2nd KuVS Fachgespräch "Machine Learning and Networking“, October 8-10, 2020, ~~Würzburg, Germany~~ Virtually

Towards a Conversational Agent for Cybersecurity Planning and Management

Muriel Franco[1], Lisandro Granville[2], Burkhard Stiller[1]
[1]Department of Informatics IfI, Communication Systems Group CSG, University of Zürich UZH
[franco¦stiller]@ifi.uzh.ch
[2]Institute of Informatics INF, Federal University of Rio Grande do Sul UFRGS
granville@inf.ufrgs.br

Universität Zürich[UZH]

Introduction
SecBot Approach
Evaluation
Conclusions and Future Work

CSG Communication Systems Group

ifi

Introduction

Introduction

- Businesses becomes proportionally more exposed to cyberattacks as their reliance on ICT increases
  - Companies investments in cybersecurity naturally should increase

ICT: Information and Communications Technologies

- Small and Medium-sized Enterprises (SMEs) often underinvest and lack efficient cybersecurity strategies
  - Misperception of their cybersecurity conditions
  - Constraints: budget, human resources, and limited time allocated to cybersecurity planning

Motivation

- It is essential to promote novel approaches to:
  - Present cybersecurity technical information in a intuitive and user-friendly way
  - Allow less-skilled personnel to make decisions
  - Enable a faster and cheaper planning and management of a cybersecurity strategy
- Different applications of Machine Learning (ML) are simplifying processes related to the Networking and Cybersecurity field
  - Most used for pattern recognition and anomaly detection

SecBot Approach

SecBot

- A cybersecurity-driven conversational agent to support SMEs and non-expert users
  - Understand symptoms and business risks
  - Recommend actions with different levels of abstraction
  - Configuration for in-house protections
- A Proof-of-Concept implemented using Rasa framework
  - Dual Intent and Entity Transformer (DIET)
  - Conditional Random Fields (CRFs)

Entities

- Specific terms or values extracted from an interaction

Entity	Description	Input's Example
@attack_name	Name of the attack	I am being target of a @DDoS Attack
@attack_type	Type of attack	It looks like a @SYN Flood
@target	Target of the attack or the component with symptoms	It is my @database server
@symptom	Describe specific problems or symptoms	My server is receiving @a lot of requests
@budget	Amount and currency available to invest	My budget is @5000 EUR
@solution, @technology	Describe in-house solutions	I have an @Iptables running on @Ubuntu 16.4
@operator, @object	Describes de users' required action	I want help to @allow @TCP traffic using the UFW firewall

Intents

- Identify the need of the user and predict the correct flow

Intent	Example	Associated Entities
Attack_notification	My Windows systems are under a Ransomware attack	@target, @attack_name
Attack_details	It is a WannaCry attack	@attack_type
Target	The target is my SQL database	@target
Problem_desc	My server is receiving a lot of requests from different Ips	@target, @symptom
Solution_config	I want to block an SYN flood using Iptables	@operator, @attack_type, @solution
ROSI_calc	Should I invest in backups against Ransomware impacts?	@attack_name
Critical_data	I have almost 10 TB of critical data	@cardinal

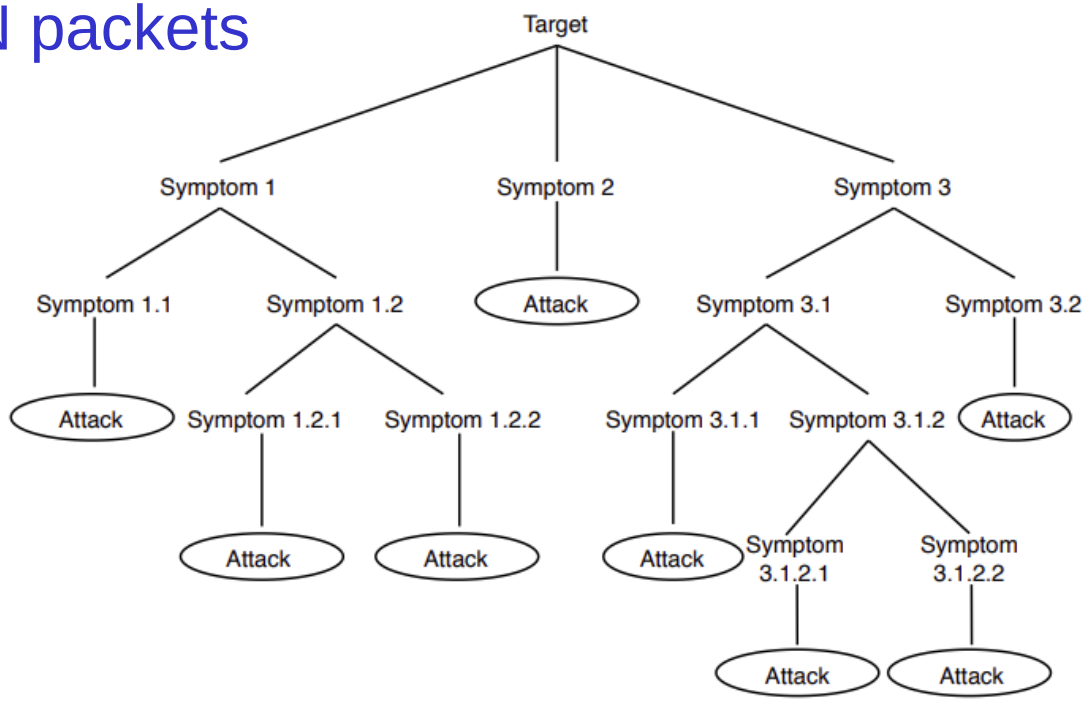
Custom Actions

- Based on the conversation flow and the extracted information, different functions can be called to process that
  - Attack Identification
  - Protection Configuration
  - Economic Analysis

- Python-native support to Custom Actions in Rasa Framework
  - API calls, database queries, machine learning processment

Attack Identification

- Based on symptoms description, the attack can be identified by searching in the attack tree
  - My Server is receiving many requests
  - Many of them are SYN packets



Protection Configuration (1)

```
<input>: "I have an IPtables installed and I want
    to protect my network against ICMP flood"
Entities_Extraction {
    "intent": solution_configuration
    "solution": IPtables
    "operator": protect
    "target": network
    "attack_name": ICMP flood
}
<custom_action>: find_configuration(solution,
    action, target, attack_name)
<output>: "The command for your configuration
    request is: iptables -t mangle -A PREROUTING -
    p icmp -j DROP"
```

Protection Configuration – JSON file (2)

```
{
  "iptables": {
    "version": "1.4.21",
    "OS": "Linux",
  "support":{
    "block": {
  "ports": "iptables -A INPUT -p <protocol> --
      destination-port <port number> -j DROP",
  "ip traffic": "iptables -A INPUT -s <ip> -j DROP
      "
    }
  },
  "protection_config": {
    "syn flood": "iptables -t raw -A PREROUTING -p
        tcp -m tcp --syn -j CT --notrack |
      iptables -A INPUT -p tcp -m tcp -m
      conntrack --ctstate INVALID,UNTRACKED -j
      SYNPROXY --sack-perm --timestamp --wscale
      7 --mss 1460 | iptables -A INPUT -m
      conntrack --ctstate INVALID -j DROP",
    "icmp flood": "iptables -t mangle -A
      PREROUTING -p icmp -j DROP",
    "port scanning": "iptables -N port-scanning |
      iptables -A port-scanning -p tcp --tcp-
      flags SYN,ACK,FIN,RST RST -m limit --limit
       1/s --limit-burst 2 -j RETURN | iptables
      -A port-scanning -j DROP"
  }
 }
}
```

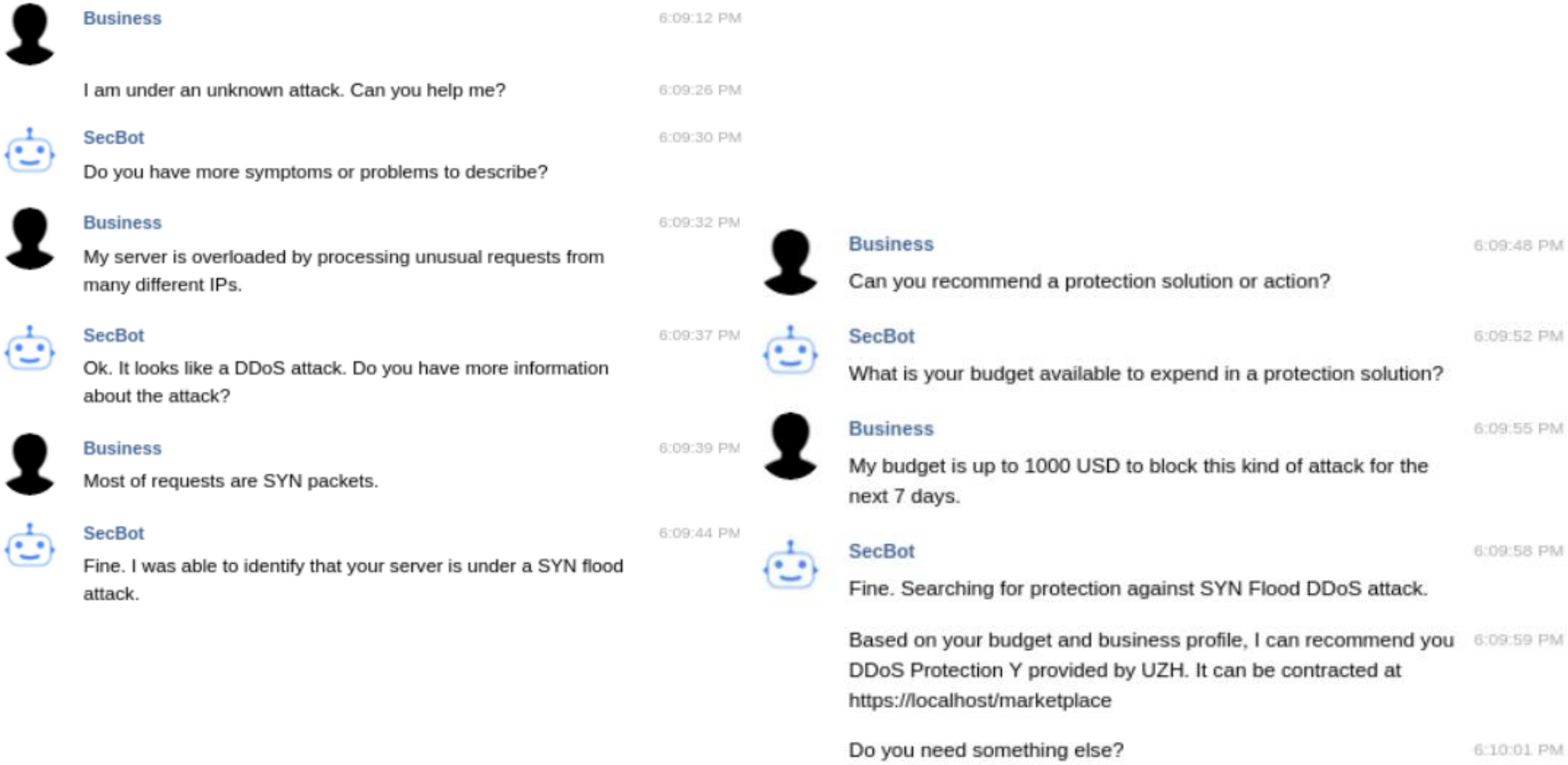
Cybersecurity Investment

- Based on the Return on Security Investment (ROSI) metric
  - Defines if an amount of money is recommended to invest in a cybersecurity protection taking into account the costs related (i.e., direct and indirect costs of a failure)

$$ROSI = \Delta T * \frac{(T_{costs} * RMC) - PMC}{PMC} \qquad (1)$$

Evaluation

Case Study: Reactive



Case Study: Proactive

Business 6:10:04 PM

I want to avoid port scanning in my network from external IPs.

SecBot 6:10:08 PM

Do you have any solution already installed?

Business 6:10:11 PM

Yes, I have an IPtables installed. Can you help me to configure?

SecBot 6:10:14 PM

Yes. I can help you with that. You can use the following command:

"iptables -N port-scanning | iptables -A port-scanning -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit --limit 1/s --limit-burst 2 -j RETURN | iptables -A port-scanning -j DROP" 6:10:16 PM

Business 6:10:22

Fine. Thanks.

In order to finish my planning, do you think should I invest in backups as a proactive approach to reduce possible impacts of a Ransomware attack in my business? 6:10:23

SecBot 6:10:29 PM

I will use the amount of 10 TB of critical data as defined in your business profile.

I will use also your business profile of 9000 per day of revenue and downtime average of 23 days for my calculation. 6:10:30 PM

The Return On Security Investment (ROSI) for your request is equal to 391. 6:10:31 PM

Based on that (ROSI>1), it is recommended you invest on Backups for this case. 6:10:33 PM

Preliminary Evaluation

- Evaluation performed using a Dell XPS desktop
  - Intel Core i7-3770, 3.40 GHz, 32GByte of RAM, running Ubuntu 18.04 LTS 64-bit
- Training: 80 examples from 15 distinct intents, 41 examples from 12 distinct entities (~150 values mapped in the knowledge database)
  - Better datasets and configurations have to be investigated to scale for complex scenarios
- Scalability: One single instance of SecBot can handle 20 messages per second (stress test)
  - Attack identification is the worst case *O(nlogn)*

Conclusions and Future Work

Conclusions

- SecBot combines the description of a formal language with ML and state-of-the-art aspects of cybersecurity
  - It helps to build foundations for long-term cybersecurity strategies
- It shows opportunities to simplify the different steps involved in cybersecurity planning and management
  - Addressing cybersecurity-related information using conversational agents
  - Providing custom actions to address specific requirements

Future Work

- Definition of different scenarios based on real-world use cases
  - Training dataset have to be carefully extended
  - New Intents and Entities
- Feed custom actions with the extracted information
  - Identify types of attacks, risks involved for the business, and estimate possible economic impacts
- Reinforcement learning to improve the accuracy of the SecBot
- Evaluate the performance and usability with real-world users and complex scenarios

Thank you for your attention!

Questions?

franco@ifi.uzh.ch