution of Mobile Wireless Communication Networks: 1G-6G," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 3, no. 5, 5 2015. [Online]. Available: http://www.ijritcc.org

[23] Giordani Marco, Polese Michele, Mezzavilla Marco, Rangan Sundeep, and Zorzi Michele, "Toward 6G Networks: Use Cases and Technologies," *IEEE Communications Magazine*, vol. 58, no. 3, 2020. [Online]. Available: https://ieeexplore.ieee.org/document/9040264

[24] L. Jiang, A. Stocco, D. M. Losey, J. A. Abernethy, C. S. Prat, and R. P. Rao, "BrainNet: A Multi-Person Brain-to-Brain Interface for Direct Collaboration Between Brains," *Scientific Reports 2019 9:1*, vol. 9, no. 1, pp. 1–11, 4 2019. [Online]. Available: https://www.nature.com/articles/s41598-019-41895-7

[25] B. K. Min, M. J. Marzelli, and S. S. Yoo, "Neuroimaging-based approaches in the brain-computer interface," *Trends in Biotechnology*, vol. 28, no. 11, pp. 552–560, 11 2010.

[26] Nayak Sabuzimaand and Patgiri Ripon, "6G Communication Technology: A Vision on Intelligent Healthcare," in *Health Informatics: A Computational Perspective in Healthcare*, Dr. Ripon Patgiri, Dr. Anupam Biswas, and Dr. Pinki Roy, Eds. Singapore: Springer Singapore, 2021, pp. 1–18. [Online]. Available: https://doi.org/10.1007/978-981-15-9735-0_1

[27] P. K. Novak, J. Smailovic, B. Sluban, and I. Mozetic, "Sentiment of Emojis," *PLOS ONE*, vol. 10, no. 12, p. e0144296, 12 2015. [Online]. Available: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0144296

[28] Pankaj Sharma, "Evolution of mobile wireless communication networks-1G to 5G as well as future prospective of next generation communication network," *International Journal of Computer Science and Mobile Computing*, vol. 2, no. 8, pp. 47–53, 2013. [Online]. Available: http://chenweixiang.github.io/docs/Evolution_of_Mobile_Wireless_Communication_Networks.pdf

[29] Pereira Vasco and Sousa Tiago, "Evolution of Mobile Communications: from 1G to 4G," *Academia*, 2004. [Online]. Available: https://www.academia.edu/download/56478913/Mobile_evolution_v1.5.1.pdf

[30] Z. Qadir, K. N. Le, N. Saeed, and H. S. Munawar, "Towards 6G Internet of Things: Recent advances, use cases, and open challenges," *ICT Express*, 6 2022.

[31] R. P. N. Rao and A. Stocco, "When two brains connect," *Scientific American Mind*, vol. 25, no. 6, pp. 36–39, 2014.

[32] M. Vilela and L. R. Hochberg, "Applications of brain-computer interfaces to the control of robotic and prosthetic arms," *Handbook of Clinical Neurology*, vol. 168, pp. 87–99, 1 2020.

[33] I. Wohlgenannt, A. Simons, and S. Stieglitz, "Virtual Reality," *Business and Information Systems Engineering*, vol. 62, no. 5, pp. 455–461, 10 2020. [Online]. Available: https://link.springer.com/article/10.1007/s12599-020-00658-9

[34] P. Yang, Y. Xiao, M. Xiao, and S. Li, "6G Wireless Communications: Vision and Potential Techniques," *IEEE Network*, vol. 33, no. 4, pp. 70–75, 7 2019.

[35] Z. Zhang, Y. Xiao, Z. Ma, M. Xiao, Z. Ding, X. Lei, G. K. Karagiannidis, and P. Fan, "6G Wireless Networks: Vision, Requirements, Architecture, and Key Technologies," *IEEE Vehicular Technology Magazine*, vol. 14, no. 3, 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8766143/

Chapter 3

An Economic Analysis of Ransomware Attacks: Should Companies Pay or Not?

Mark Rueetschi

Ransomware attacks can be described as hackers targeting organization's systems and encrypting all the data available. After that, they demand the payment of a ransom to restore access to the system. Additionally, the attackers frequently are threatening to leak the stolen files online.
This kind of attack became an increasing threat over the last years and caused enormous economic impacts. The cybersecurity market is reacting and growing rapidly as companies invest in different countermeasures. Politics and government agencies are also reacting to the increasing threat. However, the payment of ransom is still a frequent approach followed by targeted companies.
This work focuses on the following question: Should a company pay for a ransom or not? To answer this question, a game-theoretical analysis will be conducted. It will show, why it might be beneficial for criminal hackers to be fair to their victims.
The theoretical results are compared to observations on ransomware attacks. These findings show that hackers are not always acting like theory suggests. Even if paying the ransom might be a feasible option from an economic point of view, observations show, that it is very unlikely for victims to regain full access to their files. Additionally, there are more dimensions to be considered, which are legal aspects, reputational damage and becoming attractive for further ransomware attacks. Therefore it is better not to pay a ransom. Organisations should invest in countermeasures and increase awareness instead.

Contents

3.1 Introduction 24
3.1.1 Evolution of Ransomware 24
3.1.2 Ransomware as a Service 24
3.1.3 Countermeasures 25
3.2 Related work 25
3.3 Approach 26
3.3.1 Base Case 26
3.3.2 Double Extortion Scheme 27
3.3.3 Possibility to Sell Stolen Files 28
3.4 Results 28
3.4.1 Willingness to Pay 28
3.4.2 Hackers' incentives 29
3.4.3 Victim's incentives 29
3.4.4 Data Selling Ransomware 30
3.4.5 Observations on Ransomware Attacks 30
3.5 Discussion 31
3.6 Conclusion 32

3.1 Introduction

Ransomware attacks became one of the most dangerous economic threats over the last years. In this section, the evolution of ransomware, the business models of ransomware gangs, and different counter measures are introduced and discussed.

3.1.1 Evolution of Ransomware

One of the first appearance of ransomware was the, so called, AIDS virus. A floppy disk was sent to researchers around the world labelled with information about the AIDS virus. After a defined number of restarts, the screen of the computer would be locked. To unlock the screen again, a letter with cash should be sent to Panama [1; 2]. This kind of ransomware that locks a computer to prevent access is called locker ransomware [1].
Today, the most common is a more advanced type of ransomware called crypto ransomware. This type of ransomware encrypts the data on a computer to make it unusable. To regain access, a decryption key is needed. The hackers ask for a ransom payment in exchange for this key. A prominent example was WannaCry [3]. It used a flaw in the windows operating system and was able to spread itself. Therefore, it was able to infect many devices around the globe. After the files on a computer were encrypted, it demanded a ransom payment of $ 300 in Bitcoin. This amount would double after three days [3]. Even WannaCry infected many devices and became one the more famous ransomware attacks, it did not generate lots of income for the hackers. WannaCry itself could be cracked very quickly by cybersecurity experts and only a small number of payments were recognized [3]. As all transactions were made in bitcoin, it was possible to track all payments to certain addresses on the blockchain [4].
Bitcoin and other cryptocurrencies enabled large international payments without the need of a physical exchange of cash. This is a key factor in most ransomware attacks in recent years as it lowers the risk of getting caught drastically for criminals [5; 6]. In the last years, especially during the pandemic, ransomware became a large economic threat. Instead of widely spread attacks like WannaCry that aim to infect as many devices as possible, hackers conducted more targeted attacks on large organisations [1]. Ransomware gangs are targeting organisations that handle sensitive data, where they can extort more money. The most affected sectors in 2021 were Government, Education and Healthcare [7].
Due to the increasing threat and the economic damage [8], government agencies agencies and politic are getting involved in order to fight ransomware attacks. After the attack on colonial pipeline, the US president Biden addressed the Russian president Putin directly about this problem. This attack took the largest pipeline in the United States out of operation. Most of the east coast could not be supplied with oil causing disruptions on gas stations and in aviation [9; 10]. Interpol listed ransomware as second highest threat after money laundering in their 2022 global crime trend report [11].

3.1.2 Ransomware as a Service

Ransomware gangs became more professional and better organized. While earlier forms or ransomware attacks were conducted by developers itself, ransomware gangs are undergoing an evolution and specialization [12]. In spring of 2022 the hacker group CONTI got hacked and suffered a data breach. The leaked data contained protocols from communication with affiliates as well as internally. With these protocols, the internal structures of the hacker group were reverse engineered. It showed an organization similar to a modern company with 80 to 100 employees. They had teams for development of own software and for reverse engineering of anti-virus software. Additionally, they had a human resources

and a financial department. Another team was responsible for handling the negotiations with their victims. They were even recruiting staff on regular job-websites and they paid regular salary [13; 14; 15].
Modern affiliate attacks are often conducted by a collaboration of large groups like CONTI and their affiliates. The affiliate groups are handling the network access and disrupt the victims' system. Therefore they use the ransomware provided by CONTI or other groups [15]. Typically, the provider of the ransomware handles the negotiation and the payment as well. In the end, the split the their profit from the ransom payment. Mostly the larger share of the profit goes to the group that conducted the attack and compromised the system [16].

3.1.3 Countermeasures

A ransomware attack has high economic consequences for a company. Mostly they will have to rebuild their systems in a more secure way than before the attack. On top of that, they are often taken out of business [17]. Companies are investing a lot in countermeasures. The cybersecurity market generated a total revenue of $ 176 Mio. in 2021 and it is expected to grow rapidly in the upcoming years [18].
In most ransomware infections, human error is involved [19]. The most common way of a ransomware infection is via phishing e-mails that contain malicious links or files. Most companies that invest in cybersecurity also invest in awareness-training for their staff [19].
Another weakness that is often used are stolen credentials [20]. To reduce the risk of an infection due to stolen or weak credentials, companies should enforce two-factor-authentication for their logins [14]. An additional point of access for is outdated software. Vulnerabilities often get patched by software providers quickly, but hackers are still able to use it on devices that have not been updated [21]
In addition to staff training and awareness, companies invest in technical measures like firewalls and malware scanners. These technologies aim to reduce damage by detecting an infection early [14]. Probably the most important countermeasure is to have regular backups of a company's system. Optimally, these backups should be stored offline, in order to prevent an infection [14]. In case of a ransomware infection, this should ensure that the company is able to recover quickly without having to pay a ransom and reducing the costs of such an attack [16].

3.2 Related work

Chesti et al. [1] analysed the evolution of ransomware and gathered data on affected systems and countries with the most attacks. They also analyzed different entry methods of ransomware and suggested several countermeasures. Other authors looked at the business models of ransomware gangs [2; 4]. While Cartwright et al. [2] looked at the economics around ransomware and their welfare consequences, Oosthoek et al. [4] were tracking Bitcoin payments to analyze the market around ransomware attacks. They were able to associate a large set of Bitcoin addresses to several ransomware gangs. However, the focus of these papers was rather on widely spread ransomware attacks than on targeted attacks on organisations. The focus of this report is on targeted attacks on organisations rather than widely spread attacks.
Two other theoretical papers are conducted for this report. Both are using game theory to analyze the behavior of hackers and victims during a ransomware attack [8; 22]. The theoretical part of this work will be based on their studies.
There are different cybersecurity companies observing the current development of ran-

somware. Cyberseason [23] and Sophos [24; 25] are conducting surveys every year. Their reports contain global statistics and give a good overview on ransomware attacks and caused damage. Sophos considered organisations with 100 to 5000 employees for its survey [24], while Cyberseason asked cybersecurity professionals from companies with 700 or more employees [23]. Trend Micro Research [16] conducted an in depth analysis of ransomware business models combined with case studies and research in the darknet.
In this report, the theoretical behaviour modeled with game-theory will be compared to findings on ransomware attack in recent years.

3.3 Approach

To answer to question if a victim should consider paying a ransom or not, incentives to take certain actions on both, the hackers', and the victim's side, will be analyzed. Therefore, a game theoretical approach of a sequential game will be used, meaning that a player knows about every previous decision and actions are happening sequentially [26]. Costs and benefits of every possible outcome can be compared to find an optimal outcome for each player.
The model is based on several assumptions. Both players are acting rationally. Moral reasoning or legal aspects are neglected. Therefore, legal consequences for the hackers will be neglected as well. This model will also not take multiple attacks on the same victim into consideration.
However, effects of multiple attacks on multiple victims will be discussed. In most cases of ransomware, there is a possibility to communicate with the hacker which give the option for bargaining [8]. This might affect the height of a ransom payment. For simplification, in this analysis, bargaining will not be considered.
A hacker decides to conduct a ransomware attack on one or many computers. This effort causes initial costs of $C_{initial}$ to the hacker. For simplification, $C_{initial}$ will be omitted in the following model. However, it should not be ignored, as it might be an important cost factor to the hackers. A victim sees all files on its computer encrypted and the hackers asking for a ransom payment in order to return access to the files. This will be the starting point to all the following game theoretical scenarios. After the theoretical analysis, a comparison to findings on ransomware attacks in recent years is conducted. The goal is to find out how hackers and victims are acting in ransomware scenarios and whether it aligns with their theoretically optimal strategies.

3.3.1 Base Case

In the first stage of this two-stage game, the victim faces an encrypted computer and a demand for a ransom payment R. The victim gets to decide whether to pay the demanded ransom or not [8]. In the second stage of the game, the hackers receive the information if the victim has paid or not. Based on that information, the hackers decide to return access to the file or to destroy them. As the hackers are criminal, there is no guarantee for the victim that any files are returned. The hackers might destroy them even if the victim paid the ransom [8]. Returning the files will bring small costs of C_{return} to the hackers. These costs come from support that is needed to restore corrupted files. If the files are destroyed, the victim faces very high costs for rebuilding the systems C_{damage}. The cost structure looks as follows:

$$C_{damage} >> R >> C_{return}$$

The payoffs U for every possible outcome will look as follows:

Victim	Hackers	Outcome
Pay	Return access	$U_{Hacker} = R - C_{return}$ $U_{Victim} = -R$
	Destroy files	$U_{Hacker} = R$ $U_{Victim} = -R - C_{damage}$
Don't pay	Return access	$U_{Hacker} = -C_{return}$ $U_{Victim} \approx 0$
	Destroy files	$U_{Hacker} \approx 0$ $U_{Victim} = -C_{damage}$

Figure 3.1: Game-Theoretical Model - Base Case (based on [8; 22; 26])

3.3.2 Double Extortion Scheme

A common practice of hackers is to steal data from the victim's system. This allows the hackers to threaten the victim to leak the stolen files online [16]. It would bring additional costs of C_{leak} to the victim. This practice is called double extortion [4]. Within the game-theoretical model, this would add a third stage to the game. The first two stages are similar to the base case. After the hackers have decided whether to return access to the files or not, they can decide to leak them or to destroy them. Different combinations of both hackers' decisions lead to different payoffs. For that reason, the decision to leak the files or not is considered as independent from the decision of restoring access [8; 22]. The cost structure looks as follows:

$$C_{damage} >> R >> C_{leak} >> C_{return}$$

This leads to the following possible payoffs:

Victim	Hackers	Hackers	Outcome
Pay	Return access	Don't leak	$U_{Hacker} = R - C_{return}$ $U_{Victim} = -R$
		Leak files	$U_{Hacker} = R - C_{return}$ $U_{Victim} = -R - C_{leak}$
	Destroy files	Don't leak	$U_{Hacker} = R$ $U_{Victim} = -R - C_{damage}$
		Leak files	$U_{Hacker} = R$ $U_{Victim} = -R - C_{damage} - C_{leak}$
Don't pay	Return access	Don't leak	$U_{Hacker} = -C_{return}$ $U_{Victim} \approx 0$
		Leak files	$U_{Hacker} = -C_{return}$ $U_{Victim} = -C_{leak}$
	Destroy files	Don't leak	$U_{Hacker} \approx 0$ $U_{Victim} = -C_{damage}$
		Leak files	$U_{Hacker} \approx 0$ $U_{Victim} = -C_{damage} - C_{leak}$

Figure 3.2: Game-Theoretical Model - Double Extortion (based on [8; 22; 26])

3.3.3 Possibility to Sell Stolen Files

Li and Liao [22] suggest that selling the stolen data could be an additional way for hackers to increase profit. The game-theoretical model would remain a three-stage sequential game and the first two stages are the same as in the base case. Instead of deciding to leak the stolen files or not, the hackers get to decide whether to sell the files or not [22]. It is assumed that sold data causes similar damage to a victim than leaked data. This leads to the following possible payoffs:

Victim	Hackers	Hackers	Outcome
Pay	Return access	Don't sell	$U_{Hacker} = R - C_{return}$ $U_{Victim} = -R$
		Sell files	$U_{Hacker} = R + V_{Data} - C_{return}$ $U_{Victim} = -R - C_{leak}$
	Destroy files	Don't sell	$U_{Hacker} = R$ $U_{Victim} = -R - C_{damage}$
		Sell files	$U_{Hacker} = R + V_{Data}$ $U_{Victim} = -R - C_{damage} - C_{leak}$
Don't pay	Return access	Don't sell	$U_{Hacker} = -C_{return}$ $U_{Victim} \approx 0$
		Sell files	$U_{Hacker} = V_{Data} - C_{return}$ $U_{Victim} = -C_{leak}$
	Destroy files	Don't sell	$U_{Hacker} \approx 0$ $U_{Victim} = -C_{damage}$
		Sell files	$U_{Hacker} = V_{Data}$ $U_{Victim} = -C_{damage} - C_{leak}$

Figure 3.3: Game-Theoretical Model - Data Selling (based on [22; 26])

3.4 Results

In this section, the outcomes of the game-theoretical models are compared and the factor of willingness to pay is introduced. The game-theoretical models and the willingness to pay are used to explain incentives for certain actions of hackers. Similarly, the incentives for victims regarding ransomware attacks, are analyzed. Lastly, observations on ransomware attacks from recent years are collected from different reports.

3.4.1 Willingness to Pay

Looking at the payoffs for all possible outcomes in the base case, it is noticeable that the payoff for the hackers is always by C_{return} higher if the files are destroyed. Considering only one game, rational hackers would therefore destroy the files, no matter if the victim paid the ransom or not. This changes if multiple attacks with multiple victims are taken into consideration. If the victims knew that hackers would never return access to their files, they would never pay the ransom and just accept the cost to rebuild. On the other hand, if the victims would be certain about getting access to their files back, they would pay the ransom if it is smaller than C_{damage} [8; 22].
This shows that trust is an important factor on the willingness to pay of a victim. Willingness to pay W states the maximal amount a victim is willing to pay in order to regain access to its files. It is not necessarily equal to the demanded ransom R. In the base case,

a victim would pay the ransom if:

$$R < W = t * C_{damage}$$

R	Ransom
W	Willingness to pay
t	Trust $0 \leq t \leq 1$
C_{damage}	Total costs due to lost files

based on [8; 22; 26]
The possibility to leak stolen files causes additional costs to victims. This influences their willingness to pay an therefore the amount of a possible ransom payment:

$$R < W = t * (C_{damage} + C_{leak})$$

R	Ransom
W	Willingness to pay
t	Trust $0 \leq t \leq 1$
C_{damage}	Total costs due to lost files
C_{leak}	Costs caused due to leaked data

based on [8; 22; 26]

3.4.2 Hackers' incentives

Hackers are conducting a ransomware attack in order to make a profit. Considering only one attack, a hacker would never return access to the victims files, even after a payment. In order to increase profit over multiple attacks, it is beneficial for hackers to have a reputation of always returning access as victims are willing to pay a higher ransom with high trust. Rational hackers would therefore always return access to the files in case of a payment [2; 8].
The other factor on a victim's willingness to pay is the costs caused by the attack C_{damage}. In order to increase a victim's willingness to pay, hackers will cause maximal damage to any victim that does not pay the ransom [8].
To increase the damage to victims and therefore the amount of a possible ransom payment, hackers are using double extortion schemes. The payoffs for hackers are similar than in the base case. But if the hackers decide to leak the stolen files, there will be additional costs for the victim. This increases the amount hackers could demand as ransom. Due to the similar benefits on the hackers' side, the incentives remain the same with double extortion as in the base case. A rational hacker would still return access to the files in case of a payment and leak the files in case of no payment [8; 22].

3.4.3 Victim's incentives

Victims have an interest to prevent a ransomware infection in the first place. More effective countermeasures result in an increase of $C_{initial}$ to the hackers. Organisations are investing in measures like staff training, firewalls, secure networks with VPNs, regular updates and multi-factor authentication to increase costs of an attack for hackers an therefore the own risk of an infection [27].
In case of an infection, organisations have an interest in reducing their willingness to pay. Organisations have no influence on how much they can trust hackers, but it is possible to reduce C_{damage}. One part of C_{damage} are costs for rebuilding. The best way reduce these costs are regular backups of the system. Theoretically backups could bring down costs for rebuilding to zero [22]. Another way would be a cyber-insurance. However, this does

not reduce costs for rebuilding, but it moves them to a third party [28; 29].
Second, companies have an interest in minimizing the affected parts of their system. This would reduce both, costs for rebuilding and costs of a data breach. Therefore, they invest in countermeasures like anti-virus software and detection tools to detect infections early. Additionally, they implement an IT governance to make it hard for hackers to laterally move through the system. Some companies are using a zero trust approach where users and applications only get the minimal access rights that are needed to fulfil their job [28; 29; 30]. Considering the possible payoffs on the hackers' side in the base case and the double extortion scheme, it stands out that the only way to make a profit is the ransom payment. Never paying a ransom would prevent hackers from making money and make it less attractive to conduct further attacks. Therefore, it would cause positive externalities for other companies [8; 23]. For that reason, it is suggested that companies should never pay a ransom [1].

3.4.4 Data Selling Ransomware

The possibility to sell stolen data adds another source of income to the hackers' payoffs. Hackers could earn the value of the stolen data if they manage to sell it. Hackers do not depend only on ransom payments, and the victim's decision to pay, in this case. With the possibility to sell stolen files, the incentives for hackers change as well. Li and Liao [22] show that being fair does not necessarily maximize profit. A hacker might still sell the stolen data, even if a ransom was paid. The hackers' behaviour is depending on the value of the stolen data. On the other hand, this would undermine the reputation of the hackers and therefore reduce the willingness to pay on the victim's side [22].
The fact that hackers might sell the stolen data even in case of a ransom payment, adds another level of uncertainty to the victim's side. The actions of hackers would become less predictable for victims. This affects the trust factor and therefore reduces willingness to pay. The total costs remain similar to the double extortion scenario. The victims incentives remain similar to the previous scenarios, but their willingness to pay would be lower.

3.4.5 Observations on Ransomware Attacks

According to Sophos [24], there has been an increase of ransomware attacks in the last years and especially during the pandemic. They recognised an increase in number of attacks as well as in the amounts paid. Most common in recent years is the double extortion scheme [4].

Table 3.1: Observations on ransomware payments (based on [23; 24; 25])

	2020	2021
Organizations hit by ransomware*	37%	66%
Percentage of attacks that encrypted data	54%	65%
Average recovery costs	$1.85 Mio.	$1.4 Mio.
Recovery from backup	57%	73%
Companies that paid ransom after attack	32%	46%
Average data recovered after a payment	65%	61%
Full recovery after ransom payment	8%	4%
Percentage of payments larger than $1 Mio.	4%	11%
Percentage of payments smaller than $10'000	34%	21%

*at least one device, not necessarily encrypted

The hacker group REvil launched a platform to sell their stolen data in the darknet. However, this platform was not successful, they did not receive any public offer for their stolen data [16].
Even if data selling was not successful, hackers are trying new ways to extort money from their victims and to increase the damage they cause. Some hackers are threatening with DDoS attacks additionally to disrupting the victim's system and leaking the stolen files [31]. Others are asking for a second payment after receiving the first one [23]. Once a company paid a ransom it is very likely that they will be attacked again. Cybereason's report claimed that 80% percent of companies which paid a ransom, were attacked again [23].
Some hackers are checking the stolen data for other victims that could be extorted. A very dramatic case happened to vastaamo, a psychotherapy service provider. Hackers managed to steal medical records from their database and threatened to leak them online. First, the hackers demanded a ransom from the company itself and later blackmailed patients directly. This caused patient to put additional pressure on vastaamo to pay the ransom [32].
After being back in business again after a ransomware attack, organisations would have to invest in rebuilding the system to prevent future attacks [23]. This means that companies are facing costs for rebuilding regardless of the outcome, at least partially. Overall, reports suggest that paying a ransom does not pay off [23].
Besides the actual attacks, ransomware gangs and the entire ecosystem are becoming more professional. Hackers are becoming more specialized. Some hackers are only taking care of entering an organisation's network and others are programming new ransomware [15; 16]. Additionally, there is more collaboration between hackers. There are platforms where hackers sell backdoors to large companies or platforms where ransomware gangs are recruiting affiliates [16].
Companies are adapting to the increasing threat as well. Cyberseason reported an average increase of cybersecurity budget of 20% in 2021. Most of it was used for a cyber insurance, to hire additional staff, for awareness training and for security technology [23].

3.5 Discussion

The theoretical analysis shows that a reputation of always returning files is beneficial for hackers and victims. With increased trust, victims are willing to pay a higher ransom. Therefore, rational hackers would always return access to the encrypted files. But they would also cause as much damage as possible if a victim does not pay. This holds for basic ransomware attacks as well as for double extortion schemes. In reality, only few companies could fully recover after a payment. In 2021 only 61% of infected data could be recovered after a payment which leaves still a significant damage to the company. Even if access could be restored, attacked companies would have to invest in their systems to prevent future attacks.
Selling the stolen data after a ransomware attack could increase profits of hackers. Depending on the value of the data, hackers might not always play fair in order to maximize their profit. This would cause additional uncertainty on the victim's side. REvil launched an attempt to sell their stolen data on a platform in the darknet. Observations suggest that this attempt was unsuccessful. This means, that ransom payments remain the only source of income from ransomware attacks for hackers. Therefore, hackers still have an incentive to play fair and return files after a payment.
Observations suggest that hackers are finding different ways to increase damage to their victims in order to extort a higher ransom payment. Additionally, hackers are threatening customers and suppliers of their initial victims. On one side, they are extorting them

directly, on the other side, this increases the pressure on the initial victim to pay the ransom.
From a victim's perspective, a payment can be considered if the damage is higher than the demanded ransom and if it can trust the hacker. However, a payment causes negative externalities to other companies. For that reason, companies should never pay a ransom. Never paying a ransom could theoretically bring ransomware attacks to an end as ransomware attacks would become unattractive for hackers. Observations show that many companies are paying the ransom and the number increased significantly from 2020 to 2021. Additionally, the average amount of a ransom payment increased drastically as well. However, only a small fraction of companies could fully recover after a ransom payment, most companies were still left with a significant amount of damage. Many companies that paid the ransom were attacked again. This shows that a ransomware attack can not be considered a single event. There are many more consequences that have to be considered when a victim pays the ransom. Mostly, it is not worth paying the ransom due to the additional consequences.
On the companies' side there was an increase in cybersecurity budget and awareness. More companies could recover from backups after an attack and the average damage decreased from 2020 to 2021. This shows that the market is reacting to the increasing threat of ransomware and countermeasures are showing some effect. Not only companies, also governments and their agencies are reacting to the increasing threat. Therefore, further political countermeasures and a broader awareness of the problem can be expected for the upcoming years.

3.6 Conclusion

Ransomware evolved from small hacker groups to a sophisticated business. And hackers are finding more ways to cause damage to companies to extort a ransom payment from them. Due to the increasing threat, government agencies are getting involved to fight ransomware. The market for cybersecurity in growing rapidly and there are already first effects observed. More companies are investing in countermeasures and can recover with less damage from ransomware attacks.
A theoretical analysis suggests that rational hacker will always return access to encrypted files if a ransom is paid. But the hackers will also cause maximal damage to their victims in case of no payment. In reality, it was reported that very rarely full access could be restored even after a payment. Companies are often left with a significant damage after an attack. Additionally, most companies that paid a ransom were attacked again. This means that they were facing costs to rebuild their system and to prevent further attacks anyway. Considering these additional dimensions, paying a ransom is very unlikely to be the best option. In order to make it unattractive for hackers to conduct ransomware attacks, companies should have solid countermeasures in place and raise awareness among their employees.
Governments and cybersecurity companies suggest never to pay a ransom. It would cause negative externalities by financing further attacks and bring additional consequences to the organisation. But if your company was suffering under a ransomware attack, would you not consider paying the ransom? Unfortunately, many businesses are still paying, and ransomware is expected to be an increasing threat.

Bibliography

[1] I. A. Chesti, M. Humayun, N. U. Sama, and N. Z. Jhanjhi, "Evolution, Mitigation, and Prevention of Ransomware", *International Conference on Computer & Information Science (ICCIS)*, vol. 2020, doi: 10.1109

[2] J. Hernandez-Castro, A. Cartwright, and E. Cartwright, "An economic analysis of ransomware and its welfare consequences", *Royal Society open science*, vol. 7, no. 3, 2020, doi: 10.1098

[3] A. B. Turner, S. McCombie, and A. J. Uhlmann, "A target-centric intelligence approach to WannaCry 2.0" *JMLC*, vol. 22, no. 4, pp. 646-665, 2019, doi: 10.1108/JMLC-01-2019-0005.

[4] K. Oosthoek, J. Cable, and G. Smaragdakis, "A Tale of Two Markets: Investigating the Ransomware Payments Economy," *arXiv preprint arXiv:2205.05028*, 2022, doi: 10.48550

[5] M. Paquet-Clouston, B. Haslhofer, and B. Dupont, "Ransomware payments in the Bitcoin ecosystem," *Journal of Cybersecurity*, vol. 5, no. 1, 2019, doi: 10.1093/cybsec/tyz003.

[6] O. Lage Serrano and M. Saiz Santos, "Blockchain and the Decentralisation of the Cybersecurity Industry," DYNAII, vol. 96, no. 3, p. 239, 2021, doi: 10.6036/10188.

[7] The Industries Most Affected by Ransomware, `https://www.statista.com/chart/26148/number-of-publicized-ransomware-attacks-worldwide-by-sector/` (accessed 19.10.2022)

[8] E. Cartwright, J. Hernandez Castro, and A. Cartwright, "To pay or not: game theoretic models of ransomware", *Journal of Cybersecurity*, vol. 5, no. 1, 2019, doi: 10.1093

[9] D. Sanger, C. Krauss, and N. Perlroth, "Cyberattack Forces a Shutdown of a Top U.S. Pipeline," *New York Times*, 08 May., 2021.

[10] Inside the DarkSide Ransomware Attack on Colonial Pipeline, `https://www.cybereason.com/blog/inside-the-darkside-ransomware-attack-on-colonial-pipeline` (accessed 19.10.2022)

[11] INTERPOL, 2022 INTERPOL Global Crime Trend Summary Report, `https://www.interpol.int/News-and-Events/News/2022/Financial-and-cybercrimes-top-global-police-concerns-says-new-INTERPOL-report` (accessed 20.10.2022)

[12] N. Kshetri and J. Voas, "Ransomware as a Business (RaaB)," *IT Professional*, vol. 24, no. 2, pp. 83-87, 2022, doi: 10.1109/MITP.2022.3157208.

[13] The Conti Enterprise: Ransomware-Gruppe veroeffentlichte Daten von 850 Unternehmen, https://www.it-daily.net/it-sicherheit/cybercrime/the-conti-enterprise-ransomware-gruppe-veroeffentlichte-daten-von-850-unternehmen (accessed 29.09.2022)

[14] A. Farion-Melnyk, V. Rozheliuk, T. Slipchenko, S. Banakh, M. Farion, and O. Bilan, "Ransomware Attacks: Risks, Protection and Prevention Measures" *11th International Conference on Ad-vanced Computer Information Technologies (ACIT)*, Deggendorf, Germany, Sept. 2021, pp 473-478, doi: 10.1109

[15] T. Puech and L. Luce, Ransomware: Inside the former CONTI group https://www.riskinsight-wavestone.com/en/2022/07/ransomware-inside-the-former-conti-group/ (accessed 29.09.2022)

[16] M. Fuentes et al., "Modern Ransomware's Double Extortion Tactics and How to Protect Enterprises Against Them", Trend Micro Research, Irving, TX, USA, 2021.

[17] M.-A. Langer, "Unterrichtsfrei dank Hackern: Ransomware-Angreifer nehmen amerikanische Schulen ins Visier", *NZZ*, 06 Oct., 2022

[18] Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031, https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031/ (accessed 19.10.2022)

[19] Coffey, John W., "Ameliorating sources of human error in cybersecurity: technological and human-centered approaches.", *The 8th International Multi-Conference on Complexity, Informatics, and Cybernetics, Pensacola*, 2017

[20] Leading cause of ransomware infection 2020, https://www.statista.com/statistics/700965/leading-cause-of-ransomware-infection/ (accessed 19.10.2022)

[21] A. Dehghantanha, H. Karimipour, and A. Azmoodeh, "Cybersecurity in Smart Farming: Canada Market Research", *Cyber Science Lab*, 2020

[22] Z. Li and Q. Liao, "Game Theory of Data-selling Ransomware," *JCSANDM*, 2021, doi: 10.13052

[23] Ransomware: The True Cost to Business 2022, https://www.cybereason.com/ransomware-the-true-cost-to-business-2022 (accessed 15.10.2022)

[24] The State of Ransomware 2022, https://www.sophos.com/en-us/content/state-of-ransomware (accessed 15.10.2022)

[25] The State of Ransomware 2022, https://news.sophos.com/en-us/2021/04/27/the-state-of-ransomware-2021 (accessed 15.10.2022)

[26] G. Owen, *Game theory*, 4th Edition, Emerald Group Publishing, Bingley, UK, 2013

[27] 166 Cybersecurity Statistics and Trends, https://www.varonis.com/blog/cybersecurity-statistics (accessed 19.10.2022)

[28] The Worsening Cyber Insurance Landscape: Top Survival Tips for Businesses, https://www.spiceworks.com/it-security/cyber-risk-management/articles/worsening-cyber-insurance-landscape/ (accessed 20.10.2022)

[29] The Active Adversary Playbook 2022, `https://news.sophos.com/en-us/2022/06/07/active-adversary-playbook-2022/` (accessed 19.10.2022)

[30] C. Winckless and S. Olyaei, "How to Decipher Zero Trust for Your Business," Gartner, May. 2022.

[31] How Ransomware is Teaming Up with DDoS, `https://www.infosecurity-magazine.com/opinions/ransomware-teaming-ddos/` (accessed 18.10.2022)

[32] H. Tuttle, "Ransomware Attackers Turn to Double Extortion", *Risk Management*, vol. 68, no. 2, pp. 8-9, 2021

Chapter 5

Cryptocurrency Scams: Overview and Classification

Dominic Vogel

With the introduction of the blockchain in the year of 2008, new possibilities of a digital currency started emerging. Solving prior problems, the blockchain serves as a public transaction ledger, which is not only immutable, but also decentralized and publicly verifiable. Specifically, one feature stands out with the blockchain: Pseudoanonymity. Needing a private key to get access to a user's wallet, it is difficult to link, who is behind a 28 to 35 characters long alphanumeric address. This benefits scammers, who prefer to remain unknown. Moving along developments in such a modern world, scammers adopt new strategies to get to their victims. Cryptocurrencies have become widely popular in Internet scams, as a form of payment. Usually with well-known schemes from the stock market, scammers act on the unregulated markets of decentralized exchanges. These scams range from Pump-and-Dump scams, to advance fee scams, all the way over to the classic blackmail. All of these scams existed in the world before cryptocurrencies, yet they have become threats to new, naive investors who are hoping to make fast money while having little knowledge on what they are investing in. Since numbers of reported fraud losses in cryptocurrencies are rapidly increasing, research in detecting these types of scams has become prevalent and essential. Especially with the use of Machine Learning (ML) models, automating the detection of scams in the cryptocurrency world would be a huge step towards less money lost to scammers. However, discussing about different crypto-related scams can lead to a better understanding of their existence and avoid economical loss. That is why this report presents an overview of selected crypto-related scams, their key properties, and how one can detect them.

Contents

5.1 Introduction 38
5.2 Background on Cryptocurrencies 39
5.2.1 Cryptocurrencies 39
5.2.2 Tokens 41
5.2.3 Smart Contracts 41
5.3 Overview of Cryptocurrency Scams 41
5.3.1 Scams using Cryptocurrencies' Core Functionality 42
5.3.2 Scams Simplified Through Cryptocurrencies 44
5.3.3 Economical Impact of Cryptocurrency Scams 45
5.4 Detection of Scams 46
5.4.1 Reports 46
5.4.2 Academic Research 47
5.5 Summary and Conclusions 49

5.1 Introduction

The blockchain was proposed in 2008 by an author, or a group of authors, under the pseudonym *Satoshi Nakamoto*. It is meant to serve as a public transaction ledger for a new form of digital currency called Bitcoin [1]. Up until then, there have been some proposals of electronic cash, yet Bitcoin was the first approach to solve the double-spending problem, where one could spend the same coin twice. The blockchain successfully combines Peer-to-Peer (P2P) mechanisms, an application of cryptography, and timestamping principles. This leads to an immutable, decentralized and publicly verifiable ledger of transactions [2].
This proposal laid the basis of today's world of cryptocurrencies. As depicted in Figure 5.1 the market capitalization of the cryptocurrencies has grown immensely over the past couple of years. As of the first of December 2022, it is at around 854 billion US Dollars. Comparing this with a year ago, the market capitalization was at 2.2 trillion US Dollars as per the 31st of December 2021 [3]. This data can be compared with the market capitalization of the Swiss stock exchange *SIX*. According to Statista, it's market capitalization was at around 2.37 trillion US Dollars in December 2021 [4]. This comparison shows that the cryptocurrency market has gained a lot of importance over the past decade and has become a significant factor when talking about the future of money.

Figure 5.1: Timeline of the cryptocurrency market capitalization [3]

In the English Fairy Tale, "Jack and the Beanstalk", a boy named Jack trades the family cow for a sack of magical beans from a mysterious merchant at a market. At home, he gets scolded by his family for trading one of the only family valuables for something seemingly worthless. Although later on the beans begin to grow into a giant beanstalk, the initial moral of the story is, when trading with a stranger, you do not know what exactly you will get in return. There is an information asymmetry which leads to an uncertainty in one or both parties which can only be overcome by establishing trust in each other. In the fairy tale, Jack's young naivety makes him trust the mystery merchant.
With the ongoing digitalization through the Internet, cybercriminals emerged and started taking advantage of the abundance of personal information and the possibility of online and fast financial transactions. As a consequence, one of the most threatening cyber crimes, identity theft, gained in popularity. Alkhalil et al. defines it as: "*impersonating the person's identity to steal and use their personal information [...] by an attacker for the individual's own gain not just for stealing money but also for committing other crimes*" [6]. Personal data ranges from full names, private E-Mails, passwords or addresses, up to social security numbers. Since not all of this information is available through the internet, cybercriminals try to fill the missing gaps by luring their victims into voluntarily giving it to them. An example of this are the infamous phishing mails. In these scams, victims are lured onto malicious websites, that visually may look like famous websites (*e.g.,* Paypal)

and are then asked to enter their personal information like their login credentials. This is how cybercriminals establish trust over the Internet, by showing the victims familiar websites and deceiving them into thinking there is no malicious intent. By handing over personal information, in these so-called phishing scams, possible consequences can be major losses not only for individuals, but also for companies or even entire governments [6; 37].
This report presents the cohesion between cryptocurrencies and scams. First, it starts with the background on cryptocurrencies in Section 5.2. Following, an overview of the different selected types of scams is detailed in Section 5.3. Next, the detection of scams is discussed in Section 5.4. Finally, Section 5.5 summarizes and concludes the report.

5.2 Background on Cryptocurrencies

Blockchain technology has laid the ground base for almost all cryptocurrencies, especially the largest in market capitalization such as Bitcoin or Ethereum [5; 3]. Figure 5.2 depicts the growth of the amount of different cryptocurrencies listed on CoinMarketCap, a famous price-tracking website for cryptoassets:

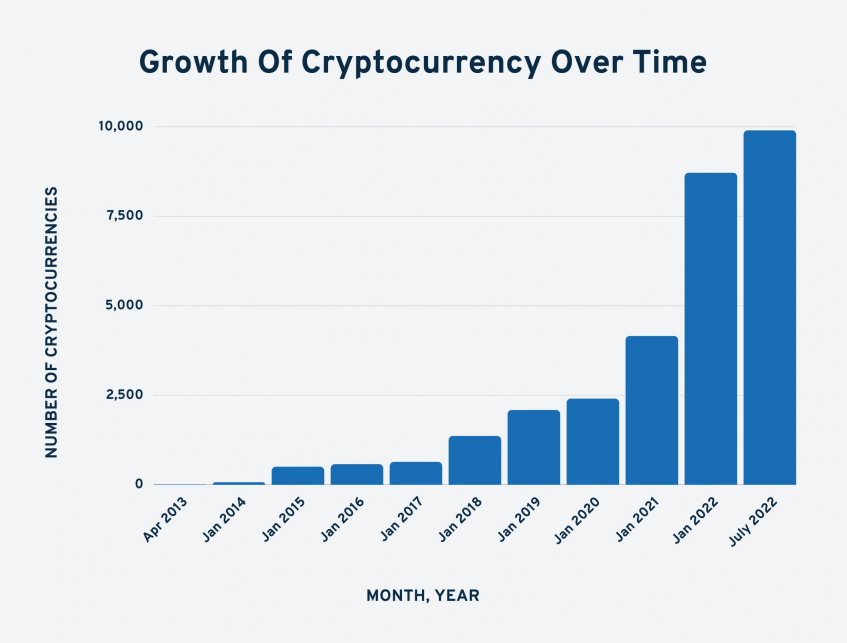

Figure 5.2: Number of cryptocurrencies over the course of 9 years [7]

Figure 5.2 demonstrates the sheer growth that cryptocurrencies had in the past couple of years. With a market capitalization of over a trillion US Dollars, cryptocurrencies have grown immensely over the past couple of years [7]. In the following sections, a deeper analysis into cryptocurrencies and tokens will be presented.

5.2.1 Cryptocurrencies

As of the first of December 2022, there are close to 22'000 different cryptocurrencies in circulation [3]. Since many of these cryptocurrencies are not active or valuable, disregarding these, there are a little less than 12'000 active cryptocurrencies left. As seen in Figure 5.2, the number of cryptocurrencies approximately doubled each year between 2020 and 2022 [7]. During these years, especially the larger cryptocurrencies regarding market capitalization, such as Bitcoin and Ethereum, experienced a boom, whereas for example Bitcoin's value had a 640% increase approximately a year after Covid-19's eruption [8].

Several governments noticed the potential of cryptocurrencies and started implementing them into their societies, to not only be ahead of the curve, but also to potentially profit from benefits such as encouraging foreign investments through improvements of the country's image. Most examples come from third world countries, such as El Salvador, who became the first country in the world to use Bitcoin as a legal tender, a second official national currency [9]. Another example is the Philippines, whose central bank approved nearly sixteen cryptocurrency exchanges [10]. Although, this has received international backlash, a slow integration of the use of cryptocurrencies in the daily life can be seen in other countries. Further selected larger Swiss merchants have started to accept Bitcoin as a payment option. Examples of larger retail groups include Digitec Galaxus and Lehner Versand [11]. Even in the service sector, Bitcoin has started to become a relevant payment method. One luxurious hotel in Zurich, the Dolder Grand, has been accepting Bitcoin as a payment method by guests since the first of May, 2019 [12].
Scheid et al. defines the blockchain, on which most cryptocurrencies are built, as an "*[...] immutable, decentralized, and publicly verifiable ledger of transactions [...]*" [2]. Each block on the blockchain contains a set of transactions. Consensus mechanisms are used to select, who is able to include a new block onto the blockchain. Depending on the type of blockchain there exist different consensus mechanisms.
According to Ferdous et al. the three major types of censensus algorithms consist of: Proof-of-Work (PoW), Proof-of-Stake (PoS) and other types of algorithms beyond the aforementioned ones. In the PoW mechanism, the work is split into two parties: A prover and a verifier [14]. Ferdous et al. defines the collaboration of the two parties as follows: "*The prover performs a resource-intensive computational task intending to achieve a goal and presents the task to a verifier or a set of verifiers for validation that requires significantly less resources. The core idea is that this asymmetry, in terms of resource required, between the proof generation and validation acts intrinsically as a deterrent measure against any system abuse."* This PoW idea was first introduced by Dwork and Naor in 1993, several years before the introduction of the blockchain. It has become the most widely-used consensus mechanism used in blockchains [15]. The PoS algorithm was proposed much later in a Bitcoin related forum called *bitcointalk* in 2012. A year later, a coin called *Peercoin* implemented a blockchain using this algorithm. Its premise is that anyone who would like to participate in the creation process of new blocks, must prove, that they hold a certain number of coins. Hence, have a certain stake already invested in the coin, on which the blockchain relies on. This stake must be locked onto an escrow account. This process limits the amount of participants who can proceed in the creation of new blocks [15].
The process of creating new blocks on a blockchain requires some sort of computational power, stake or hard disk space to verify the transactions and add new blocks to the blockchain. In return, the nodes creating the new blocks on the blockchain are incentivized depending on the consensus mechanism. According to Scheid et al. mining is the process of: "*[...]validating transactions, adding a new block, solving a crypto puzzle, and minting (i.e., creating) new coins [...] in Proof-of-Work (PoW)-based BCs [blockchains]*" [2]. Bamakran et al. mentions, that the mining reward for Bitcoin is halved every 210'000 blocks [16]. As of September 2022, the reward for successfully adding a new block onto the blockchain is 6.25 bitcoins [17]. Converting this into US Dollars with the conversion rate from the 13th of November 2022, this equals a reward of about $100'000 [18]. Regarding the PoS consensus mechanism, blockchains have a set amount of rewards for validating a block of transactions. By being chosen to validate a group of transactions, a node will receive these rewards [19].
Native coins are cryptocurrencies that have their own blockchain as its ledger of transactions. They act as a medium of exchange and have the main role to a sort of digital

currency. They can be mined through PoW or earned through PoS consensus mechanisms. Examples for native coins include Bitcoin, Ether and Cardano [21; 20].

5.2.2 Tokens

Another type of cryptocurrency assets are tokens. Houben and Snyers refer to them as: "[...] digital representations of interests, or rights to (access) certain assets, products or services" [21]. They are issued on an existing coins' blockchain with the intent to raise capital for new entrepreneurial projects, the funding of start-ups or development of new innovative services. In contrast to the the creation of the first type of native coin to emerge back in 2008, the Bitcoin, tokens only became popular by the end of 2017 [21]. To add a relative size between cryptocurrencies and tokens, Chen et al. estimated in 2020, that there are around 160'000 tokens on the Ethereum blockchain [22].

5.2.3 Smart Contracts

Tokens can be created using smart contracts. The term "smart contract" was first used by Nick Szabo in 1994. He defined a smart contract as: *"[...] a computerized transaction protocol that executes the terms of a contract"* [23]. His vision was to bring efficiency to written agreements, which then would be enforced automatically. According to Metcalfe, the Ethereum blockchain declared itself as a decentralized platform that runs smart contracts, which are no other than a special type of software programs [24].
Blockchain-based smart contracts are scripts, which are stored on the blockchain. The blockchain has the ability to execute these scripts [25]. A token contract is a type of smart contract that "defines a token and keeps track of its balances across user accounts" [26], according to Oliva et al. Although there is a lot of creative freedom when designing a token, for example with Ethereum's *Solidity* language, there are two main standards of tokens used in the Ethereum blockchain: ERC-20 and ERC-721 [26]. This standardization helps with the interoperability between tokens and facilitates smart contracts working on tokens. Both ERC-20 and ERC-721 act as object-oriented interfaces containing functions like `totalSupply()`, `balanceOf(address)`, and `transfer(address to, uint256 value)` [26]. In one of these examples we can also see, that with the help of using a smart contract, you can handle transactions from one account to another.

5.3 Overview of Cryptocurrency Scams

Scams involving cryptocurrencies have emerged over the past decade [35]. The reason why cryptocurrencies are used is due to their attribute of pseudoanonimity [2]. Although, every blockchain user can have one or multiple addresses, consisting of 26 to 34 alphanumeric characters, it is difficult to link who is the owner of an address. The blockchain is publicly verifiable, meaning anyone can access the transactions located in each block, and see not only both addresses involved in each transaction, but also the amount of cryptocurrency that was sent from one address to another. This makes tracing scammers that use cryptocurrencies as a payment method a not trivial task.
When looking into different cryptocurrency scams, a clear distinction between two types of cryptocurrency scams can be made. All of the later mentioned scams existed before cryptocurrencies, yet are now usually implemented using them. On one hand, there are scams which use some of cryptocurrencies' core functionality, such as prices, that rely on demand and supply. On the other hand, there are classic scams such as blackmail or malware, where cryptocurrencies are only used as a form of payment method. These two categories are detailed in the next sections.

5.3.1 Scams using Cryptocurrencies' Core Functionality

In the following section, scams will be analyzed that each utilize a part of cryptocurrencies' core functionality. They are all well-known scams in stock-markets that have been adopted for the crypto-assets markets [35].

5.3.1.1 Pump-and-Dump

Pump-and-Dump scams base off the premise that the value of cryptocurrencies is determined by demand and supply. If demand for a crypto-asset rises, so does its price. If it sinks, so will the value of crypto-asset as well [30]. Pump-and-Dump scams usually follow the same procedure. Early on, fraudsters invest in a cryptocurrency at a very low price. Following, the scammers create hype for that cryptocurrency. This is achieved using chat groups such as as Telegram or Discord. This rise in demand leads to a pump-phase. The value of the crypto-asset rises drastically in very little time. At a certain point, the scammers will sell their assets and take away a big profit. Since there is a large drop off in demand, the price of the crypto asset drops as well. The large value decrease leads to panic selling among other investors, who want to lose as little of their investment as possible. This ultimately leaves the value of the crypto-asset at a price range similar to before the pump-and-dump scheme [29]. Figure 5.3 shows the timeline of an exemplary pump-and-dump scheme:

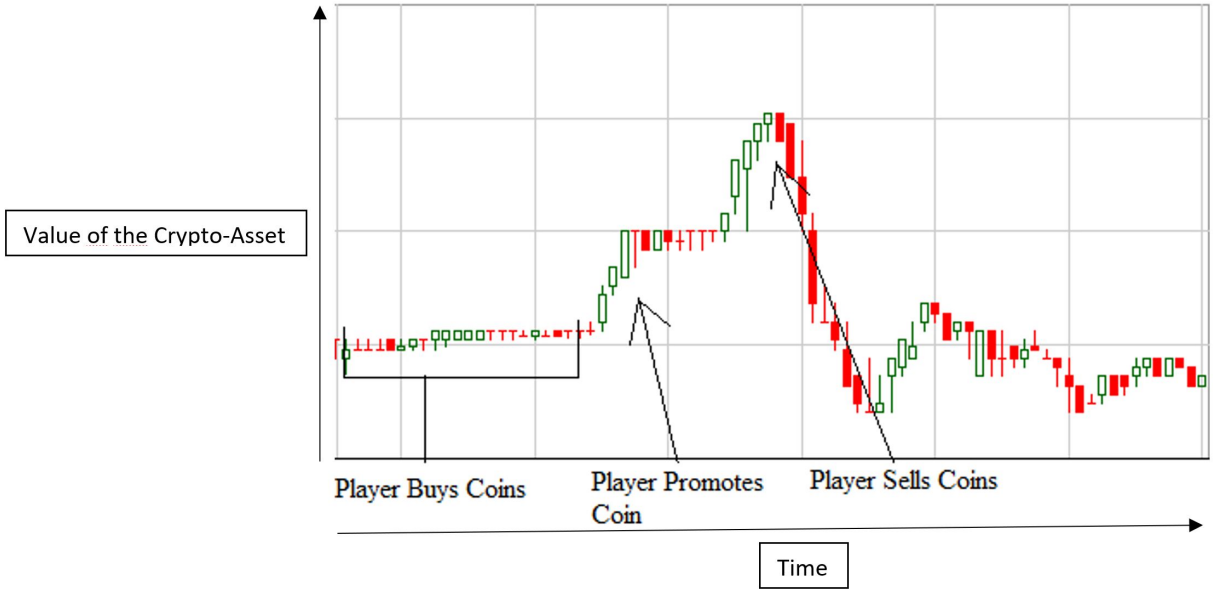

Figure 5.3: Pump-and-Dump chart [31]

At first, one is able to see a stable price trend at a relatively low value. That is where the scammers (in the figure called player) buy their assets. Upon promotion of the crypto-asset, the value is driven upwards. Following, at the high point in value, the scammers sell their assets, causing the value to drop initially. And lastly, panic selling leads to huge losses in value.
On CoinMarketCap.com [3] there is an overview called "Top Crypto Gainers And Losers Today", where one can see the crypto-assets, with the biggest gains and losses within the last 24 hours. There, one can see gains of up to a couple hundred percent and losses where the value decreased almost a full 100% over a timespan of only 24 hours. These are none other than pump-and-dump schemes in their pump (top gainers) and dump (top losers) phases [32].

5.3.1.2 Ponzi-Schemes

Ponzi-Schemes were first made popular by Charles Ponzi in the beginning of the 20th century [33]. The US government describes the scam as follows: "*A Ponzi scheme is an investment fraud that pays existing investors with funds collected from new investors. Ponzi scheme organizers often promise to invest your money and generate high returns with little or no risk. But in many Ponzi schemes, the fraudsters do not invest the money. Instead, they use it to pay those who invested earlier and may keep some for themselves*" [34]. Similar to the pump-and-dump scam, the Ponzi-Scheme follows a pattern of the scammers lying to their victims. They promise high returns with little risk involved.
Ponzi-Schemes have become infamous scams in the world of cryptocurrencies, and are advertised as "*High Yield Investment Programs*" [35]. The high returns are paid with investments from new users, and as soon as no new users keep joining, the scheme stops working and most investors lose their money. The scammer makes a profit by taking small cuts out of each investment and keeping it for themself. Usually, Ponzi-Schemes contain a time-limited aspect. Meaning, potential victims have to act fast before the offer expires and therefore the chance for them to act irrational and fall for the *low risk, high reward* bait is higher.
Ponzi-Schemes have become a well-known scam in the cryptocurrency world. They are implemented with the help of smart contracts, where the capability of handling transactions is used. Bartoletti et al. studied the automatic detection of Ponzi-Schemes, and came to the conclusion, that there is a set of criteria for determining when a smart contract implements a Ponzi-Scheme: "*1) the contract distributes money among investors, 2) the contract receives money only from investors, 3) each investor makes a profit if enough investors invest enough money in the contract afterwards, 4) the later an investor joins the contract, the greater the risk of losing his investment*" [36]. In practice, there have been cases, where single cryptocurrency-based Ponzi-Schemes attracted millions of dollars worth in investments. An example is PlusToken, which got investors to spend over $2 billion [37].

5.3.1.3 Rug Pull

The rug pull works by removing the liquidity of a crypto-asset. The developer of the token is the scammer. Mackenzie defines the rug pull in his paper *"criminology towards the metaverse"* as follows: "*In a fast rug pull, a scammer will make a new token, add liquidity to a dex to allow traders to buy it and then when a suitable amount of buying has happened so that the liquidity pool has become inflated on the dex [decentralized exchange], the scammer will remove it.*" [29]. By taking out the liquidity, investors can not trade the token anymore, leaving them with a non-tradeable worthless token [29]. This scam works because decentralized exchanges are non-regulated P2P cryptocurrency marketplaces which operate using an automated market maker. This means, a liquidity pool exists and having a large amount invested in a crypto-asset leaves you with the ability to sell it all at once into a predictable amount. In contrast, on a regulated centralized stock market this would not be possible, as one could only sell their shares in relatively small amounts. After each sale, the market maker refreshes its quotes. Additionally, only a small amount of liquidity is available. This is different in decentralized exchanges, where the entire capital is continually available [38].
Figure 5.4 shows the time chart of a cryptocurrency rug pull. Similar to the Pump and Dump chart, Figure 5.3, one can see a large decrease in value over little time. The difference is that, here the value decrease is instant and that there are no trades afterward. The entire liquidity of the asset got removed instantaneously, meaning no trades were possible after the rug pull.

Figure 5.4: Rug Pull [39]

5.3.2 Scams Simplified Through Cryptocurrencies

There are many classical scams, that have evolved, along with new developments in technology [35]. With the introduction of cryptocurrencies, many started using them as forms of payment, due to the fact of the untraceability between an account and the user behind it. This pseudoanonymity helps criminals to stay hidden, while stealing the victims' money.

5.3.2.1 Advance Fee

Advance fee scams all follow the basic premise: "*I have something valuable to give you, to release it, send me a payment*" [28]. Mackenzie defines them as giveaway scams: "*Giveaway scams plague naive crypto investors on twitter and other platforms. The scammers set up impersonation accounts, pretending to be one of the big names in crypto and expressing the desire to reward followers*" [29].
A famous example of an advance fee scam happened in May 2021 when Elon Musk appeared on the television show Saturday Night Live (SNL). A group of scammers setup fake SNL Twitter accounts beforehand. On the night of the appearance, they created posts and websites with giveaway links, where they impersonated Elon Musk and promised to return multiples of the amount in cryptocurrencies that his followers sent him [29].
Generally, after the victim sends the payment to the address, the scammer either disappears or adds several additional charges for the victim to pay [35]. Advance fee scams have taken over social media and content sharing devices. They often appear on sites like Twitter or Youtube, where famous celebrities like Bill Gates, Elon Musk or Vitalik Buterin, the co-founder of the famous cryptocurrency *Ether*, are impersonated [37; 35].

5.3.2.2 Malware

Cryptocurrency related malware scams can be classified into two different types: Ransomware and Crypto loggers. The first one encrypts data on a victims' device after infecting it with malware, in order to receive a ransom payment from the victim to recover

their files. The payment is done using Bitcoin or other cryptocurrencies, which makes it difficult to trace who is behind the address of the scammer. In contrast, Crypto loggers are a type of malware, that try to steal information about a victim's cryptocurrency account. In detail, they try to extract the private key necessary to transfer crypto-assets from the victims' account to another. Having obtained this, scammers can send a victims' money onto their own account and thus steal from them [35].

5.3.2.3 Blackmail

In blackmail scammers claim to have hacked a victims' personal device and have installed a key logger or webcam recording software. Using this they obtained some information, that could potentially harm the victim's reputation. They request a ransom payment from the victim and threaten to otherwise release it to the public, if the victim does not pay up. This revelation of personal material could potentially cause serious damage [35]. Sexual extortion, also known as *sextortion*, has emerged over the past couple of years. Paquet-Clouston et al. conducted research on this topic, and has come to the following conclusions: "*[S]exual extortion that requires payments in Bitcoin. The scheme, known as spam sextortion, is simple: it aims to threat that compromising photos or videos will be sent to the recipients' contacts if the amount asked in Bitcoin is not paid*" [40]. Believing that a criminal may potentially be in the hands of sensitive information will leave the victim in a panic stage. This, paired with a time urgency can lead to the victim handling irrationally and paying off the criminal, without even being sure, that the scammers has the material, which he claims.
Depending on current events going on in the world, scammers have to adapt their strategies and implement new ways to get to their victims. Covid-19 acts as a real life example for this. There have been Covid-19 related blackmail scams going around as the example in Figure 5.5. Here, an individual claims to be the victim's neighbour and lets him know that he has contracted Covid-19. If the victim does not pay a ransom, the scammer threatens to infect the victim [27].

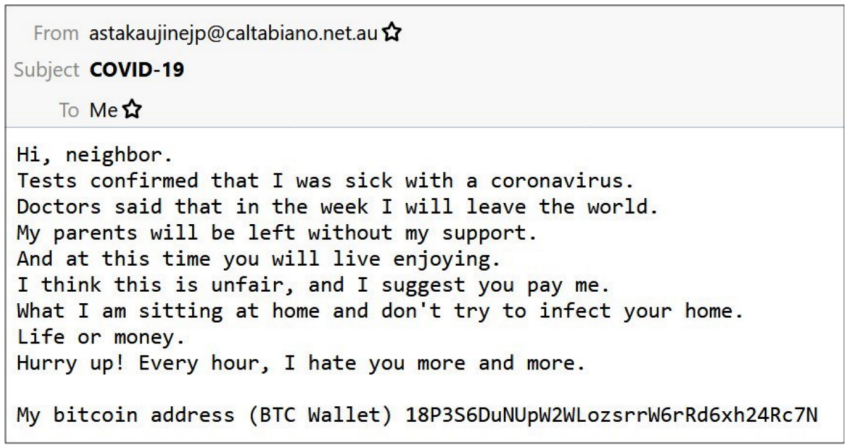

Figure 5.5: A Covid-19 related blackmail E-Mail [27]

5.3.3 Economical Impact of Cryptocurrency Scams

It is difficult to put the damage of each single type of scam into numbers. In total, it has been reported that just in the year 2021 alone, victims lost around $680 million worth in cryptocurrencies to scammers. The worrying part is, that this number has multiplied each year and it does not seem like it is slowing down. Just in the first quarter of 2022, there have already been reported $330 million lost, half of 2021's amount in a quarter of the time [41].

The median reported loss per individual is at $2600 [41]. Conclusively, there is a common denominator regarding the cryptocurrency fraud losses reports. A large portion of the reports were on so called investment scams. The victims were lured in with false promises of easy money. Pairing this with new investors joining the world of cryptocurrency trading with limited knowledge, makes a potentially very dangerous combination for the investors' side.

5.4 Detection of Scams

There are several ways to detect scams; one straightforward manner is when a potential victim is aware of it and can stop him/herself from falling for it. All humans are exposed to their own emotions and this is what scammers try to exploit. DeLiema et al. summarizes it as: "*Susceptibility to persuasion is greater when targets are in a state of high emotional arousal*" [42]. Scammers know this and that is why several scams play off of human emotions. Examples for the emotions are greed in *too good to be true* scams, or happiness, in lottery scams, where the victim is told that he allegedly won the lottery. Emotions cloud our judgement and this might lead to irrational thinking. That is why, being aware of the methods scammers use to get to their victims is a way of scam prevention. The human way of detecting scams. However, whenever there is a human involved, there is always going to be human error. And no matter how well a human is trained on a topic, the probability of a mistake happening still exists.
This is why automated scam detection methods exist. Famous ones are spam folders in mail servers, where malicious spam mails get diverted into automatically [43]. Regarding cryptocurrency scams there is research involved in different types of detection methods.

5.4.1 Reports

Reports can be divided into two different types: URL-reported scams and Address-reported scams. The first one contains reports for scam websites. An earlier mentioned scam, the Ponzi-Scheme, is usually advertised and run on a Website. There are different webpages dedicated to constructing datasets of URL-Reported Scams. An example is BadBitcoin. Here, users can register potentially misleading webpages as scamming websites. Other users, that are unsure, wether a website is legit or not, have the option to look for said website on BadBitcoin, to verify its legitimacy. Another example for URL-reported scam detection is EtherAddressLookup [44], which is a browser add-on, alerting users when they try to access a known scam domain on the Ethereum realm [35].
Address-reported scams work in reporting addresses of cryptocurrency addresses belonging to scammers. A prominent example is BitcoinAbuse [45], which is a public database of addresses belonging to scammers. These can be downloaded using BitCoinAbuse's API. The following figure, Figure 5.6, shows the amount of scams there are per address as of 2021. With a total of around 47'000 addresses in a dataset of 160'000 reports, we can see, that many reports correspond to the same address [35]. This relation makes sense, as the scammer will send his scam to multiple potential victims, instead of just one and therefore get reported several times.

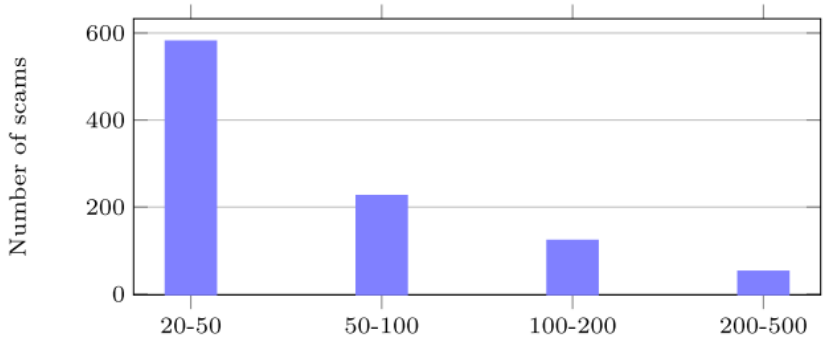

Figure 5.6: Distribution of number of scams per Address on BitcoinAbuse [35]

5.4.2 Academic Research

There are a lot of recent studies regarding the automatic detection of cryptocurrency scams using Machine Learning (ML) methods [46; 35]. Since Ponzi-Schemes are, mostly implemented using the programming language *Solidity* there exist code fragments, which are shared among different Ponzi-Scheme smart contracts. In practicality this means, that the bytecode of a known Ponzi-Scheme has a small Levenshtein distance to the Bytecode of an unknown one [35]. Therefore, there is very little difference in the essential functions of two smart contracts, where one of which is known and the other one is unknown. Using a regression tree model, Chen et al. has achieved a precision of 97% and a recall of 81% on a dataset containing 1382 smart contracts, 131 of those being Ponzi-Schemes [47].
In the following two paragraphs the papers *Don't Fish in Troubled Waters! Characterizing Coronavirus-themed Cryptocurrency Scams* by Xia et al. [27] and *Who are the Phishers? Phishing Scam Detection on Ethereum via Network Embedding* by Wu et al [46]. will be presented with a focus on the scam detection methods.
Don't fish in troubled waters! by Wu et al. focuses on cryptocurrency scams that include some sort of COVID-19 theme. They collected data from various scam reporting websites, e.g., BitcoinAbuse or CryptoScamDB. Additionally, they detected unrevealed scams by using the website Etherscan, which tracks tokens on the Ethereum Blockchain, and searched through ERC-20 and ERC-721 tokens using COVID-19 related keywords. They conducted background checks on these tokens, to verify that they are scams indeed. Continuing, they used various methods to conclude on an extensive dataset of COVID-19 related cryptocurrency scams. In total, they had a list of 195 different scam cases, with 201 individual addresses. They used different tools to analyse the data at hand.

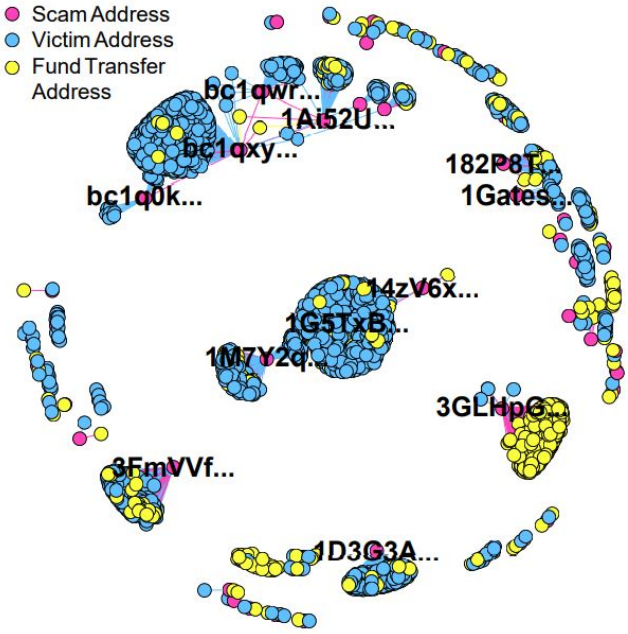

Figure 5.7: The relationship between scam addresses [27]

To check, whether different scam addresses belonged to the same scam campaign, they drew a relationship graph, connecting nodes of addresses, which have interacted with each other. This is depicted in Figure 5.7, where there is a differentiation between Scam, Victim and Fund Transfer Addresses. The Fund Transfer Addresses serve as money laundering channels, where the victim would send his money to, and from there the scammer forwards it to his own address. There are close to 2'400 different nodes in Figure 5.7. 56 of these are scam addresses, 1'741 of the addresses belong to victims and the remaining 600 are fund transfer addresses. Each scam address is connected to 6.5 victim addresses. Interestingly, one can see that some scam addresses are clustered into the same group. On the top left of Figure 5.7 there are four different addresses in the same cluster. They are all part of a *Twitter Hack Address Group (Giveaway Scam)*, in this report referred to as advance fee scams, and have connected 533 victim addresses and 38 transfer addresses. Conclusively, most of the money was transferred to one address, namely address *1Ai52U...*. Their study shows, that this address received 14.75 Bitcoin, which equaled close to $135'000 dollars at the point in time the study was conducted (2020) [27].
While [27] chooses a graphical analysis to investigate into the scam addresses, in *Who Are the Phishers?*, Wu et al. applies network embedding algorithms and ML to train models, which can automatically detect phishing scams. They began by extracting a transaction record dataset from the Ethereum blockchain. Using this and data they pulled from authoritative websites like EtherScam DB and Etherscan, databases of known scam addresses, they created a transaction network, depicted in Figure 5.8. In the transaction network, "*[...] each node represents an address and each edge indicates the ether transaction between a pair of addresses*" [46]. Red nodes are known phishing addresses, blue nodes are known exchanges, yellow nodes are smart contract addresses and other points are unknown addresses [46]

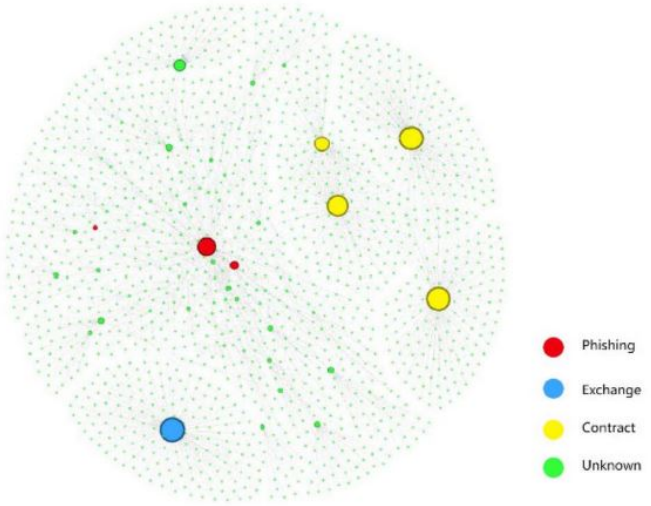

Figure 5.8: transaction network [46]

There exists a large data imbalance, since there are around 500 million addresses and 3.8 billion transaction records on the ethereum blockchain, yet only 1259 addresses are labeled as phishing addresses. This imbalance makes a supervised binary classification rather difficult. Out of this reason, Wu et al. decided to adopt an unsupervised anomaly detection approach, *one-class support vector machine (SVM)*. To improve performance, they applied a *Network Embedding algorithm*, which is a learning paradigm that embeds nodes, links or entire graphs. This makes it more efficient and automatic to extract features from large-scale networked data. Wu et al. designed a novel network embedding algorithm called *trans2vec* with biases towards the transaction amount and timestamp. Finally, they adopted a one-class SVM to classify the addresses into phishing and other addresses. The *trans2vec* algorithm had the following performance on the dataset: Precision: 0.927, Recall: 0.893, F-score: 0.908. Out of different network embedding algorithms which were applied, *trans2vec* had the best performance regarding all of the aforementioned metrics [46].

5.5 Summary and Conclusions

From the infamous Ponzi-Scheme by Charles Ponzi in the beginning of the 20th century, scams have moved alongside developments in technology [33]. This report described selected scams related with cryptocurrencies to date. It mentioned the pseudonanonimity feature of cryptocurrencies and tries to explain its consequences. Different types of cryptocurrency scams are mentioned, ranging from scams building off of cryptocurrencies' core functionalities to scams whose effectiveness is supported through cryptocurrencies. Lastly, it discussed the detection of these scams, also mentioning examples of newest advances using ML methods.
Conclusively, many of these scams share similar traits: They have an appearance of legitimacy to the naked eye, they have an element of time sensitivity and they employ techniques used in the gambling industry. Although appearing legitimate, the victim will usually blame himself in hindsight for falling for such a scam, since they just seem *too good to be true*, when looked at objectively. The aspect of time is implemented in different ways. Either the offers may be time limited, for example with advanced fee scams, where a potential victim only has very little time to take up on the offer, or the user may feel like getting ahead of the crowd is the key to success. The latter also has parallels with the phenomenon *fear of missing out* (FOMO). FOMO works as follows: "*The underlying mechanism of FOMO is the basic human drive for need satisfaction. When individuals*

experience situational or chronic deficits in need satisfaction, they attempt to self-regulate by seeking information about important things that are happening in their communities to avoid missing out" [48]. This description of FOMO by Sultan can be applied to the world of cryptocurrencies. For example, with investors, who see a new token of which everyone is talking about and they can envision the value rising to three times its current value. To avoid missing out on this big profit and not being part of everyone's success, they invest without having much knowledge about what they are investing in [29; 48]. Hence, being a possible victim for the different scams described in this report.
Investors in cryptocurrencies tend to be educated, young, and digital natives [50]. This is partially due to the fact, that the older population is more risk-averse than younger individuals. The reason for this, is that they have a lower expected utility from the future income [51]. Potential adopters of cryptocurrencies are younger and have a higher willingness to accept financial risks. Although, these investors can be considered as digital natives, not all are as well-informed [50]. As a consequence, scammers try to exploit these types of unknowing, naive investors by luring them into their traps and aim to make a profit off of them using the aforementioned techniques. Therefore, it is important to research on the investment and be aware of the different scams being applied in such a domain.

Bibliography

[1] S. Nakamoto: *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008, https://bitcoin.org/bitcoin.pdf.

[2] E. Scheid, B. Rodrigues, C. Killer, M. Franco, S. Rafati, B. Stiller: *Blockchains and Distributed Ledgers Uncovered: Clarifications, Achievements, and Open Issues*, Communication Systems Group, Department of Informatics, University of Zurich, August 2021.

[3] CoinMarketCap, "Global Cryptocurrency Charts", `https://coinmarketcap.com/charts/`, December, 2022.

[4] Statista; `https://de.statista.com/statistik/daten/studie/971159/umfrage/marktkapitalisierung-der-an-der-six-swiss-exchange-gelisteten-unternehmen/#:~:text=Im%20Juni%202022%20belief%20sich,,53%20Milliarden%20US-Dollar`, December, 2022.

[5] Wikipedia; `https://en.wikipedia.org/wiki/Blockchain`, December, 2022.

[6] Z. Alkhalil, L. Nawaf, I. Khan: *Phishing Attacks: A Recent Comprehensive Study and A New Anatomy*, Cardiff School of Technologies, Cardiff Metropolitan University, March, 2021, `https://doi.org/10.3389/fcomp.2021.563060`.

[7] Exploding Topics; `https://explodingtopics.com/blog/number-of-cryptocurrencies`, December, 2022.

[8] The CLS Blue Sky Blog; `https://clsbluesky.law.columbia.edu/2021/03/26/how-the-covid-19-pandemic-affected-the-cryptocurrency-market/`, October, 2022.

[9] Wikipedia; `https://en.wikipedia.org/wiki/Bitcoin_in_El_Salvador`, October, 2022.

[10] The Economic Times; `https://economictimes.indiatimes.com/markets/cryptocurrency/cryptocurrency-has-risen-despite-the-pandemic-is-expected-to-continue/articleshow/82800680.cms`, December, 2022.

[11] Moneyland; `https://www.moneyland.ch/en/bitcoin-switzerland-buy-and-use`, December, 2022.

[12] Wikipedia; `https://en.wikipedia.org/wiki/Dolder_Grand`, December, 2022.

[13] L. Malherbe, M. Montalban, N. Bédu, C. Granier: *Cryptocurrencies and Blockchain: Opportunities and Limits of a New Monetary Regime*, International Journal of Political Economy, Volume 48, 2019, Issue 2, pp. 127-152.

[14] Sadek Ferdous, Mohammad Jabed Morshed Chowdhury, Mohammad A.Hoque: *A survey of consensus algorithms in public blockchain systems for crypto-currencies*, Journal of Network and Computer Applications, Volume 182, 2021.

[15] Dwork Cynthia, Naor Moni: *Pricing via processing or combatting junkmail*, Annual International Cryptology Conference, 1992, pp. 139-147.

[16] Bamakran Seyed, Motavali Amirhossein, Bondarti Alireza: *A survey of blockchain consensur algorithms performance evaluation criteria*, Expert Systems with Applications, Volume 154, 2020.

[17] Bankrate; `https://www.bankrate.com/investing/what-is-bitcoin-mining/understanding`, December, 2022.

[18] Coindesk; `https://www.coindesk.com/price/bitcoin/`, December, 2022.

[19] The Motley Fool; `https://www.fool.com/investing/stock-market/market-sectors/financials/cryptocurrency-stocks/what-is-staking/:~:text=Proof%20of%20stake%20is%20one,validating%20a%20block%20of%20transactions`, December, 2022.

[20] Crypto; `https://crypto.com/university/crypto-tokens-vs-coins-difference`, December, 2022.

[21] R. Houben, A. Snyers, *Crypto-assets Key developments,regulatory concerns and responses*, Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies, 2020.

[22] W. Chen, T. Zhang, Z. Chen, Z. Zheng, and Y. Lu, *Traveling the token world: A graph analysis of ethereum erc20 token ecosystem*, in Proceedings of The Web Conference 2020 (WWW '20), 2020, pp. 1411-1421.

[23] N. Szabo, *Smart Contracts*, 1994. `https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html`

[24] W. Metcalfe, *Ethereum, Smart Contracts, DApps*, Blockchain and Crypto Currency. Economics, Law, and Institutions in Asia Pacific. Springer, Singapore, 2020, pp. 77.

[25] B. Mohanta, S. Panda, D. Jena, *An Overview of Smart Contract and Use cases in Blockchain Technology*, 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2018, pp. 1-4.

[26] G. Oliva, A. Hassan, Z. Ming Jiang, *An exploratory study of smart contracts in the Ethereum blockchain platform*, Empir Software Eng 25, 2020, pp. 1864-1904.

[27] P. Xia, H. Wang, X. Luo, L. Wu, Y. Zhou, G. Bai, G. Xu, G. Huang, X. Liu: *Don't Fish in Troubled Waters! Characterizing Coronavirus-themed Cryptocurrency Scams*, APWG Symposium on Electronic Crime Research (eCrime), 2020, pp. 1-14.

[28] Peter Grabosky, Russel Smith, Gillian Dempsey, *Electronic Theft*, September 2001.

[29] S. Mackenzie, *Criminology towards the metaverse: Cryptocurrency scams, grey economy and the technosocial*, The British Journal of Criminology, 2022, pp. 1-16.

[30] Daytradetheworld; `https://www.daytradetheworld.com/trading-blog/supply-and-demand-of-cryptocurrencies/`, December, 2022.

[31] Quote; `https://www.quora.com/What-are-some-examples-of-pump-and-dump-cryptocurrencies`, December, 2022.

[32] CoinMarketCap; `https://coinmarketcap.com/gainers-losers/`, December, 2022.

[33] Wikipedia; https://de.wikipedia.org/wiki/Charles_Ponzi, December, 2022.

[34] Investor; https://www.investor.gov/protect-your-investments/fraud/types-fraud/Ponzi-Scheme#:~:text=A%20Ponzi%20scheme%20is%20an,do%20not%20invest%20the%20money, December, 2022.

[35] M. Bartoletti, S. Lande, A. Loddo, L. Pompianu and S. Serusi, "Cryptocurrency Scams: Analysis and Perspectives", vol. 9, 2021, pp. 148353-148373.

[36] M. Bartoletti, S. Carta, T. Cimoli, and . Saia, *Dissecting Ponzi schemes on Ethereum: Identification, analysis, and impact*, Future Gener. Comput. Syst., vol. 102, 2020, pp. 259-277.

[37] R. Phillips and H. Wilder, *Tracing Cryptocurrency Scams: Clustering Replicated Advance-Fee and Phishing Websites*, 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2020, pp. 1-8.

[38] Bloomberg; https://www.bloomberg.com/opinion/articles/2021-07-01/pump-and-dump-and-pull-the-rug, December, 2022.

[39] CryptoStarts; https://blog.cryptostars.is/crypto-scams-whats-a-rug-pull-f55e22f12cc2, December, 2022.

[40] M. Paquet-Clouston, M. Romiti, B. Haslhofer, and T. Charvat, *Spams meet Cryptocurrencies: Sextortion in the Bitcoin Ecosystem*, Proceedings of the 1st ACM Conference on Advances in Financial Technologies, 2019.

[41] Federal Trade Comission; https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammers-cashing-crypto-craze, December, 2022.

[42] M. DeLiema, and P. Witt. *Mixed Methods Analysis of Consumer Fraud Reports of the Social Security Administration Impostor Scam*, Ann Arbor, MI. University of Michigan Retirement and Disability Research Center (MRDRC) Working Paper; MRDRC WP 2021-434.

[43] F. Jáñez-Martino, R. Alaiz-Rodríguez, V. González-Castro, E. Fidalgo, E. Alegre, *A review of spam email detection: analysis of spammer strategies and the dataset shift problem*, Artif Intell Rev, 2022.

[44] Github; https://github.com/409H/EtherAddressLookup, December, 2022.

[45] Bitcoinabuse; https://www.bitcoinabuse.com/, December, 2022.

[46] J. Wu, Q. Yuahn, D. Lin, W. You, W. Chen, C. Chen, Z. Zheng, *Who Are the Phishers? Phishing Scam Detection on Ethereum via Network Embedding*, 2019.

[47] W. Chen, Z. Zheng, J. Cui, E. Ngai, P. Zheng, and Y. Zhou, *Detecting Ponzi Schemes on Ethereum: Towards Healthier Blockchain Technology*, In Proceedings of the 2018 World Wide Web Conference (WWW '18). International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE, 2018, pp. 1409-1418.

[48] A. Sultan, *Fear of missing out and self-disclosure on social media: the paradox of tie strength and social media addiction among young users*, Young Consumers, Volume 22 Issue 4, 2021.

[49] D. Rozgonjuk, C. Sindermann, j. Elhai, C. Montag, *Individual differences in Fear of Missing Out (FoMO): Age, gender, and the Big Five personality trait domains, facets, and items*, Personality and Individual Differences, volume 171, 2021.

[50] R. Auer, D. Tercero-Lucas, *Distrust or speculation? The socioeconomic drivers of U.S. cryptocurrency investments*, Journal of Financial Stability, Volume 62, 2022.

[51] S. Albert, J. Duffy, *Differences in Risk Aversion between Young and Older Adults*, Neurosci Neuroecon, 2012.

All links were accessed December 7, 2022

Chapter 6

On the Security of Processes: An Overview of Business Process Compromise (BPC) Attacks

Jasmin Hochuli

Globalization and digitization of the economy have an impact on the management of a business' processes and the use of information systems [13]. Even though the re-engineering and automation of business processes enables enterprises to stay in a market, the transformation comes with high risks [9].
The business process re-engineering can lead to so called business process compromise (BPC) attacks. When a company becomes a target, different attack vectors are applied to gain access to the system [13]. Once a backdoor has been found, the attackers intend to take control over the enterprise's business processes, which enables them to alter the enterprise's operations to their advantage [13]. The transformation of the business processes often happens unnoticed and seems legitimate to the company, which contributes to devastating consequences [12]. Known incidents like these are the Bangladesh Bank Heist in 2016 or the attack on the container tracking system in Antwerp in 2013 [12].
This paper's purpose is to find out which types of attack vectors are applied when a company becomes a victim of a BPC attack, why such an attack is successful, and what impacts that this attack has on the company. Furthermore, the paper suggests countermeasures which could help to prevent becoming a victim.
Three types were found in the reported cases to distinguish between different BPC attacks: diversion, piggybacking, and financial manipulation. The countermeasures that can be taken are authentication, authorisation, education of employees, regular audits, separation of duties, and isolation of business processes [1; 5; 7; 13; 14].

Contents

6.1 Introduction 57
6.2 Background 57
6.2.1 Terminology 57
6.2.2 Digitization of Business Processes 57
6.2.3 Attack Vectors on Businesses 58
6.2.4 Cybersecurity Countermeasures 58
6.3 Process Attacks 59
6.3.1 Business Process Compromise 59
6.3.2 Example Cases 59
6.3.3 Business Email Compromise 61
6.4 Discussion 61
6.4.1 Types of BPC attacks 61
6.4.2 Why BPC attacks are successful 62
6.4.3 Impact on businesses 63
6.4.4 Relation to BEC 63
6.4.5 Countermeasures 63
6.5 Summary and Conclusion 64

6.1 Introduction

Globalization and digitization have contributed to the transformation of a company's objectives and characteristics [9]. Information can be seen as a "new factor of production, which gradually replaces other factors of production" [11]. Primarily, this had an impact on the management of their business processes and the use of distributed IT-systems [13]. For every business in a market, it is essential to push down the costs to the lowest level possible to keep up with its competitors. To accomplish this, the re-engineering as well as the digitisation of business processes are indispensable [9; 11].
The transformation of a business' processes comes with many benefits, such as increased efficiency or rapid development [11]. However, it can also depict risks, which should not be neglected. These risks include giving the responsibility for specific workflows out of human hands to a system, revealing business specific information, and giving access to a number of people across many countries [1]. These vulnerabilities can be exploited by attackers to take over control of the business process and change it in their favor, which is called a Business Process Compromise attack [13].
So far, only little research on BPC attacks has been carried out. However, the topic can be found in several blogs for cybersecurity like in the MTI blog [13]. MTI describes how BPC attacks proceed and which countermeasures could be taken against [13]. Likewise, the paper "Hacking the Process" [12] mentions the sequence of events of a BPC attack and additionally gives an overview of example cases and countermeasures. The blog entry of Trend Micro compares BPC attacks to targeted attacks, categorizes the types of BPC attacks, gives short explanations about known incidents, and suggests high level defense strategies [14].
What has not been examined until now, is a full overview of BPC attacks, why they are successful and how they impact a targeted business. This paper aims to reveal the security risks for companies when they automate their business processes, investigate the attack vectors that were used in the past and the impacts such attacks had on a company when it became a victim of a BPC attack. Furthermore, it suggests countermeasures which could help to prevent becoming a victim.

6.2 Background

In order to understand why process attacks can occur, this section offers an explanation of the most important terms used, as well as an introduction into the environment where these attacks happen.

6.2.1 Terminology

Vulnerability A vulnerability is a weakness in a system that can potentially be used as a target of a cyberattack [10].

Threat A threat is when security weaknesses are used to infiltrate a system and have a negative impact on it [10].

Attack When an attack happens, "actions are taken to damage a system or disturb its routine operations by exploiting vulnerabilities using various tools and techniques" [10].

6.2.2 Digitization of Business Processes

Due to the globalization and the digitization of the economy, businesses need to adjust to the technological innovations in order to stay competitive in the market. When information becomes a new factor of production, the business' focus needs to be shifted. Mostly,

enterprises implement an ERP-system to internally track all their business processes and make the information available to the different departments [4; 9; 11].
Restructuring of business processes is one aspect that is looked at when a business wants to catch up with the digitization. Business processes are analyzed and adjusted by eliminating bottlenecks, changing the sequence or parallelizing processes. This can help an enterprise to increase the productivity, achieve competitiveness, and decrease costs [1].
Additionally, business processes can be fully automated, which can prevent human errors and reduce the time of execution of a business process. One single database is available for many different systems, such that the re-entry of data can be eliminated and it can be made use of computing power, which accelerates the execution of business processes [4].

6.2.3 Attack Vectors on Businesses

When processes in enterprises have been automated, they are exposed to risks. One of this risk is being attacked by an external party. They, however, do not need to be criminally intended attacks, they can also occur because the system has security vulnerabilities [5]. In this subsection, the different attack vectors which can target companies are discussed [11].

Malware When "the attacker deploys malicious software programs to gain unauthorized access to computer systems by exploiting its security vulnerabilities" [10] the victim is attacked by malware.

Denial-of-Service In a Denial-of-Service attack, a device becomes inaccessiblex because the network is overloaded by a huge number of requests sent by the attacker [10].

Brute force attack This attack is defined as trying to gain access to any data by repeatedly attempting to guess a key, like a password [5].

Phishing When social engineering is used by an attacker imitating a trustworthy party to extract sensitive data from a user, this is called phishing [10; 5].

Man-in-the-Middle attacks Man-in-the-Middle attacks target the communication between two parties to gain control of their channel without noticing of the sender or receiver [10].

6.2.4 Cybersecurity Countermeasures

There are various countermeasures which can be taken by businesses in order to prevent the cyberattacks that were mentioned in the previous subsection. [5] suggests the following ones:

Continuous risk assessment Each company has different characteristics, and they might change over time, such that risk assessments should be done regularly [5; 13].

IT environment's health An enterprise should make sure that all hard- and software has the latest updates [5].

Authentication Business information should only be accessible via a password or more complex authentication [5].

Internal commitment and responsibility The personnel of a company should be briefed which policies and procedures they should follow [5; 13].

Access of information It is important to only give those users access who are currently working in the company [5].

Data retention Data that is outdated or not used anymore should be removed [5; 12].

6.3 Process Attacks

After the description of how businesses deal with globalization and digitization, explanations of the most important terms, what kind of attacks vectors exist and how they could be prevented in general, this section covers the main topic of this report, namely process attacks.

6.3.1 Business Process Compromise

A Business Process Compromise is an attack which aims to change the operations of a business process in an enterprise to the attacker's favor [13].
When a company becomes a target of a BPC attack, different attack vectors are applied to gain access to the system. Once a backdoor has been found, the attackers intend to control the business' processes. This can be achieved by learning from the business processes which are precedent and following to the initially targeted process to find out more about a company's procedures and structure. With this knowledge, the adversaries are able to change the business processes according to their benefit. Usually, the operations in the business process happen without detection and can be seen as legitimate by the company, because the attacker groups use technology to erase their traces [12; 13].
The main motivation for BPC attacks is the financial profit. The perpetrators do their best to stay unnoticed as long as possible to take money from the company. For example, in the attack on the Bangladesh Central Bank, the criminals were able to steal 81 million US dollars by transferring money to their bank account [3; 12; 13].
When looking at the cases of known BPC attacks, it can be noticed, that they sometimes differ in the actions taken by the hacker groups. According to Trend Micro [14] three different types of BPC attacks can be distinguished:

Diversion BPC attacks can be categorized as diversion when hackers manage to transfer money to trusted channels. This can be done by either changing codes or making use of malware to transfer the money to the desired account. [14]

Piggybacking Piggybacking means that an attacker takes advantage of having access to key business processes to transfer malware via the network or illegal goods in the real world [14].

Financial Manipulation A business process is financially manipulated if attacker groups "introduce malicious variables into a key business system or process" [14].

6.3.2 Example Cases

There have been several incidents that can be categorized as BPC attacks. The two most well-known ones are the Bangladesh Bank Heist and the Attack in the Port of Antwerp.

6.3.2.1 Bangladesh Bank Heist

In February 2016, the Bank of Bangladesh became a victim of a business process compromise attack. The group of hackers stole $81 million dollars by taking over control of the SWIFT gateway in order to request fund transfers in the name of the bank. In Figure 6.1, the diamond model has been applied to understand thoroughly what happened in the incident [3; 12].
First, the attackers used spear phishing emails which included malicious files. Once they found a backdoor with the malware *MACKTRUCK*, they were able to control the bank's workstations. The communication with these stations was driven by a command and

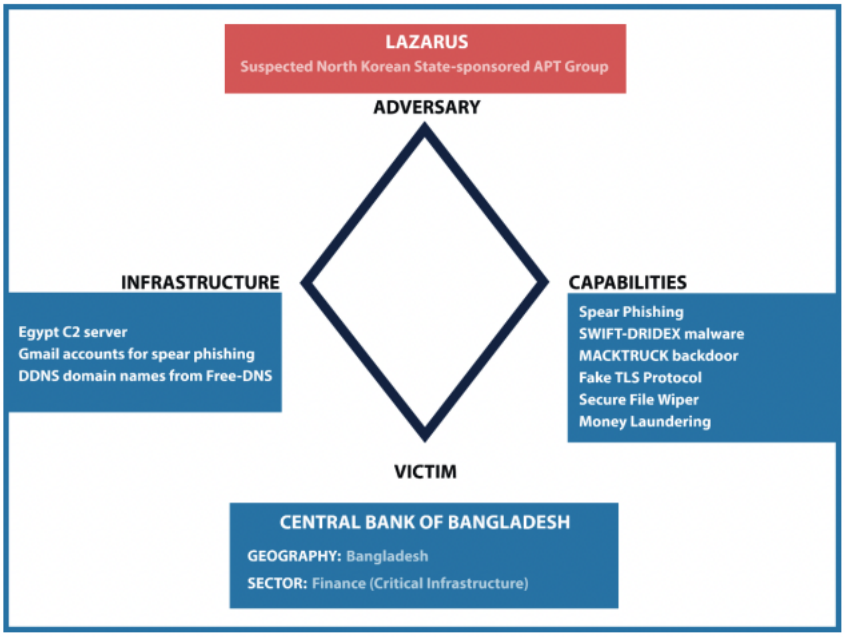

Figure 6.1: Diamond model of the Bangladesh Bank Heist [3]

control server, which faked a TLS protocol. With this communication protocol, the attackers were able to send messages in the network while staying undetected. Furthermore, a malware called *DRIDEX* enabled the attackers to control the SWIFT software. With this control, they could fake payment requests and cover their intrigues with tampering SWIFT responses. Finally, they used a Secure File Wiper malware to erase all their traces [3].
All in all, the attacker group tried to take $951 million US dollars in 35 fund transfer requests, which all seemed like legitimate payment requests. However, they 'only' managed to steal $81 million US dollars [3].
A year after the attack, the SWIFT provider tightened their security controls and introduced annual checks of each customer regarding their level of compliance. Moreover, in 2019 they released a new version which was able to detect suspicious payments which could be a threat [3].

6.3.2.2 Attack on Port of Antwerp

In 2013, a group of hackers managed to infiltrate the container tracking system of the Port of Antwerp in Belgium [12]. Since this enabled them to locate specific containers, they could smuggle drugs worth $17 million US dollars without noticing [14; 7].
In order to gain access to the port's system, spear phishing emails containing malware were sent to the port authorities or shipping companies. Even though this infiltration was discovered and countermeasures were taken by installing a firewall, the perpetrators found a way to continue their operations. They broke into the building where the computers for controlling the containers were located and placed devices to regain access to the network [7].
After that, the attacker group could learn from the business processes in the system to understand the container handling systems [12]. Soon they were able "to locate specific containers, find the security code for a container, change the location and scheduled delivery time, and make off with smuggled drugs before the scheduled pickup" [7]. Due to this access, they could move the containers without anybody noticing and delete all traces about the existence of any fraudulent operations [7].

6.3.3 Business Email Compromise

A closely related topic to Business Process Compromises are Business Email Compromises (BEC).
Business email compromises are attacks where a threat actor sends a malicious file or link via email using an address that seems to be known by the victim [8; 15]. Social engineering is used to deceive employees of a company, which can be "some form of encouraging language, a request, an alert conveying a sense of urgency, or a proposal seemingly too good to pass up" [15] [2].
The FBI has categorised the BEC attacks into the following three types:

Spoofing If an email address has tiny changes which can be easily overseen to convince the victim to be somebody they know [8].

Spear Phishing Spear Phishing is the impersonation of an attacker to get confidential information of the victim to gain access to accounts or sensitive data [8].

Malware Malicious software that is being downloaded when clicking on a malicious link can enable access to an enterprise's network, which can be used to steal sensitive data or communicate [8].

BEC are mainly carried out to convince victims to transfer money to the attackers. According to the report of PwC, phishing is one of the most popular attack vectors [15].

6.4 Discussion

So far, the paper has given different definitions and explanations for BPC attacks. This section focuses on putting the theory of BPC attacks into context to the known incidents and give suggestions on how they can be prevented.

6.4.1 Types of BPC attacks

Trend Micro [14] has created an overview of even more incidents than mentioned until now. They were categorized into the three types of BPC attacks, namely diversion, piggybacking, and financial manipulation as described before. Figure 6.2 shows a timeline of past attacks, each categorized in one of these three types using different colors.
Noticeable in Figure 6.2 is that most of the BPC attacks have been assigned to the category of Diversion, which are colored in red. It matches with the assumption that the motivation of the perpetrators is for the most part financial [13].
On the one hand, the Bangladesh Bank Heist which was described in Section 6.3.2.1 belongs to the type diversion [14]. This can be explained by the fact that the perpetrators used the bank's business processes to send money to their accounts and therefore diverted the flow of money [3; 13].
On the other hand, the attack on the Port of Antwerp is categorized as a piggybacking attack because the perpetuates did not divert the path of transferring money. Hence, they took advantage of the port's container tracking system to illegally ship drugs [7; 14].
The third attack type, financial manipulation, has only one reported case, namely the attack on the Russian trading system in 2014. In this incident, exchange rates of currencies were manipulated [14].

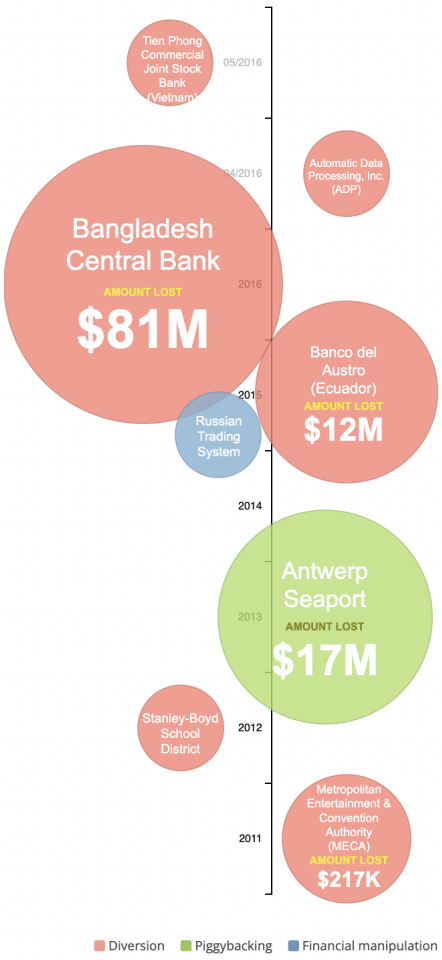

Figure 6.2: Timeline of Known BPC Attacks [14]

6.4.2 Why BPC attacks are successful

To begin with, the paper of [4] has found out that the more business processes are integrated into information systems, the more effort is put into cybersecurity to cancel out the risks of cyberattacks. However, the realization of these demands is a challenge for enterprises, because they have to cover every possible vulnerability. Although a lot is invested into testing systems, there can always be loopholes and human errors which were not foreseen [12].

In addition, since there is a lot of effort taken by the attackers to stay unnoticed, it is difficult for a company to detect such an incident. The perpetrators in both example cases used programs to erase their traces, which made it nearly impossible to discover that there was a change in business processes [3; 7].

Furthermore, many employees expect the business processes to work without any problems, which can help BPC attacker groups to stay undiscovered. If every worker in a company blindly trusts the technology, hence assumes that every request is legitimate and does not get suspicious by any misleading statements, it can positively contribute to the success of the attackers [13].

Moreover, it is possible that the transparency of the business process model structure forms a way to learn about a company's standard procedures and manipulate them. If too many employees have access to a great amount of detailed information about business processes, the risk of a worker manipulating a business process increases [1].

6.4.3 Impact on businesses

Clearly, the biggest impact a BPC attack has on a company is the vast amount of money it can lose. The sum of the loss depends on how long the perpetrators stay undiscovered and how profoundly they alter business processes. In addition, if an attacker group has gained access to a business process and learns from it, the damage can increase exponentially, because as seen in the example cases, the hackers moved laterally to other business processes and compromised those as well [3; 7; 12; 13].
Furthermore, it can be claimed that a business loses its reputation when it becomes public that a hacker group has been operating with the business processes of the enterprise. It is likely that the attackers have come across many sensitive data, which leads to a loss of trust and damages the company's image [5].
Lastly, because the perpetrators have altered the business processes, the company can also lose a lot of information, which was diverted to someone else. However, this is not the typical goal of a BPC attack [5].

6.4.4 Relation to BEC

On the one hand, since the entry point of both example cases was spear phishing, one could argue that BPC attacks can be closely related to BEC attacks. In order to gain access to a system, the attacker group somehow needs to pass the border of authentication in a company's network, which is mostly done using phishing and social engineering techniques [15; 12].
On the other hand, BPC and BEC attacks still have a main difference. The target of the attacker group to steal money from a business in BEC are the employees, while it is a specific business process in BPC attacks. This means, that the motivation for phishing or other BEC attack vectors in BPC attacks is only the access to the company's system in order to manipulate its business processes.To conclude, BPC and BEC have the same goal, but different targets.

6.4.5 Countermeasures

To prevent BPC attacks, a company should take a set of countermeasures. Firstly, it is important, that the sensitive data is protected and confidentiality is ensured throughout the whole process [1]. This includes only having access through authentication, which makes it harder for hackers to find an entry point into the business' system [5].
Secondly, only people who are authorized to know certain information or actions should have access. It is therefore important to keep the list of people who have access to a certain set of information always up-to-date in order to prevent any outside party to have access to sensitive data [1; 5].
To continue, the employees of a company should be briefed on cybersecurity topics in order to establish awareness to suspicious communication, which can help to recognize early if there could be any intruder in the network [13].
Moreover, there should be regular checks to test the business processes model and long-established policies [13]. A security analysis of business processes as suggested by [9] could look like this:

1. "Identification of the business processes, their elements, and the related human principals
2. Valuation of the assets contained in the business processes and definition of their security levels
3. Identification of security requirements resp. vulnerabilities and threats

4. Assessment of resulting risks

5. Planning, design, and evaluation of suitable countermeasures" [9]

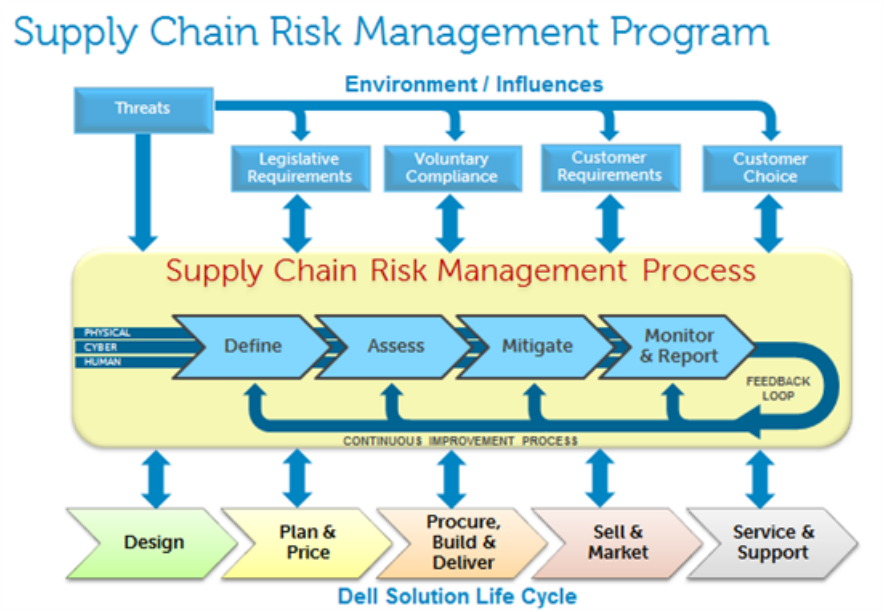

Figure 6.3: Supply Chain Risk Management of Dell [6]

Figure 6.3 gives an idea how the regular audits could be structured. Even though the company dell looks at the whole supply chain and not only on their internal business processes, the Figure reflects the view of regular checks in cycle where updated information is always fed back into the process of risk management [6].
In addition, the duties of the employees should be split up to different tasks. Hence, each worker should have their own responsibilities and tasks and, accordingly, also only access to the tools in the system they need for their specific duties. This countermeasure helps to decrease the likely-hood of an inside threat [1; 14].
Finally, the business processes themselves should work in isolation. The interfaces in between the processes should be encoded such that the lateral movement to learn from other business processes can be prevented [7; 13].

6.5 Summary and Conclusion

As explained in this paper, every business can possibly be a target of a BPC attack. It is therefore important to raise the awareness of such cyber incidents to prevent them from happening.
A BPC attack can be categorized into three different types: diversion, piggybacking and financial manipulation. Diversion is the category where the most attacks have been reported so far. Therefore, especially the financial department should be trained in detecting suspicious communication which could lead to BPC attacks.
The examination of how much a business wants to integrate their business processes into an information system is a crucial element for business process management. Because the more is integrated, the more it has to be tested. For testing, a lot of effort is needed and even when everything seems to be working perfectly, there can still be loopholes or human errors.
Furthermore, the perpetrators do their best to stay unnoticed, which makes it even harder to discover a BPC attack. For the employees, this is especially a challenge because they usually think that everything works without any problems.

A BPC attack can lead to a loss of a lot of money, when a hacker group manages to stay unnoticed for a long time and use the company's business processes to benefit from them. Other impacts are loss of reputation or information.
Due to the mentioned risks of BPC attacks, this paper suggests the following countermeasures to prevent them:

- Authentication
- Authorization
- Education of employees
- Regular audits
- Separation of duties
- Isolation of business processes

To conclude, every digitization step in a business is linked to cybersecurity risks and should therefore be thought through in depth before the implementation to prevent attacks like BPC. Especially due to the fact that there are many touch points of business processes which affect different parts of a company, every single component of an enterprise should be adjusted to fight cybersecurity risks. This also means that only the combination of several countermeasures can lead to sufficient protection against BPC attacks.
For future work, it would be interesting to investigate how companies are affected by BPC attacks today in connection with the cloud. It could be examined whether it is harder to alter business processes and if the vulnerabilities change when businesses use a cloud for their system. Moreover, it would be interesting to find a tool or standardized process which would help to discover or prevent process attacks in enterprises.

Bibliography

[1] A. Alhanouf and A. Alturki: *An Empirical Investigation of the Relationship Between Business Process Transparency and Business Process Attack.*, International journal of advanced computer science & applications, vol. 12, no.4, pp. 534-545, 2021.

[2] N. Saud Al-Musiba, F. Mohammad Al-Serhania, M. Humayuna and N.Z. Jhanjhi: *Business email compromise (BEC) attacks*, Materials Today: Proceedings, 2021.

[3] R. Balu: *Bangladesh Bank Cyber Heist: Incident Analysis*, October, 2022. `https://smartech.gatech.edu/bitstream/handle/1853/67083/BB%20Heist%20-%20Incident%20Analysis.pdf?sequence=1&isAllowed=y`. [Accessed Nov. 2, 2022].

[4] R. Baskerville, F. Rowe and F-C. Wolff: *Integration of Information Systems and Cybersecurity Countermeasures: An Exposure to Risk Perspective*, Association for Computing Machinery, vol. 49, no.1, February 2018.

[5] A. Bendovschi: *Cyber-Attacks-Trends, Patterns and Security Countermeasures*, Procedia Economics and Finance, vol. 28, pp. 24-31, 2015.

[6] J. D'Andrea: *Live from the ARC World Industry Forum!*, Dell Company Updates, February 8, 2012. `https://www.dell.com/en-in/blog/live-from-the-arc-world-industry-forum/`. [Accessed Nov. 24, 2022].

[7] J. DiRenzo, D.A. Goward and F.S. Roberts: *The Little-known Challenge of Maritime Cyber Security.* `http://archive.dimacs.rutgers.edu/People/Staff/froberts/MaritimeCyberCorfuPaper.final.pdf`. [Accessed Nov. 2, 2022].

[8] Federal Bureau of Investigation: *Business Email Compromise*, Scams and Safety. `https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/business-email-compromise`. [Accessed Nov. 2, 2022].

[9] P. Herrmann and G. Herrmann: *Security requirement analysis of business processes*, Electron Commerce Res, vol. 6, pp. 305-335, October, 2006.

[10] M. Humayun, M. Niazi, N. Jhanjhi, M. Alshayeb and S. Mahmood: *Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study*, Arab J Sci Eng, vol. 45, pp. 3171-3189, April, 2020.

[11] L. Lytvyn, A. Hryhoruk, L. Verbivska, O. Poprotskyy, T. Medynska and O. Pelekh: *Enterpreneship Transformation in the Context of the Digitization of Business Processes*, Postmodern Openings, vol. 13, no. 2, pp. 396-408, 2022.

[12] S. Moodley and J. Hasewinkle: *Hacking the Process - Business Process Compromise*, Offensive Security Zyston LLC, October, 2022.

[13] MTI Technology: *Security 101: Business Process Compromise*, Trend Micro Blog. https://mti.com/blog/2020/10/29/security-101-business-process-compromise/. [Accessed Nov. 2 2022].

[14] Trend Micro: *Business Process Compromise*. https://www.trendmicro.com/vinfo/us/security/definition/business-process-compromise/#BPCTypes. [Accessed Nov. 2 2022].

[15] PwC: *Cyber Threats 2021: A Year in Retrospect - PwC*. https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-annex-download.pdf. [Accessed Nov. 2 2022].

Chapter 8

An Overview into Pulse-Wave DDoS Attacks

Aleksandar Ristic

Distributed denial of service (DDoS) attacks can have severe consequences for companies from various industries. As DDoS attacks evolve, new threats like pulse-wave DDoS attacks arise, forcing companies to invest in protection or risk an attack. Awareness needs to be created about those new threats such that companies can react to reduce the impacts of such attacks. With the research of literature, this paper provides an overview such that basic knowledge about pulse-wave DDoS attacks can be collected without the need to have previous knowledge about this topic. As a result, this paper covers, on one side the technical aspects of pulse-wave DDoS attacks and, on the other side, the economic aspects related to the actors involved in such an attack.

Contents

8.1 Introduction 70
8.2 Pulse-Wave DDoS Attacks 70
8.2.1 Botnets 70
8.2.2 Types of Botnets 71
8.2.3 DDoS Attacks 71
8.2.4 Pulse-Wave DDoS Attacks 72
8.3 Protection against DDoS Attacks 73
8.3.1 Types of Protections 73
8.3.2 Pulse-Wave DDoS attacks against traditional DDoS Protection 75
8.3.3 Defence against Pulse-Wave DDoS Attacks 75
8.4 The Business with DDoS Attacks 76
8.4.1 How attackers make money with DDoS Attacks 76
8.4.2 How third parties make money with DDoS Attacks 77
8.5 The Consequences of DDoS Attacks 79
8.5.1 Use Cases 79
8.5.2 Impacts of DDoS Attacks 80
8.5.3 Discussion 81
8.6 Conclusion 81

8.1 Introduction

For large information technology companies, organizations, educational institutions, social media companies, and government sectors, distributed denial of service (DDoS) attacks can cause disturbance in day-to-day business. Those attacks can lead to data theft, revenue loss, broken infrastructure, productivity loss, and more [1]. A new type of DDoS attack is pulse-wave. They are more threatening to existing DDoS mitigation systems, and therefore, additional protection is needed against pulse-wave DDoS attacks [2]. Companies that have to fear a pulse-wave DDoS attack are now forced to spend more money on detection and protection. In the meantime, DDoS attack as a service is becoming more popular. It allows the attackers to execute DDoS attacks increasingly cheaper such that attackers benefit even more because of the low costs they have [3]. This report aims to extend the comprehension of the features and functioning of pulse-wave DDoS attacks, presenting its definition and characteristics, and also the challenges towards detection and mitigation. Further on, economic impacts of DDoS attacks are analysed. The first section 8.1 contains the introduction. Then the section 8.2 follows and explains relevant terms for understanding the report's content like the concept of botnets, the types of botnets, DDoS attacks and what pulse-wave DDoS attacks are. After that, the section 8.3 will explain how one can repel DDoS attacks and the problems of repelling pulse-wave DDoS attacks. The second part of the report will then deal with the business with DDoS attacks in section 8.4. There, the economics behind DDoS attacks, the different actors involved and how they profit or lose through such attacks will be addressed. The consequences will be discussed in section 8.5 that also contains use cases of DDoS attacks. Finally, the third part of the report contains the conclusion in section 8.6 that summarizes the findings and discussions and presents the author's perception of the work. To carry out the work for creating this report, a literature research was conducted. Collecting multiple literature enabled the creation of an overview that contains different aspects related to pulse-wave DDoS attacks.

8.2 Pulse-Wave DDoS Attacks

8.2.1 Botnets

To explain botnets, one first needs to know what a bot is. A bot is a software program designed to perform automated functions [4]. One example of a bot would be a content scraping bot designed to save content on different web pages [5]. Bots do not have to be malicious, but they can. If a network of compromised computers is under the remote control of a human operator, then this is called a botnet. The human operator controlling the bots in a botnet is called "Botmaster" [4]. Hackers create a piece of malware (or a ready-to-use malware that can be modified) and use the malware to control infected computers and devices remotely. This enables them to infect millions of computers because they can infect other devices it interacts with after a computer has been compromised. Those infections can happen, for example, by automatically sending spam emails, pop-up advertising, where clicking on the ad will download an executable file, or downloading software from an untrustworthy source, which might be a botnet malware [5]. The spread of botnets can happen in two modes: active (without needing any user intervention by having a designed mechanism to find other potential devices on the internet and infecting them) or passive (with the help of human intervention, for example, infecting other devices with phishing or social engineering) [5].

8.2.2 Types of Botnets

Types of botnets can be differentiated based on how the attacker controls them. The most common botnets are the following ones observed in Table 8.1.

Table 8.1: Most common botnet types [5]

Type	Description
Command and Control	All the devices in the botnet communicate with one central server.
Internet Relay Chat (IRC)	Focuses on using low bandwidth and simpler communication to mask its identity and avoid detection.
Telnet	All devices in the botnet are connected to the main command server. Therefore, it is a subtype of Command and Control. New computers are added to the botnet via a scanning script that runs on an external server. When the scanner finds the login, then the new computers are infected with malware.
Domains	When a device is infected, then is accesses web pages or domains that distribute commands. The code can be updated by the botnet owner from time to time.
P2P	In this case, botnets are not connected to a central server. They are connected peer to peer. Every infected device in the botnet acts as a server and client.

Those different types of botnets can do different forms of botnet attacks and cyber crimes. Some attacks are spam attacks (when botnets send spam and fraud emails to fraud the recipient and infect the device), stealing personal data such as mail accounts or bank credentials, or launching denial of service attacks [6].

8.2.3 DDoS Attacks

Distributed Denial-of-Service (DDoS) attacks firstly appeared in June 1998 [7]. They aim to make a victim unable to provide services regularly on the Internet. Figure 8.1 shows the architecture of a DDoS attack. To set up the hierarchical attack architecture, the attacker first chooses more than one handler which has security vulnerabilities [8]. Then he intrudes on them by gaining access rights. After that, the attacker selects agents the same way he selected handlers, but this time indirectly through handlers. The agents are then used to perform DDoS attacks by simultaneously sending uncontrollable amounts of malicious traffic to a target system. This traffic overwhelms the victim's system and causes the disruption or denial of service to legitimate traffic since the victim's system has now to deal with the attack.
The attacker controls the communications among the three systems to compromise the attack. The attacker scans to select handlers and agents to find hosts with security vulnerabilities. For secure communication and compromise among the three systems, the attacker encrypts the messages for information exchange. The agents randomly generate the source IP addresses of attack packets to hide their real addresses. This makes it difficult to trace and identify the real attacker [8]. A typical DDoS attack has a waveform, with a gradual traffic ramp-up that leads to a peak followed by either an abrupt drop or a

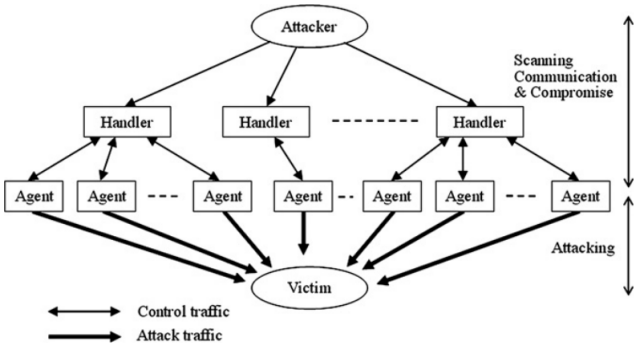

Figure 8.1: Architecture of DDoS Attack [8]

slow descent. This can be seen in Figure 8.2. The pattern resembles a triangle or sawtooth waveform.

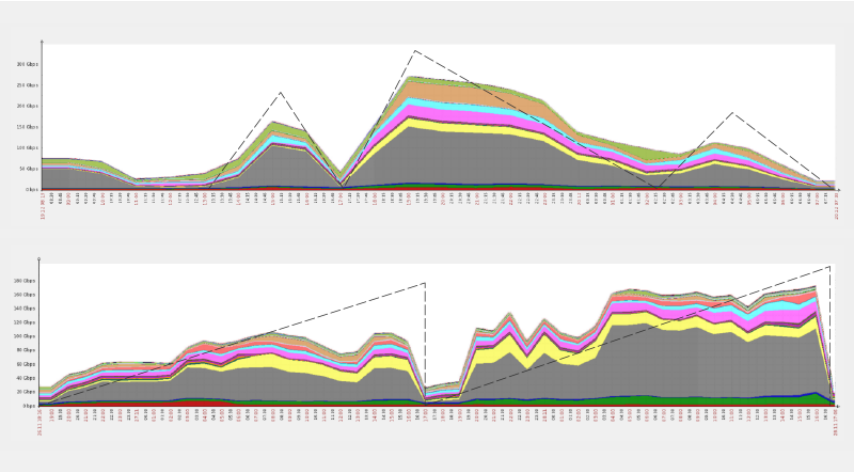

Figure 8.2: Typical DDoS traffic patterns [9]

Whenever the attackers are mobilizing their botnets, this can be seen in the incline of the DDoS waves until the peak. Therefore the incline represents the time the attackers need to rally up the geographically scattered networks that can consist of tens of thousands of different devices [9]. After an attack, the DDoS wave declines because the attacker is stopping the malicious traffic and attacks then after a time period again. The longer the attack lasts, the higher its chances are of being detected by the defense systems of the victim. Limiting the attack duration per attack allows the attacker to reduce the detection rate and then repetitively launch more attacks later without risking being detected [10].

8.2.4 Pulse-Wave DDoS Attacks

Pulse-wave DDoS attacks consist of short, high-rate traffic pulses. The attacker generates a pulse-wave DDoS attack towards a critical network link. This can exhaust the network's capacity and prevent legitimate flows from using it. There exist different kinds of attack traffic. On the one hand, the attacker could use a botnet of infected devices which directly floods traffic toward the link. On the other hand, the attacker could use reflection and amplification techniques, which send spoofed requests to open servers such that their responses cross the link. Or the attacker could also use complex link-flooding attacks, which exchange low-rate flows from numerous sources to numerous destinations such that they also cross the link [2].

Figure 8.3 shows the pattern of a pulse-wave DDoS attack. When looking at the pulse-wave patterns, it stands out that there is no gradual incline like in typical DDoS attacks. The incline of Gbps happens much faster, such that within a matter of seconds, a 300Gbps botnet is mobilized.

Figure 8.3: Pulse-wave DDoS traffic patterns [9]

Besides the large increase of Gbps within the smaller period, the attacks are repeated with high precision and can last for days. Instead of shutting down the botnets after an attack and mobilizing them again for another attack, the attackers switch their targets on-the-fly. This explains why the peaks are reached so much faster than in a typical DDoS attack [9].

8.3 Protection against DDoS Attacks

8.3.1 Types of Protections

8.3.1.1 Analysis-Detecting-Switching-Cleansing Scheme

The analysis-detecting-switching-cleansing scheme is the scheme that most DDoS mitigation systems use. Figure 8.4 shows the architecture of such a defense scheme. Stage one shows the normal operating mode where legitimate traffic is happening, and stage two shows the situation when an attack is launched. When an attack pulse happens, the resource remains unprotected and is usually unavailable for 1-5 minutes (often up to 10 minutes) until stage three is reached.
In stage three, the traffic is redirected to a scrubbing device. This may take 5-20 minutes, and then stage four is reached, where the traffic passes through a mitigation device. After the attack, stage one is reached again with the normal operating mode [11].

8.3.1.2 Hybrid solution

A second type of protection against DDoS attacks is to employ hybrid solutions. Hybrid solutions combine hardware scrubbing equipment installed in the local network and cloud DDoS protection services [11]. The first defense line is hardware on-premise products,

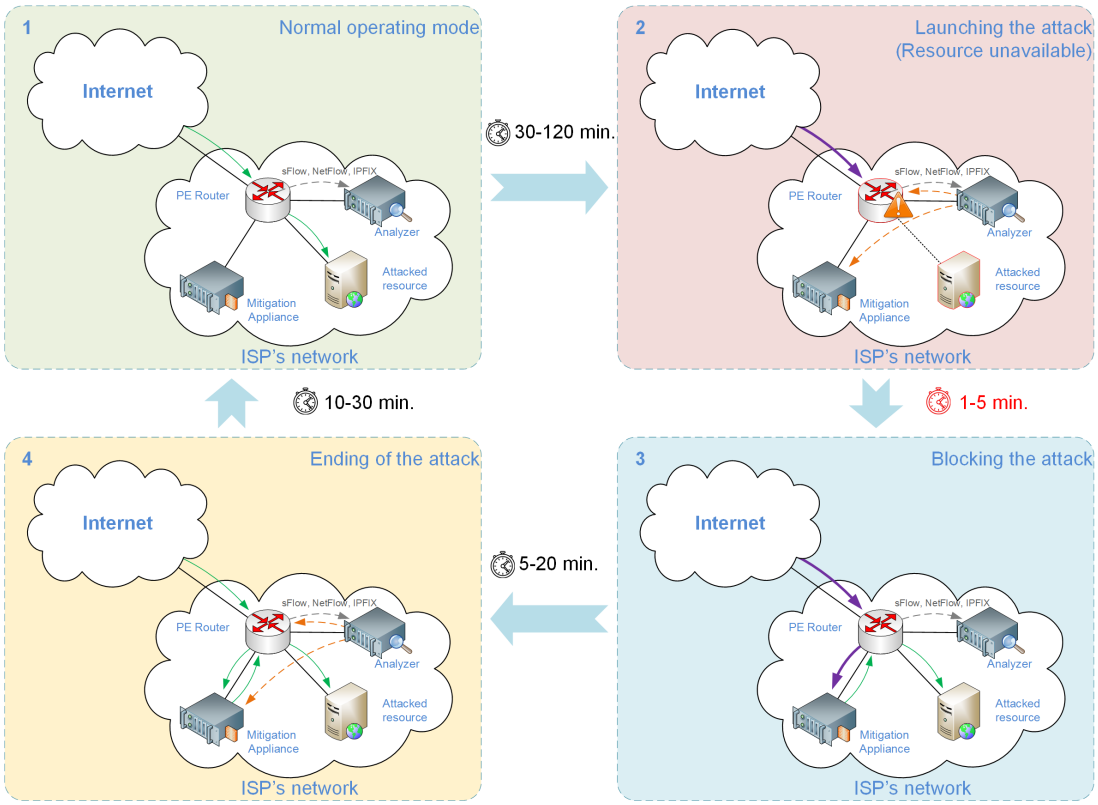

Figure 8.4: Analysis-Detecting-Switching-Cleansing Scheme [11]

and the second layer of protection is the cloud solution [12]. Figure 8.5 shows how an attack on a hybrid solution would look like.

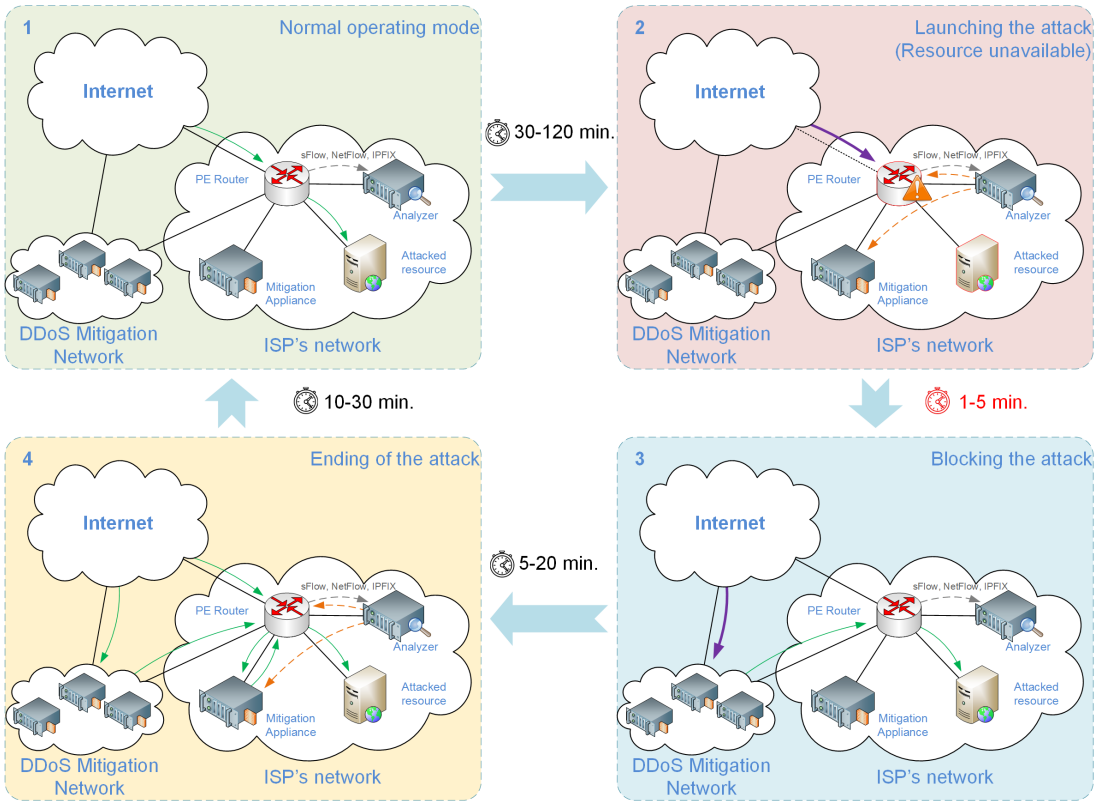

Figure 8.5: Hybrid solution [11]

The normal operating mode changes if an attack happens from stage one to stage two. The DDoS attack overloads the channel and isolates a victim's network from the internet.

The resources are unavailable for up to 5 minutes while the engineers try unloading the channels. This is done by removing the announcements of the attacked networks and sending them to the protected channel of a specialized operator, shown in stage three. While the engineers were busy redirecting the traffic to the protected channel, the DDoS attack had already ended and reached stage four. Attackers then use a new pulse to attack other resources (networks) of the same operators, while cloud protection is still used for the first victims. Like in the Analysis-Detecting-Switching-Cleansing Scheme, the DDoS attack cycles can be repeated multiple times [11].

8.3.2 Pulse-Wave DDoS attacks against traditional DDoS Protection

Whether the analysis-detecting-switching-cleansing scheme or the hybrid solutions are used, pulse-wave DDoS attacks remain a threat for both [11].
Regarding the analysis-detecting-switching-cleansing scheme, companies purchase mitigation equipment of limited channel and computing capacity since they do not expect multiple targets to be attacked at once [11]. However, one advantage of pulse-wave attacks is that attackers can attack multiple targets simultaneously. When the impulse stops and a short break happens, then the botnet is doing nothing but attacking another target [12]. So in such a case, the limited capacity of a company's mitigation equipment may not be enough to repel the attacks.
One way to address this problem is to use hybrid solutions, such that in cases of limited defense capacity, cloud DDoS protection services can be used. But another advantage of pulse-wave attacks is that with each pulse, they disconnect the equipment of the target company [12]. In an attack, the first pulse cuts off the network's ability to communicate with the outside world, resulting in a denial of service and preventing the mitigation appliance from activating the cloud scrubbing platform. For the pulse duration, the entire network shuts down completely [9]. So, restoring the performance after one pulse takes several minutes. While busy restoring the performance, the next pulse follows such that the correct operation of the security solutions is interfered with repeatedly because of the repeatedly arriving pulses. The result is that the on-premise hardware defense (the first layer in the hybrid solution) does not have enough time or bandwidth to request aid cloud and the server crashes [12]. At some point, the cloud may be reconfigured to activate itself when trouble is detected automatically, but the scrubbing process is still delayed because of the verification process. Also, the pulses disturb the creation of an attack signature, such that even if the cloud does come online, it still has to resample the traffic from scratch before being able to start the filtering process. In this case, the results would still be several mitigation process delays [9]. To summarize, the hybrid solutions are also not enough to defend against pulse-wave DDoS attacks.

8.3.3 Defence against Pulse-Wave DDoS Attacks

Although such on-demand DDoS mitigation systems are useful against traditional DDoS attacks, they can still not ensure an appropriate level of protection against pulse-wave DDoS attacks, as discussed in the previous chapter. In both presented solutions, every pulse of an attack can cause up to 5 minutes of unavailable web resources. This may not sound much in the first place, but if the pulses repeat themselves multiple times a day, this can be a problem for a company [11]. One possible solution that can help against pulse-wave DDoS attacks is round-the-clock DDoS protection or always-on protection. The operating principle is shown in Figure 8.6.
Such solutions have large channel and scrubbing capacities. They analyze and clean any incoming package, as seen in stage one. All traffic (whether legitimate or malicious) must pass the mitigation device. Therefore, there is no response time for an attack or changing

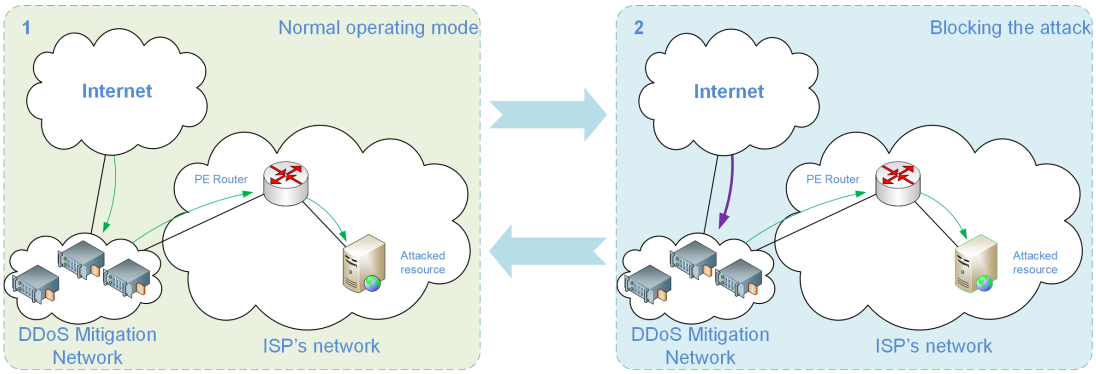

Figure 8.6: Round-the-clock DDoS Protection [11]

the routes because if malicious traffic is found, it is filtered before reaching the attacked resource. This can be seen in stage two. Thus, degradation of services is not noticed, even during large pulse-wave DDoS attacks that may last for hours or days [11].
A traffic scrubbing algorithm is necessary to separate and filter malicious traffic from legitimate traffic. A DDoS defense needs to be generic. With generic, the algorithm needs to identify various attack vectors at different granularity. This is because the list of new attacks is constantly growing, and having only a small set of coverable attack vectors will not be enough for a defense system [2]. But the more generic an algorithm, the bigger the risk of misclassifying traffic (meaning that an algorithm wrongly identifies legitimate traffic as malicious or vice versa). Therefore, the algorithm must also be safe in responding to attacks to avoid the risk of strong performance degradation in case of misclassification [2].
Those characteristics of an algorithm were fulfilled with the Aggregate-based Congestion Control (ACC). ACC works for conventional DDoS attacks but fails against pulse-wave attacks because it cannot keep up with the required fast reaction times. So, next to the generic and safe characteristics, the defense against pulse-wave DDoS attacks also needs to be fast and automated. It has to be fast to detect each of the pulses from a pulse-wave DDoS attack and automated so that there is no risk of misconfiguration of the mitigation device. Usually, the manual configuration of the threshold in mitigation devices is difficult. There is a risk of misconfiguration resulting in either too high or too low threshold configuration [2]. For example, if the threshold is too high, the mitigation device will miss an attack on traffic. Otherwise, if the threshold is too low, the risk of false positives is high since the mitigation device would consider legitimate traffic malicious. Therefore ACC-Turbo was developed considering those additional characteristics. It uses online clustering to effectively identify attack pulses and programmable scheduling to satisfy deprioritized traffic according to its maliciousness. ACC-Turbo enables real-time mitigation of pulse-wave DDoS attacks [2].

8.4 The Business with DDoS Attacks

8.4.1 How attackers make money with DDoS Attacks

The motives for an attacker to launch a DDoS attack can be different. Figure 8.7 shows why attackers execute DDoS attacks.
For example, for online gaming-related reasons, DDoS attacks can be executed by computer geeks without monetary interests. Other reasons can be based on revenge or protest against a particular company or organization, like the competitive rivalry between businesses or inter-personal/inter-group rivalries. Also, political or ideological disputes, for example, based on nationalism or religious controversy, can lead to DDoS attacks. Look-

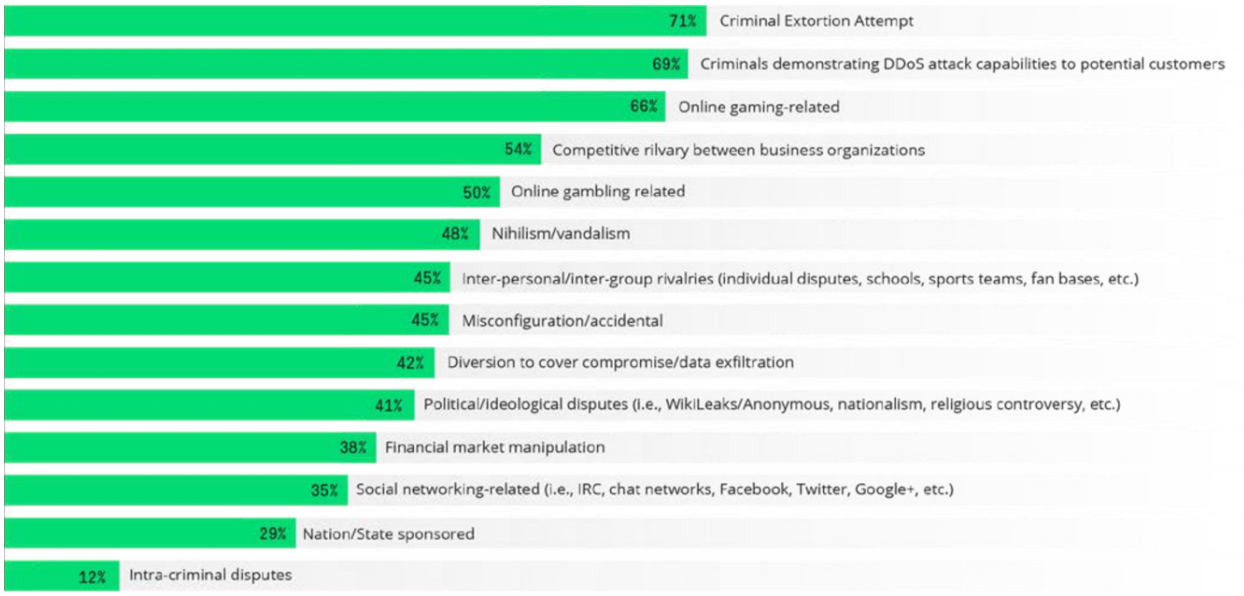

Figure 8.7: Motivations for DDoS attacks [13]

ing at how to make money as an attacker, one way, as shown in Figure 8.7 is by financial market manipulation [13]. Attackers could manipulate the financial market by combining DDoS attacks with misinformation disseminated through social media. This could be done by creating fake accounts or hacking existing ones in social media, investing heavily in equities that increase in value as target equity value drops, launching a DDoS attack, and spreading fake information through fake or hacked accounts. Then, when the target stock value has devaluated and the value of the derivative asset which the attacker possesses increases, the attacker can liquidate his assets and make illicit profits [14].
However, as Figure 8.7 shows, the most reported attack motive is criminal extortion. Attackers would send extortion letters to a company with an internet presence demanding the payment of a specific sum by a set deadline. If no payment happens, the threats in the extortion letter are initiated, and an enormous number of requests are sent to the web servers until they become inaccessible. Another method of an attacker would be to first block the company's online presence without warning with a DDoS attack. Then during the attack, the attacked company would receive a letter claiming responsibility, for example, by e-mail demanding either payment to an account by a deadline or another condition that must be met. If the deadline passes and the conditions are not met, then the attacks are continued [13]. The second largest motive for DDoS attacks is criminals demonstrating DDoS attack capabilities to potential customers. Thus, many DDoS attacks are advertisements for illegal DDoS-for-hire services [15].

8.4.2 How third parties make money with DDoS Attacks

8.4.2.1 DDoS as a Service

Traditionally, the execution of a DDoS attack was considered in multiple stages like shown in Figure 8.1. Attackers needed to create a botnet that was used to conduct the attack. But in recent years, a new model of DDoS execution has emerged, the DDoS-for-hire (or botnet-for-hire) that allows the attacks to be executed simply by renting an already established botnet. With DDoS-for-hire, the execution of a DDoS attack has been greatly simplified because the attackers no longer need to worry about the setup and maintenance of a DDoS botnet. Additionally, DDoS-for-hire have extremely low fees allowing a powerful DDoS attack for only $38/hour. Currently, about 40% of all DDoS attacks are executed

with DDoS-for-hire services [16]. The hackers that develop such DDoS-for-hire services make more money by using the power of one large botnet to service more than one customer simultaneously. As soon as a botnet is up and running, it can hit one target with a burst, then switch quickly to hit another target with a burst and alternate between the targets [17]. Since DDoS attacks are illegal, DDoS-for-hire service providers had to find a creative way of advertising their services for the mass market since they cannot openly advertise DDoS attacks. Therefore, to still reach the mass market and allow their business to fly under the radar, they call their services ”stressers” or ”booters” with the implication that their service can be used to test the resilience of one’s server. But since no verification of the service user’s identity or ownership of the target server is needed when using stressers or booters, users of such a service can ”stress test” anybody, which ultimately enables cybercrime [18].

8.4.2.2 Protection providers

The digital transformation related to the Coronavirus led to a significant increase in DDoS attacks. Kaspersky reports, that the DDoS attacks were 217% higher in the second quarter of 2020 than in the same period in 2019 [19]. Other DDoS data providers like Cloudflare reported that in specific months from 2021-2022, up to 28% of their customers were attacked or threatened as Figure 8.8 shows [20]. If there are more DDoS attacks, then more protection against DDoS attacks is necessary. Looking at the DDoS protection market with the protection providers, the DDoS protection market reached an estimated value of US$ 1,567.8 million in 2021 with a total revenue of US$ 1,375.6 million. Cloud-based solutions accounted for around 54% market share in the global DDoS protection market in that year. With the growing threat environment of IoT (Internet of Things) devices, the DDoS protection market is expected to reach US$ 6,530.5 million by 2032 [21].

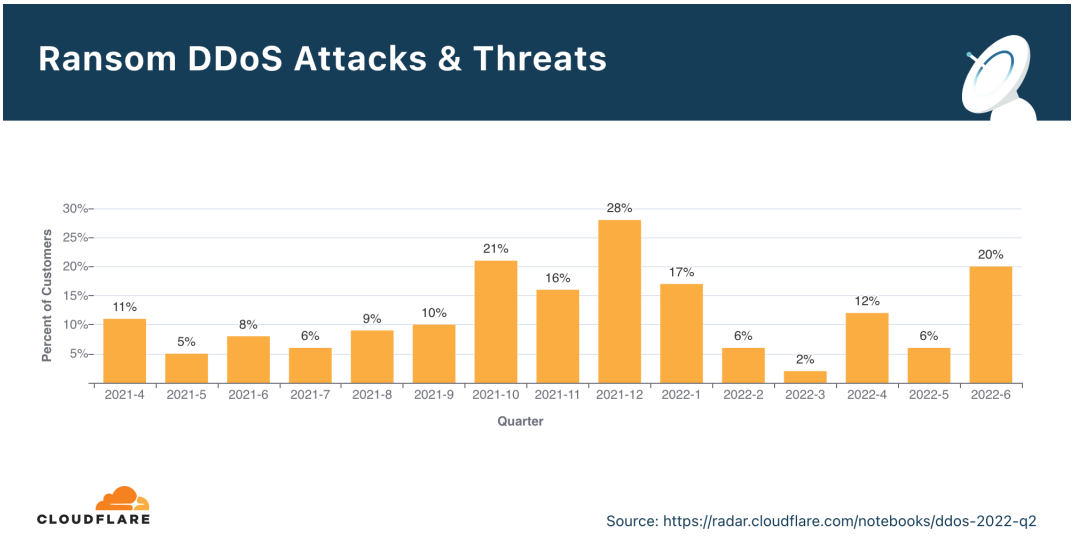

Figure 8.8: Ransom DDoS Attacks & Threats 2021-2022 [20]

This would mean a CAGR (Compound annual growth rate) of 15.3 % for 2022-2032. The cloud-based solution segment is expected to grow by 4.5x between 2022 & 2032 because of the rising of technologies such as AI, ML, and IoT. The cloud-based software helps organizations to scale up rapidly with the help of real-time configuration. The landscape of DDoS protection providers is competitive; therefore, they are focusing on various strategies for increasing their investments in research and development. To develop their DDoS protection to serve the customers and reduce the churn rate, protection providers acquire and enter into partnerships with other companies [21].

8.5 The Consequences of DDoS Attacks

8.5.1 Use Cases

8.5.1.1 The largest layer 7 DDoS Attack to date

A recently released report from Google Cloud describes the largest layer 7 DDoS attacks. This attack happened on June 1 on a Google Cloud Armor customer. The attacker sent a series of HTTPS DDoS attacks which peaked at 46 million requests per second, shown in Figure 8.9 [22].

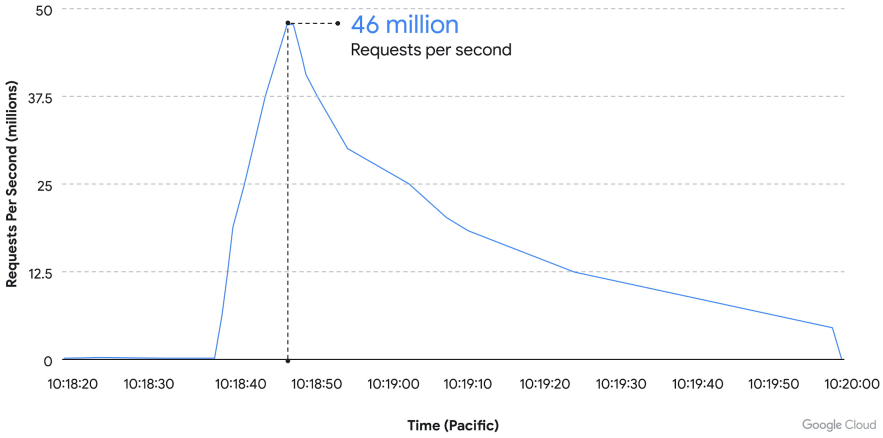

Figure 8.9: DDoS attack on Google Cloud Armor customer [22]

Before the attack started, the customer had configured the Cloud Armor Adaptive Protection of Google in their relevant Cloud Armor security policy. This enabled Adaptive Protection to learn and establish a baseline model of the normal traffic patterns for their service by using machine learning. At around 9:45 a.m., the attack began with more than 10,000 requests per second (rps) targeting the customer of Google. After eight minutes, the attack grew to 100,000 requests per second. The Cloud Armor Adaptive Protection of Google detected the attack because it classified it as abnormal, analyzed its incoming traffic, and generated an alert containing the attack signature. A rule to block the malicious signature was added to the alert so the customer's network security team could deploy the Cloud-Armor-recommended rule into their security policy. The deployment of the rule enabled the throttling of the attack traffic by dropping most of the attack volume at Google's network edge and thus blocking the attack on the customer. After two minutes, the attack started to ramp up, growing from 100,000 rps to a peak of 46 million rps. But since Adaptive Protection was already blocking the attack traffic on the customer, the target workload continued to operate as usual, and the targeted applications and services remained available. The attack decreased in the next few minutes, ending 69 minutes later at 10:54 a.m. Google noticed, that 5,256 source IPs from 132 countries were contributing to the attack [22].

8.5.1.2 The Spamhaus DDoS Attacks in 2013

Another prominent DDoS attack was the one on Spamhaus in 2013. But in this case, the victim was not as lucky as the previous one in the Google Example. Spamhaus is an anti-spam organization, that tracks email spammers and spam-related activities. After Spamhaus added the Dutch hosting provider Cyberbunker (known for hosting a wide-ranging collection of websites and is connected to criminal activities) to its global blacklist, DDoS attacks started against Spamhaus. According to The New York Times, an alleged spokesman for the attackers said that Cyberbunker was retaliating because Spamhaus

had abused its influence on the Internet [23]. Spamhaus had DDoS protection services already in place and was used for DDoS attacks, nevertheless, this attack, estimated at 300 gigabits of traffic per second was successful for the attackers. The attack knocked down the websites and part of the email services of Spamhaus offline. The consequences were immense brand damage [24].

8.5.2 Impacts of DDoS Attacks

As described in the last use case, one impact on the victims of DDoS attacks can be damage on the company's reputation and customer confidence in the company. This is even worse if the company has a large portion of its business online. Another impact can be a huge loss in revenue due to non-operable e-services [13]. A DDoS attack can cost a company, on average, between $20,000- $40,000 per hour. Kaspersky reported, that large companies even lose $417,000 on average due to a DoS attack, small and mid-sized businesses around $53,000 [25]. Thereby, the technology and telecommunications companies are the most targeted ones, as Figure 8.10 shows [26].

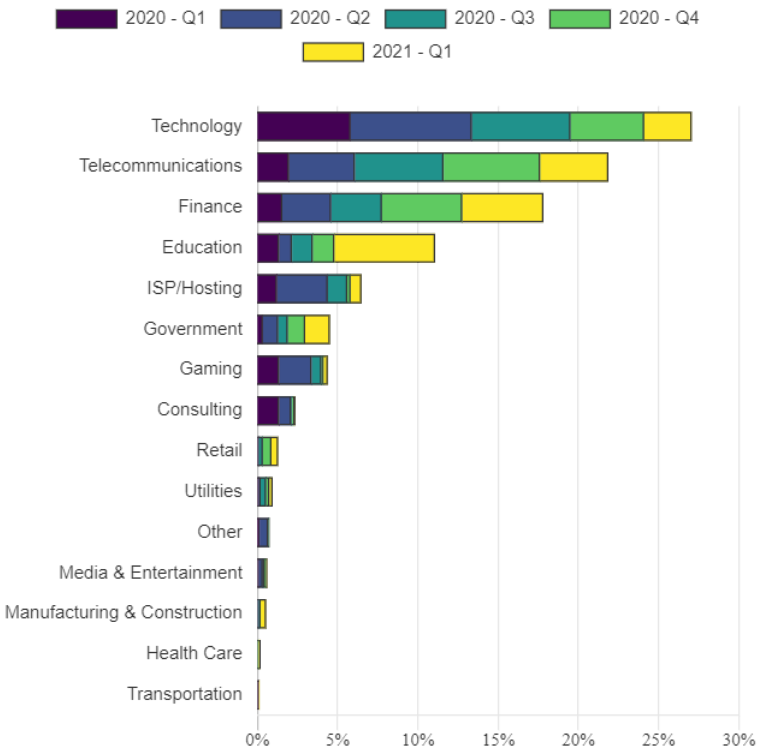

Figure 8.10: DDoS attacks by industry sector 2020-2021 [26]

DDoS attacks do not only slow down networks and prevent website access or availability, but they can also cause costs for restoring the services to employees or customers. Since DDoS attacks are becoming more powerful and taking longer to resolve, most businesses must manage without the target service for at least a workday. This leads to additional costs for offline or backup systems to continue operations during an attack. It can also happen that the attackers use DDoS attacks as a smokescreen for more dangerous cyber-attacks. Attackers can overwhelm a business's servers with decoy traffic from a DDoS attack and then steal data during the distraction [27]. An attack can result in losses of intellectual property, personal data of customers or financial information [28].

Companies must buy products from protection providers to prevent those impacts from a DDoS attack. But those products are not cheap. As an example, DataDome sells their cheapest DDoS protection for $2,990 per month [29], and Azure for $2,944 [30]. For tech companies that offer DDoS protection, the high cost of a DDoS attack on one of their clients can result in the clients filing a cyber liability lawsuit against the companies. If the clients can prove that the tech company could have prevented the attack, it can even result in high costs for the tech company [27].

8.5.3 Discussion

With the adoption of Software-as-a-Service (SaaS) in the form of DDoS-for-hire for executing DDoS attacks, attackers can use user-friendly and freely available attack tools. This leads to an immense reduction of boundaries that attackers have for executing DDoS attacks with no technical knowledge required and low execution costs. Since renting a DDoS-for-hire also enables the attacker to attack multiple targets, the attacker can profit from paying once for a limited amount of time and executing as many attacks as possible within the rented timeframe. If the attacker attacks multiple companies, he/she could profit from extorting money from multiple victims and maximizing his own profit. Therefore, the attractiveness of using a DDoS-for-hire service increases. This, and the insidious advertisement of DDoS-for-hire as a "stress test" could lead to an increase in DDoS attacks in the future.
The constant evolution of DDoS attacks requires a constant adaption of protection against DDoS attacks. Whenever new tactics or technologies are used from the attacker side, the defender side has to keep up, which results in an endless cat-and-mouse game. Anyway, the victims lose, because either they have to risk a DDoS attack or they have to buy protection against DDoS attacks. The costs for the victims rise in both scenarios.

8.6 Conclusion

The stated objective of providing an overview of pulse-wave DDoS attacks and their impacts has been achieved. The report provides an overview so readers with no prior knowledge about this topic get informed about the most important aspects. To provide an overview, various sources had to be considered and elaborated. There were cases, where more research was necessary to find numbers related to specific use cases or scenarios since not every company provides full transparency. The scope defined in the project phase could be reached by providing information about pulse-wave DDoS (technical perspective) and their impacts (economic perspective). The schedule could be fulfilled since enough time for the report creation was provided.
DDoS attacks are constantly increasing in quantity and complexity as the literature research showed. The results are new dangerous DDoS attack types like the pulse-wave DDoS attack. The impacts that DDoS attacks are causing can be horrific for their victims, and this increases the need to create awareness and adopt defense against them. On one side, the costs for companies increase to defend against DDoS attacks because of their increasing complexity of them. On the other side, the costs for the attackers are constantly decreasing as attackers are benefiting from the use of Software as a Service for the execution of DDoS attacks. In this context, future research should focus on dealing with DDoS attacks and reducing the impact as much as possible for the victims.

Bibliography

[1] Subburaj Thangavel, Suthendran Kannan: *Bit-and-Piece DDoS attack Detection based on the Statistical Metrics*; International Journal of Engineering and Advanced Technology (IJEAT), Vol. 9, No. 1S4, December 2019, 48-55, https://doi.org/10.35940/ijeat.A1086.1291S419.

[2] Albert Gran Alcoz, Martin Strohmeier, Vincent Lenders, Laurent Vanbever: *Aggregate-based congestion control for pulse-wave DDoS defense*; In Proceedings of the ACM SIGCOMM 2022 Conference (SIGCOMM '22), August 2022, 693-706, https://doi.org/10.1145/3544216.3544263.

[3] DataDome: *Understanding Botnet for Hire Services: DDoS Booter, Stressers, & Other Terminology*; https://datadome.co/learning-center/what-is-ddos-booter-botnet-booter/, November 2022.

[4] Maryam Feily, Alireza Sharestani, Sureswaran Ramadass: *A Survey of Botnet and Botnet Detection*; In Proceedings of the 2009 Third International Conference on Emerging Security Information, Systems and Technologies, June 2009, 268-273, https://doi.org/10.1109/SECURWARE.2009.48.

[5] DataDome: *How to stop and prevent botnet attacks on your website and server*; https://datadome.co/learning-center/how-to-stop-and-prevent-botnet-attacks-on-your-website-and-server/, November 2022.

[6] Nazrul Hoque, Dhruba K. Bhattacharyya, Jugal K. Kalita: *Botnet in DDoS Attacks: Trends and Challenges*; IEEE Communications Surveys & Tutorials, Vol. 17, No. 4, July 2015, 2242-2270, https://doi.org/10.1109/COMST.2015.2457491.

[7] Shun-Chieh Lin, Shian-Shyong Tseng: *Constructing detection knowledge for DDoS intrusion tolerance*; Expert Systems with Applications, Vol. 27, No. 3, October 2004, 379-390, https://doi.org/10.1016/j.eswa.2004.05.016.

[8] Keunsoo Lee, Juhyun Kim, Ki Hoon Kwon, Younggoo Han, Sehun Kim: *DDoS attack detection method using cluster analysis*; Expert Systems with Applications, Vol. 34, No. 3, April 2008, 1659-1665, https://doi.org/10.1016/j.eswa.2007.01.040.

[9] Igal Zeifman: *Attackers Use DDoS Pulses to Pin Down Multiple Targets*; https://www.imperva.com/blog/pulse-wave-ddos-pins-down-multiple-targets/, November 2022.

[10] An Wang, Wentao Chang, Songqing Chen, Aziz Mohaisen: *Delving Into Internet DDoS Attacks by Botnets: Characterization and Analysis*; IEEE/ACM Transactions on Networking, Vol. 26, No. 6, December 2018, 2843-2855, https://doi.org/10.1109/TNET.2018.2874896.

[11] DDoS-Guard: *Hidden threat of Pulse Wave DDoS attacks*; https://ddos-guard.net/en/info/blog-detail/hidden-threat-of-pulse-wave-ddos-attacks, November 2022.

[12] Ilya V. Chugunkov, Leonid O. Federov, Bela Sh. Achmiz, Zarina R. Sayfullina: *Development of the algorithm for protection against DDoS-attacks of type pulse wave*; In Proceedings of the 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), January 2018, 292-294, https://doi.org/10.1109/EIConRus.2018.8317090.

[13] Swisscom: *DDoS Protection Service*; White Paper, may 2020, 18, https://documents.swisscom.com/product/1000098-IP-Plus_Business_Internet/Documents/Whitepaper/BIS_IPP_WP_DDoS_mm03104-en.pdf, November 2022

[14] M. Mantere: *Stock Market Manipulation Using Cyberattacks Together with Misinformation Disseminated through Social Media*; In Proceedings of the 2013 International Conference on Social Computing, September 2013, 950-954, https://doi.org/10.1109/SocialCom.2013.149.

[15] Netscout: *NETSCOUT THREAT INTELLIGENCE REPORT*; White Paper, No. 4, 2020, 40, https://www.netscout.com/sites/default/files/2020-02/SECR_001_EN-2001_Web.pdf, November 2022.

[16] Natalija Vlajic, Daiwei Zhou: *IoT as a Land of Opportunity for DDoS Hackers*; Computer, Vol. 51, No. 7, July 2018, 26-34, https://doi.org/10.1109/MC.2018.3011046.

[17] Sean Newman: *Bursts, Waves and DDoS: What You Need to Know*; https://www.corero.com/blog/bursts-waves-and-ddos-what-you-need-to-know/, November 2022.

[18] Imperva: *Booters, Stressers and DDoSers*; https://www.imperva.com/learn/ddos/booters-stressers-ddosers/, November 2022.

[19] Ghada Amer, Ehab Hany Abdelhay, Ibrahim Abdel-Baset, Mohamed Abdel-Azim Mohamed: *Development Machine Learning Techniques to Enhance Cyber Security Algorithms*; MANSOURA ENGINEERING JOURNAL (MEJ), Vol. 46, No. 4, DECEMBER 2021, 36-46, https://doi.org/10.21608/bfemu.2021.206401.

[20] Omer Yoachimik: *DDoS attack trends for 2022 Q2*; https://blog.cloudflare.com/ddos-attack-trends-for-2022-q2/, November 2022.

[21] Future Market Insights: *DDoS Protection Market Outlook (2022-2032)*; https://www.futuremarketinsights.com/reports/ddos-protection-market, November 2022.

[22] Google Cloud: *How Google Cloud blocked the largest Layer 7 DDoS attack at 46 million rps*; https://cloud.google.com/blog/products/identity-security/how-google-cloud-blocked-largest-layer-7-ddos-attack-at-46-million-rps?hl=en, November 2022.

[23] Jaikumar Vijayan: *Update: Spamhaus hit by biggest-ever DDoS attacks*; https://www.computerworld.com/article/2495967/update--spamhaus-hit-by-biggest-ever-ddos-attacks.html, November 2022.

[24] Paul Nicholson: *Five Most Famous DDoS Attacks and Then Some*; https://www.a10networks.com/blog/5-most-famous-ddos-attacks/, November 2022.

[25] Nick Galov: *39 Jaw-Dropping DDoS Statistics to Keep in Mind for 2022*; https://webtribunal.net/blog/ddos-statistics/#gref, November 2022.

[26] David Warburton, Edgar Ojeda: *DDoS Attack Trends for 2020*; https://www.f5.com/labs/articles/threat-intelligence/ddos-attack-trends-for-2020, November 2022.

[27] TechInsurance: *How much will a DDoS attack cost your small business?*; https://www.techinsurance.com/resources/ddos-small-business-costs, November 2022.

[28] Vladimir Galyaev, Evgenia Zykova, Dimitry Repin, Denis Bokov: *Recent Trends in Development of DDoS Attacks and Protection Systems Against Them*; International Journal of Network Security, Vol. 21, No. 4, July 2019, 635-647, https://doi.org/10.6633/IJNS.201907_21(4).13.

[29] DataDome: *Pricing Plans*; https://datadome.co/pricing/, November 2022.

[30] Azure: *Azure DDoS Protection pricing*; https://azure.microsoft.com/en-gb/pricing/details/ddos-protection/, November 2022.

Chapter 9

How does Public Trust Affect the Economic Value of IoT Products

Tram Vo

The COVID-19 pandemic gave a rise to adoption for a lot of IoT products as more people demanded digital solutions for connectivity. The multi-billion dollar market for Internet of Things continues to grow as more industries and households begin to adopt these technologies into normal life. As IoT products advance, the public's incident anxiety increases due to lack of knowledge for how their data is being collected and used by these devices. This paper investigates the relationship of consumer trust and IoT products by diving deeper into the privacy concerns many of the IoT product categories display. We will be analyzing consumer's attitudes toward IoT devices and also review public policy and economic implications regarding the privacy concerns for IoT products.

Contents

9.1 Introduction: IoT Products and their Rising Popularity 87
9.2 Exploring Consumer Attitudes and Privacy Implications regarding IoT Products 88
9.3 Product Case Study: Air Tag 89
9.4 Product Case Study: Smart Home Devices 90
9.4.1 Smart TV and Privacy Concerns 91
9.4.2 Voice Assistants and Privacy Concerns 92
9.5 IoT in Healthcare 94
9.6 Economic Value of IoT Products 95
9.6.1 The Influence of Public Perception and Trust 95
9.7 Conclusions and Summary 95

9.1 Introduction: IoT Products and their Rising Popularity

What is IoT? Though there can be a variety of definitions depending on different contexts, according to Insider Intelligence, the ecosystem of Internet of Things products encompass a wide variety of internet-connected devices that enable business, governments and consumers to be connected to carry out a variety of functions [27]. As advancements continue in the future, many more devices will be introduced and added to the IoT list. Computer Scientist Kevin Ashton was the person who coined the term 'Internet of Things' in 1999. The first application of IoT was when he worked at Procter and Gamble and proposed putting radio-frequency identification (RFID) chips to track products through a supply chain. Two decades later, IoT has come quite far.
McKinsey's report 'The Internet of Things: Catching up to an accelerating opportunity'[26] mentioned that IoT is a fundamental growing trend underlying the digital transformation of business and the economy. Digital transformation is at the forefront of many businesses now more than ever before. It is estimated that by 2030, the economic potential IoT could unlock would be around '5.5 trillion to 12.6 trillion dollars in value globally, including the value captured by consumers and customers of IoT products and services.[26]' To paint a picture of how the physical and digital world today are increasingly merging, Insider Intelligence predicts that by 2026, there will be more than 64 billion IoT devices installed around the world [27]. This means that consumers and companies will be spending a lot more on these IoT solutions and systems - creating immense economic value. Many of the world's biggest corporations are responsible for innovation within the field of information and communication technologies.
There are technical requirements for the concept of the Internet of Things. The concept of IoT can be represented as a equation below[31]:

$$IOT = A.\ (Sensing)\ + B.\ (Communication)\ +\ C.\ (Computation) \quad (1)$$

Figure 9.1: Taken from reference[31]

Essentially, the 3 main components of IoT are sensing, communication and computation. For each of these components, they can be broken down further into IoT technologies that are representing each of the component, pictured below[31]:

IOT Components			
Basic Components		Detailed Component	
Symbol	*Name*	*Name*	*Examples*
A	**Sensing**	MICRO-SENSORS	Pressure, air quality, Temperature
		TAGS	RFID, NFC, Quick Response codes (QR)
B	**Communication**	ENERGY EFFICIENT COMMUNICATION	Personal Area network (PAN), Bluetooth, ZigBee
		MICRO-COMPUTING	Micro multi-core chips, Raspberry Pi, Intel
C	**Computation**	CLOUD COMPUTING	Little or no local computing (SAAS,etc)
		OPEN/ SMALL OPERATING SYSTEMS	Linux

Figure 9.2: Taken from reference[31]

It is important to point out that IoT refers to wireless network between objects, like a network of networks, and usually the network will be self-configuring[31]. It allows anything to connect any time at any place either human to human (H2H) or human to things (H2T) or things to things (T2T) [31].

Items	Benefits	Example
1	Dynamic control of industry and daily life	Energy conservation
2	Improve the resource utilization ratio	Resource efficiency
3	Better relationship between human and nature	Pollution and disaster avoidance
4	Forming an intellectual entity	Integrating human society and physical systems
5	Reduce Costs	Consumers Government
6	Improve Efficiency	
7	Create Innovative Products	
8	New Revenue Streams	Business

Figure 9.3: Taken from reference[31]

The below table details the various benefits IoT presents to society, showing the many applications of IoT touching all sectors within society.

9.2 Exploring Consumer Attitudes and Privacy Implications regarding IoT Products

As the world heads towards 64 billion IoT devices by 2025, along with the great benefits for productivity and connectivity, comes higher risk of privacy issues. According to Insider Intelligence, IoT privacy issues can be broken down to a few main causes. Firstly, the issue of too much data. An IoT report from the Federal Trade Commission on Privacy and Security in the Connected World found that fewer than 10,000 households can generate 150 million discrete data points every day. These entry points can put the consumer‘s information at a vulnerable state to hackers [29].
The increasing amount of data being produced by devices means that IoT devices are also collecting a higher quantity of granular data from individuals. The UNESCO Inclusive Policy Lab ‘Data Privacy and the Internet of Things‘ article brings up the concept of ’surveillance capitalism‘, something companies have enabled for the goal of ‘predicting and modifying human behavior as a means to produce revenue and market control [30]‘. Surveillance capitalism can be taken advantage of by companies when it comes to merger and acquisitions and corporate bankruptcy proceedings, where personal data may be disclosed and transferred to other entities. Despite consumers often having to review and accept privacy policies for IoT devices and services, there are still risks of personal identifiable data being disclosed to other third parties[30].
At present, in the United States, there is no comprehensive federal privacy legislation. Different industries are governed by certain regulatory bodies and therefore, there is room for regulatory gaps. Different U.S states have more active data privacy regulations. According to the National Conference of State Legislatures, California, Colorado, Connecticut, Utah and Virginia are five states that have enacted comprehensive consumer data privacy laws [1]. Consumers in California have more rights and can decide whether or not companies are able to sell their individual data to third parties [16]. Nevertheless, policy regarding protection for cybersecurity and data privacy protection varies in many different locations and can be tricky to implement. New York is an example of a state that failed to pass their legislature for the ‘New York Privacy Act‘ due to conflicts with the business community through stringent regulations on data privacy and cybersecurity concerns - leaving companies vulnerable to consumer lawsuits for data breaches for example.
The European Union, on the other hand, put into effect the ‘toughest privacy and security law in the world‘ in May 2018 [2]. The General Data Protection Regulation (GDPR) even includes entities outside of the EU, if they process personal data or offer goods and services to EU citizens or residents [2]. The GDPR includes terms on personal data, data processing, data subject, data controller and the data processor with the main data protection principles focusing on lawfulness-fairness-transparency, purpose limitation, data minimization, data accuracy, storage limitation, integrity and confidentiality, and lastly accountability [2].

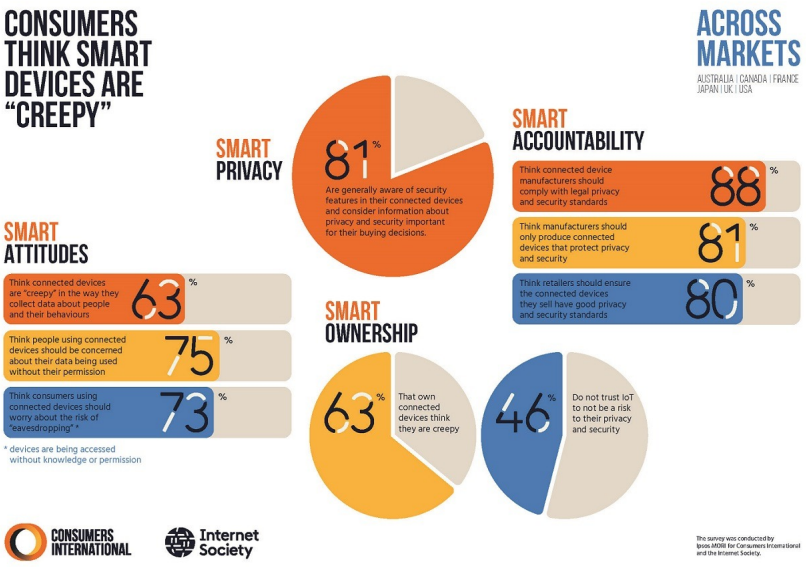

Figure 9.4: Taken from reference [3]

Consumers International and the Internet Society conducted research in 2019 that explored consumer perceptions and attitudes toward trust, security and privacy of IoT devices[3]. It is found that 'On average, 65 percent of consumers across all markets report being concerned with the way connected devices collect and use personal data, with the US showing the highest concern levels at 70 percent [3]'. The research pointed out how consumers' concerns differ depending on the form of technology. Mobile apps had the highest levels of concern about collection of personal data, and lowest was for laptops and tablets. Other insightful findings include how only 50 percent of consumers are aware of settings that control what data is collected and who it is shared with. It is good to preface that the concept of consumer trust can be hard to define based on the individual's background and cultures [3]. Nevertheless, Consumers International and the Internet Society's research found that 63 percent of people agree that connected devices are 'creepy' in the way they collect data [3]. Distrust in IoT devices is high in consumers, as 'Across markets, over half of people tend to distrust their connected devices to protect their privacy and handle their information in a respectful manner (53 percent) [3]'. These survey findings provide some understanding into consumers from different areas of the world, and presents an opportunity for players within the IoT field such as companies, computer scientists, manufacturers and others to realize the importance of security and privacy for their business.

9.3 Product Case Study: Air Tag

Apple released the AirTag in 2021, a tracking device designed for people to find their personal objects such as keys, wallet, luggage, bags and more. Unlike phones and GPS devices, AirTags use bluetooth wireless signals and report their nearby presence to devices connected to the Internet [21]. Since its release, numerous accounts of AirTag and unwanted tracking have arisen. These inexpensive trackers are priced at 30 dollars with removable batteries and small size makes it convenient to clip to objects for many users but also brings possibilities of hiding and misusage [21]. Stalking reports continued to increase, where the company even released an Apple Statement in February 2022 titled 'An update on AirTag and unwanted tracking', which mentions the many ways the company plans to update the AirTag safety warnings and working with law enforcement groups

[19]. This statement was a response to individuals who have been receiving unwanted tracking alerts and reports of malicious attempts of people misusing the AirTag[19].
Many examples of people stalking incidents have happened. BBC News spoke to 6 women who reported they have been tracked using Apple AirTags in the U.S. One pointed out a loophole in Apple AirTag safeguards - where the perpetrator who tracked the woman tracked the woman all the way until she got home and turned off the AirTag after - making her unable to locate the AirTag [20]. This is from the safeguard feature where the AirTag will make a beeping sound 8-24 hours after a device is detected moving with an unregistered phone, but it's also easy to register then disable an AirTag. Many also say that the 'beeping' - a 60 decibel beep, is very easy to muffle, and many complain that the time it takes for the noise to go off is too late [20]. Similar complaint about the AirTag alarm was said from an experiment done by The Washington Post where the sound was described as a 'light chirping' that lasted for 15 seconds and rang after three days. The sound also went silent for several hours and then started chirping again for 15 seconds. The Washington Post experiment pointed out the risk of abusers gaming the alarm countdown timing, and abusers can also turn off the item safety alerts in the Find My app as adjusting these settings require no PIN or password [21]. Many users want the ability for the Find My app to instantly scan the vicinity for any AirTags to make sure of their safety [21].
Tracking devices are not unique to the AirTag. In fact these tracking devices are widely available and made by other producers, and Apple is actually taking action to improve the security of AirTags, whereas tracking-device competitors like Tile have done nothing [21]. The problem comes to the widely used Find My network that uses a billion Apple devices around the world and their bluetooth connectivity. The Find My network is free with all Iphones and allows for significant precision, and with newer Iphone models, contains a wireless technology called ultra-wideband that makes them even more precise [21]. The Apple AirTag spotlight regarding danger is due to its accuracy in long-range tracking[22]. Every AirTag has a unique serial number and paired AirTags are associated with an Apple ID [19], and Apple plans to provide paired account details to law enforcement when tracing back perpetrators.
The lack of trust in Apple AirTag has led to many asking the company to stop producing the product, which is a direct effect on the economic value of an IoT product. In 2021 when the product was released, a professional industry analyst from Forbes had estimated that the AirTag would be Apple's next 1 billion dollar business. This estimation was from the widely used Find My network that includes 1 billion devices, making it conceivable for the company to make 1 billion in revenue if they sell 35 million units [22]. According to Apple Insider and analyst Ming-Chi Kuo, Apple sold 20 million in 2021 and is on course to sell 35 million in 2022 [23]. For a product with such success and potential for growth, it's clear how important it is that the company takes action to combat user security and privacy concerns as user trust and safety can greatly affect the economic value of the product.

9.4 Product Case Study: Smart Home Devices

Smart home technology continues to gain prevalence in modern day homes. The COVID-19 pandemic accelerated this growth as people spent more time indoors, leading to more adoption of digital technologies[4]. A GlobalData forecast predicts the home automation market will expand to 75.3 billion by 2025. This compound annual growth is up by 16 percent by 2020's 35.9 billion [11].
What do consumers want from smart home adoption? It would be to have an integrated system to make their life more connected and capable of delivering personalized

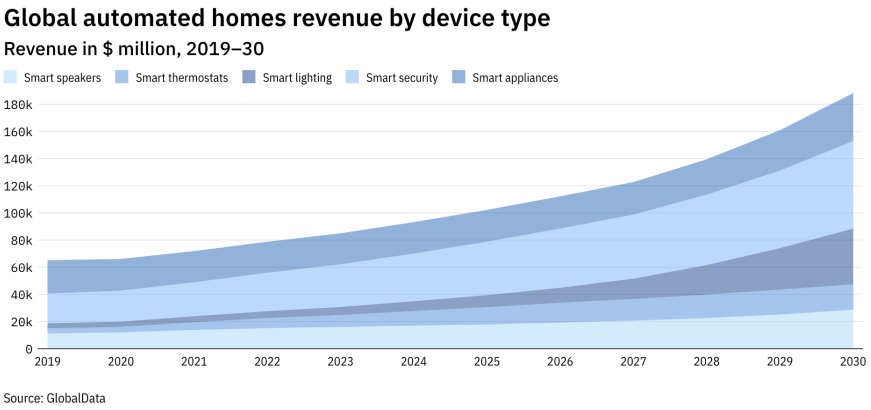

Figure 9.5: Taken from reference[11]

experiences[11]. The goal of this system integration should be to provide enhanced entertainment services, easier management of domestic chores and protection from domestic risks, including flood, burglary and fire, and to lower energy consumption [7].
The downside of many smart home devices currently is their overreliance on the cloud to process data. Cloud connectivity can be concerning as consumer‘s information is being constantly recorded and transferred online. Many smart home devices have sensors that continuously monitor consumer‘s behavior without the consumer‘s full awareness, for example - voice assistants.
Findings from a nationally representative survey of UK consumers show that people tend to agree with the statement that unauthorized data collection will influence their willingness to use smart home devices Unauthorized data collection, therefore, is a big part when defining consumer trust. It‘s also found that older people are less willing to use smart home devices in case of unauthorized data collection than younger people. Higher age and higher education are factors that can make people less likely to trust the integrity of businesses providing smart home devices[7]. Data collection security and transparency can be a point of opportunity for businesses wanting to improve the barrier to consumer adoption process for integrated smart home technologies.

9.4.1 Smart TV and Privacy Concerns

The Smart TV has become one of the most common smart home technologies with the rise in popularity of streaming services [5]. Smart TVs also facilitate content that require internet access - such as games, browsing the web, and entertainment. There are a variety of privacy risks consumers are usually not aware of by the Smart TV ecosystem. There is the risk of vendors and broadcasters collecting Smart TV usage-related data, recording and analyzing speech and sharing that to third party services to extract commands for operating the TV. Compared to smartphones and desktop computers, Smart TVs are said to be less reliably secured [3]. Consumers are to make a decision on compromising their privacy for the functionalities the Smart TV offers.
We can look at an example of the Android TV Ecosystem developed by Google on top of Android OS. Developers of TV apps, similar to mobile apps, run on a sandbox with minimum permissions by default. These TV apps use third party libraries to add services or functions to their app similar to on mobile - these services include analytics, advertising, social networks, and more [5]. These third party libraries can collect sensitive user data and sometimes even the developers are unaware of these data collection methods - putting their users privacy at risk. Third parties collection of personal identifiable information such as viewing history can be used for user profiling. In one study up to 70 percent of Smart TV users find advertisers having access to their viewing history unacceptable

[5]. Additionally, developers can add malicious code or malware exploiting consumer‘s vulnerability in TV apps. Bad development practices can request more permissions from the user than they need, present incomplete or false information in signing certificates, expose the Smart TVs to more bugs and vulnerabilities, and also introduce privilege escalation attacks on the consumer [5].
There have also been numerous other privacy incidents that have happened in the past with Smart TVs. In 2015, Samsung was accused by the Electronic Privacy Information Center(Epic) of breaking federal privacy laws concerning the collection and disclosure of electronic communications. Consumers and Epic who found out about how their private communications were being recorded by the voice recognition feature and transmitted over the internet to a third party, thought that this was an intrusive surveillance activity, was unfair and deceptive [12]. Epic stated in its complaint that everything the user says in front of the Samsung SmartTV is recorded when the voice recognition feature is enabled and it was found that its smart TVs were transmitting voice data and recognized text unencrypted across the internet. This was after Samsung had claimed that ‘all private data is encrypted when passed between the TV to the voice recognition servers‘[14].
That was in 2015, and now in September of 2022, Samsung recently disclosed to their US consumers of a recent data breach which compromised name, personal demographics data and product registration information. This data includes serial numbers for devices like Smart TVs. The company had disclosed this breach a month after discovering it. Breaching this type of data can expose their customers to potential incidents of phishing or unwarranted advertisement.
Lack of encryption and transmitting information onto the internet puts customers in a position that is vulnerable to hackers to spy on them through microphones or cameras [24]. This can be a challenge as streaming services - which require internet connection, is one of the main usages for Smart TVs. Users can be more aware of ways on how to protect their privacy when using Smart TVs by using a VPN with their streaming device[24]. Users can look more into the privacy terms of their Smart TVs and adjust settings such as disagreeing or turning off permission on data collection, tracking policies or other smart settings [24].

9.4.2 Voice Assistants and Privacy Concerns

Another smart home technology that is experiencing great growth is voice assistants and smart speakers. For the United States, Insider Intelligence predicts 42.1 percent of the population, or 142 million people, will be using a voice assistant[29]. This number will increase to 45.4 percent in 2026 [29]. Users are using voice assistants through their smartphones and also other IoT devices, like their cars or smart home tech [25].
The leading players in the voice assistant market are Google, Apple and Amazon, with their respective popular voice assistants Google Assistant, Apple Siri and Alexa. Insider Intelligence noted that voice assistant users are likely to use more than one type of voice assistant since they are all interoperable across devices. The flexibility of voice assistants being used across platforms and devices shows how these devices are being integrated into many products and people‘s daily lives, functioning as their own ecosystems. One example is Alexa - which is compatible with over 140,000 smart home products [29]. The Voice Interoperability Initiative founded by Amazon has over 90 companies that are committed to giving customers the choice and flexibility to access multiple voice services on a single device [14].
The technical name for smart assistant device is called Voice-Controlled Digital Assistants (VCDAs) and below is the basic structure of how one works:
The ‘wake word‘ is the term for the word that the user would use to activate their smart voice assistant. Large tech companies claim their smart speakers are only listening for the

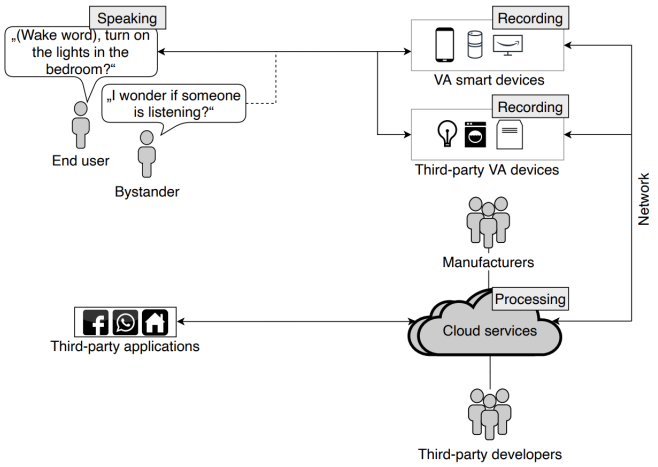

Figure 9.6: Taken from reference[16]

‘wake word‘, but this is not the case as the speakers can mistake certain words and begin the recording without the user knowing [16].
There are two main concerns regarding privacy for users when it comes to voice assistants. The first concern deals with the ‘always-listening‘ feature of VCDAs. The second concern deals with the data collection and processing by manufacturers and or third parties that users are not aware of due to a lack of transparency [15]. There‘s also a term called ‘dolphin attack‘ where inaudible audio signals are picked up and activate the smart speakers without the knowledge of the end users [15]. The collection of audio data can reveal a lot of information about the end user. For example, interests, location, buying behavior, current activities or mood. Other background noises and contexts collected can further develop a better profile of the user. Device manufacturers and third party developers would be able to use this information for sending of targeted advertisements and or profiling [15].
So what power does the end user have right now for using these devices? Currently, end users can manage skills or acting permissions and control sharing of information when using Google Assistant or Alexa. Users can also opt out utilization of their data for additional purposes such as system improvements [15]. Apple Siri for example currently does not allow users to view data or manage skill permissions. One suggested solution when it comes to protecting the user‘s privacy while using VCDAs is local data processing as opposed to cloud processing. Locally processing the data on the device examples include a system called Snips which allow for offline processing of voice commands, but this solution requires crowdsourcing data and semi-supervised machine learning instead of using the user‘s own data. There are other offline, open-source and privacy-friendly voice assistant service platforms out there as well [15]. Another suggested preventative solution is altering/conversion of user voice data before the processing stage by the cloud service. The diagram below shows the VCDA process with this additional sanitization step [15]:
This sanitization process can anonymize the end user‘s voice using a frequency warping process and keyword substitution predefined by the end users. This additional step reduces the risk of third party developers being able to identify end users and infer further on their personal characteristics [15].

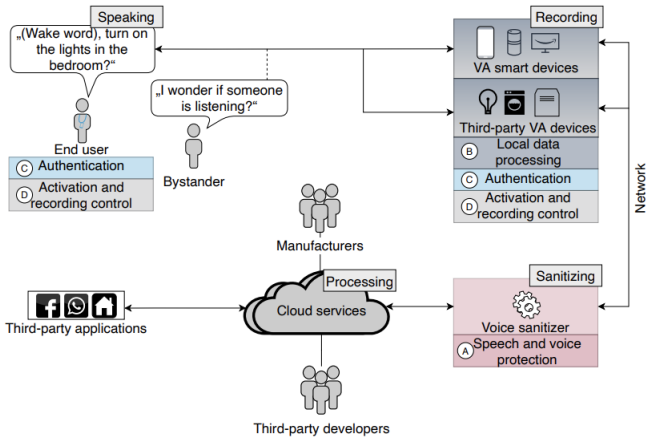

Figure 9.7: Taken from reference[16]

9.5 IoT in Healthcare

According to Market Watch by Deloitte, the global IoT healthcare market is expected to be worth 158.1 billion dollars in 2022 [18]. Another study by Allied Market shows the global Internet of Things in the healthcare market is valued at 11.751 billion in 2019 and is expected to reach 22.2672 billion by 2027. This results in a compound annual growth rate (CAGR) of 13.20 percent from 2020 to 2027. Another statistic in 2019 shows up to 86 percent of healthcare organizations were using IoT technology in some way. It can be assumed that the percentage of healthcare organizations using IoT technology is ever increasing.

Many of these IoT healthcare usage include applications monitoring hardware and other ways to improve the way patients keep track of their health [18]. One example of this type of tracking technology is the Broolyn-based nursing facility Allure introducing EarlySense, a product that is able to track vital signs and movements from sensors placed under mattresses and pillows. According to the Allure Group, their investment in Iot technology showed a 45 percent decrease in patient falls, a 60 percent reduction in bedsores, and an 80 percent decrease in code blue events [18]. Another example is a Bluetooth- and IoT-enabled device that allows patients to monitor how quickly their blood clots - released by Roche in 2016. The device allows self-testing of their blood, sets targets and allows for both the patient and healthcare provider parties to add leave comments on results[18]. Apple Watches also launched a new ‘Movement Disorder API‘ that allows for the monitoring of Parkinson‘s Disease symptoms in 2018. The Apple watch monitors daily, hourly and minute-by-minute breakdowns of symptom fluctuation and produces a graph that gets sent to caregivers. It‘s also said that this technology also has benefits for patients with epilepsy and arthritis [18]. According to one study, 85 percent of doctors confirmed that handheld medical devices encourage devices to take better care of themselves, and 75 percent of patients believe using the technology can help them improve their health [17]. Forbes estimated 646 million IoT devices were used in hospitals, clinics and medical offices in 2020. The large volumes of medical data generated now being managed by IoT means more pressure on security, confidentiality and appropriate storage solutions [18]. A study aiming to examine the impact of trust on the engagement in the use of IoT for healthcare states that in the healthcare context, the use of IoT devices enables better diagnosis and monitoring of patient health [17]. These devices collect user-health data and therefore raise concerns about security and trust that can affect user‘s adoption of this technology. The study explains that patients must be informed by healthcare professionals on how their data will be collected and used, patient data are to be kept for administrative purposes and

confidential patient information should not be revealed. These factors help patients trust IoTs to monitor their health without compromising their privacy [17]. The study finds that autonomy is a factor that helps users feel more engaged with IoT technology. Hence, IoT service providers should work on allowing users the perceived autonomy to make life easier for users. The study also finds that users are more engaged with IoT for health when they perceive that the technology is allowing them to develop their performance. The desire for self-development is also another point providers should pay attention to for the IoT healthcare products to gain the user‘s trust [17]. It‘s also important to note that the user must be aware and be able to give consent for their treatment of health-data. The delegated actions to IoT healthcare devices must be asked by the user and not be misleading, which can impact the user‘s trust and sense of freedom [17].

9.6 Economic Value of IoT Products

According to a CDN Report, the Internet of Things has the potential to generate 4-11 trillion dollars in economic value in 2025. The strongest sector in terms of economic impact is the industrial sector with an expectation of 1.2 and 3.7 billion in contribution, coming from factories. The report predicts the rest IoT‘s the economic impact will be coming from smart cities in Europe, connected healthcare in the Americas, custom production environments and IoT usage in homes and offices around the globe[18]. McKinsey also predicts 40 percent of the value IoT generates will come from developing countries [18].
The use of IoT products continues to increase with Statista predicting the number of IoT devices surpassing 75 billion by the end of 2025. Currently in 2021, there are more than 10 billion active IoT devices [18]. Market Research Engine estimates the consumer IoT Market to reach 142 billion by 2026, with the largest market being in North America and Asia-Pacific being the fastest-growing area [18]. These figures ultimately show the significant impact the Internet of Things has on the economy.

9.6.1 The Influence of Public Perception and Trust

Companies can differentiate themselves by putting privacy and security at their forefront of their products. Even though consumers pay for IoT products, they are also the product themselves [7]. Consumer anxiety of security incidents with IoT products, whether that be smart home devices, tracking devices, or healthcare products serve as a constraint for trust and adoption of IoT.
Policymakers and businesses can work together to address barriers of adoption of IoT products. These barriers are consumer anxiety and lack of data privacy transparency from companies. This means companies should be providing more clarity about usage of consumer data, increase education and resources for risk-related incidents, and overall decrease the risk-likelihood to increase trust in consumers [7]. As the statistics have shown in the previous section, the IoT market is estimated at billions of dollars with more potential for growth as the digital revolution continues to be adopted in every industry and household, so it‘s very important to take action towards increased public trust for IoT technologies.

9.7 Conclusions and Summary

Based on the gathered findings from many sources, Internet of Things technologies have and will continue to grow exponentially, contribute to the global economy, and become a part of society on a business and consumer level. Businesses want to increase adoption for IoT technologies, but with this comes implications regarding privacy, security and

Figure 9.8: Taken from reference[3]

trust from the public. Concerns with surveillance capitalism become more relevant as the hyper-connectivity increases and the ecosystem of IoT products continues to expand, leading to more generation of user data - and hence concerns of data collection, processing, and usage. Consumers have incident anxiety from many IoT products such as smart home devices, tracking devices, healthcare products, and more - which the paper addressed each product area and the privacy risk implications more in depth.

The risks of privacy for individuals become a data ethics issue [9]. It is not enough for legal requirements such as privacy legislation to be the sole player in protecting data privacy rights for the public.

Even the strictest privacy legislation currently in the world, the EU Data Act, can't fully protect the consumer. The problem with IoT Data Governance is difficult because IoT devices generate both personal and non-personal data, but only the personal data are subject to the EU General Data Protection Regulation (GDPR), and for most non-personal data generated by IoT devices, no 'de jure' rights exist [32]. The main problems arise then with the complexities of how data is classified, transferred and used and how those processes align within the current legislation terms. For example, one of the main problems is that it is very difficult to determine ex ante, i.e. before litigation in courts, whether certain data of the data holders are trade secrets. This can lead to the problem that data holders can easily claim, without clarification, that the data that should be shared are trade secrets and require far-reaching confidentiality agreements and technical protection measures [32]. Other various examples also show how personal data and compliance with regulations like the GDPR can lead to many disputes and the data sharing agreements are unclear.

Organizations and businesses should have a more fundamental conversation on what is the core objective they are trying to achieve with IoT and how does that balance against risks with individuals [9]. Behind IoT products are tech teams with scientists, product and risk teams that also have as much impact as data privacy officers and lawyers [9]. Overall, it's undeniable the benefits and economic value IoT brings to society, but also public trust can greatly influence the adoption of these technologies. In the future, technology companies should tailor their value propositions and prioritize increasing consumer trust.

Bibliography

[1] National Conference of State Legislatures, State Laws Related to Digital Privacy, June 7, 2022. https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internetprivacy.aspx#:~:text=Five%20states%E2%80%94California%2C%20Colorado%2C,of%20personal%20information%2C%20among%20others

[2] GDPR.eu, Proton Technologies AG, What is GDPR, the EU's new data protection law? https://gdpr.eu/what-is-gdpr/

[3] Consumers International and the Internet Society, The Trust Opportunity: Exploring Consumer Attitudes to the Internet of Things, May 1, 2019. https://www.internetsociety.org/resources/doc/2019/trust-opportunity-exploring-consumer-attitudes-to-iot/

[4] Mark Lippett, Privacy, Intelligence, Agency: Security In The Smart Home, Forbes Technology Council Post, May 6, 2022 https://www.forbes.com/sites/forbestechcouncil/2022/05/05/privacy-intelligence-agency-security-in-the-smart-home/?sh=1cac6cad4aac

[5] Tileria, Marcos, and Blasco, Jorge, Watch over your TV: A Security and Privacy Analysis of the Android TV ecosystem, Proceedings on Privacy Enhancing Technologies, 2022. https://petsymposium.org/2022/files/papers/issue3/popets-2022-0092.pdf

[6] Guhr, Nadine and Werth, Oliver and Blacha, Philip and Breitner, Michael. (2020). Privacy concerns in the smart home context. SN Applied Sciences. 2. 10.1007/s42452-020-2025-8. https://www.researchgate.net/publication/338743740_Privacy_concerns_in_the_smart_home_context

[7] Cannizzaro S, Procter R, Ma S, Maple C. Trust in the smart home: Findings from a nationally representative survey in the UK. PLoS One. 2020 May 29;15(5):e0231615. doi: 10.1371/journal.pone.0231615. PMID: 32469883; PMCID: PMC7259745. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7259745/

[8] Andrew Meola, Researchers discover multiple vulnerabilities in Samsung's SmartThings platform, Insider, May 3, 2016 https://www.businessinsider.com/samsung-smartthings-platform-iot-security-issues-internet-of-things-2016-5?r=US&IR=T

[9] Dr. Davide Borelli, Ningxin Xie and Eing Kai Timothy Neo, The Internet of Things: Is it just about GDPR?, PwC Insights, December 18, 2018. https://www.pwc.co.uk/services/risk/technology-data-analytics/data-protection/insights/the-internet-of-things-is-it-just-about-gdpr.html

[10] Maalsen, S., and Dowling, R. (2020). Covid-19 and the accelerating smart home. Big Data and Society, 7(2). https://doi.org/10.1177/2053951720938073 https://journals.sagepub.com/doi/pdf/10.1177/2053951720938073

[11] Giacomo Lee, Smart homes: Inside a new fast growing market, set to be worth $75bn by 2025, Private Banker International Thematic Research, August 6, 2021, updated August 9, 2021. https://www.privatebankerinternational.com/uncategorized/smart-home-automation-market-2025/

[12] Samuel Gibbs, Samsung's voice-recording smart TVs breach privacy law, campaigners claim, The Guardian, February 27, 2015. https://www.theguardian.com/technology/2015/feb/27/samsung-voice-recording-smart-tv-breach-privacy-law-campaigners-claim

[13] Ghiglieri, M., Volkamer, M., Renaud, K. (2017). Exploring Consumers' Attitudes of Smart TV Related Privacy Risks. In: Tryfonas, T. (eds) Human Aspects of Information Security, Privacy and Trust. HAS 2017. Lecture Notes in Computer Science(), vol 10292. Springer, Cham. https://doi.org/10.1007/978-3-319-58460-7_45

[14] Molly Killeen, Voice assistants under fire in IoT competition report, Euractiv, Euractiv Media Network BV, January 20, 2022, updated January 26, 2022. https://www.euractiv.com/section/digital/news/voice-assistants-under-fire-in-iot-competition-report/

[15] Luca Hernandez Acosta, Delphine Reinhardt, A survey on privacy issues and solutions for Voice-controlled Digital Assistants, Pervasive and Mobile Computing, Volume 80, 2022, 101523, ISSN 1574-1192. https://doi.org/10.1016/j.pmcj.2021.101523.

[16] Manzoor, Jacob A. (2021) ""Hey Siri, What Does the Government Know About Me?": Increasing the Volume on Smart Speaker Awareness," Hofstra Law Review: Vol. 49: Iss. 3, Article 7. Available at: https://scholarlycommons.law.hofstra.edu/hlr/vol49/iss3/7

[17] Khalid Samhale, The impact of trust in the internet of things for health on user engagement, Digital Business, Volume 2, Issue 1, 2022, 100021, ISSN 2666-9544. https://doi.org/10.1016/j.digbus.2022.100021.

[18] Bojan Jovanovic, Internet of Things statistics for 2022 - Taking Things Apart, Data Prot, May 13, 2022. https://dataprot.net/statistics/iot-statistics/

[19] Apple Statement, An update on AirTag and unwanted tracking, Apple Newsroom, February 10, 2022. https://www.apple.com/newsroom/2022/02/an-update-on-airtag-and-unwanted-tracking/

[20] James Clayton and Jasmin Dyer, Apple AirTags - A perfect tool for stalking, BBC News, January 20, 2022 https://www.bbc.com/news/technology-60004257

[21] Geoffrey A. Fowler, Apple's AirTag trackers made it frighteningly easy to 'stalk' me in a test, The Washington Post, Consumer Tech, May 5, 2021. https://www.washingtonpost.com/technology/2021/05/05/apple-airtags-stalking/

[22] Tim Bajarin, AirTags Are Apple's Next Billion Dollar Business, Forbes, Consumer Tech, April 20, 2021. https://www.forbes.com/sites/timbajarin/2021/04/20/airtags-are-apples-next-billion-dollar-business/?sh=75ec4c6c5d18

[23] Stephen Warwick, AirTags 2 could be on the way if strong sales continue, iMore, Future US Inc., June 20, 2022. https://www.imore.com/airtags-2-could-be-way-if-strong-sales-continue

[24] Proteus Cyber Lcd. , How to Stop Your Smart TV from Spying on You, January 7, 2021. https://proteuscyber.com/privacy-database/news/3231-how-to-stop-your-smart-tv-from-spying-on-you-updated-2021#:~:text=When%20you%20use%20a%20smart,used%20to%20spy%20on%20you.

[25] Jessica Lis, How big is the voice assistant market?, Insider Intelligence, US Voice Assistants and Smart Speakers Forecast 2022, September 16, 2022. https://www.insiderintelligence.com/content/how-big-voice-assistant-market

[26] Michael Chui, Mark Collins, and Mark Patel, The Internet of Things: Catching up to an accelerating opportunity, McKinsey Digital, McKinsey Report, November 9, 2021. https://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/iot%20value%20set%20to%20accelerate%20through%202030%20where%20and%20how%20to%20capture%20it/the-internet-of-things-catching-up-to-an-accelerating-opportunity-final.pdf

[27] Andrew Meola, What is the Internet of Things? What IoT means and how it works, Insider Intelligence, April 15, 2022. https://www.insiderintelligence.com/insights/internet-of-things-definition/

[28] Natalie Merchant ,World Economic Forum, IoT Technologies Explained: History, Examples, Risks and Future, Vision of Humanity, Institute for Economics and Peace, March 31, 2021. https://www.visionofhumanity.org/what-is-the-internet-of-things/#:~:text=The%20term%20'Internet%20of%20Things,them%20through%20a%20supply%20chain

[29] Insider Intelligence, The security and privacy issues that come with the Internet of Things, April 15, 2022. https://www.insiderintelligence.com/insights/iot-security-privacy/

[30] Stacy-Ann Elvy, Data privacy and the Internet of Things, UNESCO Inclusive Policy Lab, UNESCO.org, February 9, 2022. https://en.unesco.org/inclusivepolicylab/analytics/data-privacy-and-internet-things

[31] Awad ElAdl, Gamal. (2017). Technical Requirements for the Application of Internet of Things. https://www.researchgate.net/publication/324538559_Technical_Requirements_for_the_Application_of_Internet_of_Things

[32] Wolfgang Kerber, Governance of IoT Data: Why the EU Data Act Will not Fulfill Its Objectives, GRUR International, 2022;, ikac107, https://doi.org/10.1093/grurint/ikac107