The Research on IoT Botnet

-- Use Mirai Botnet as an Example

Presentation for the Tentative Structure and References

Internet of Things & Security (Seminar Technische Informatik)

Freie Universität Berlin

Fang Lin

05.05.2021

Outline

1. Introduction and Motivation
2. Tentative Structure
3. References
   1). General
   2). The References I Will Focus on
   3). The References I Will Not Focus on
4. Tentative Schedule

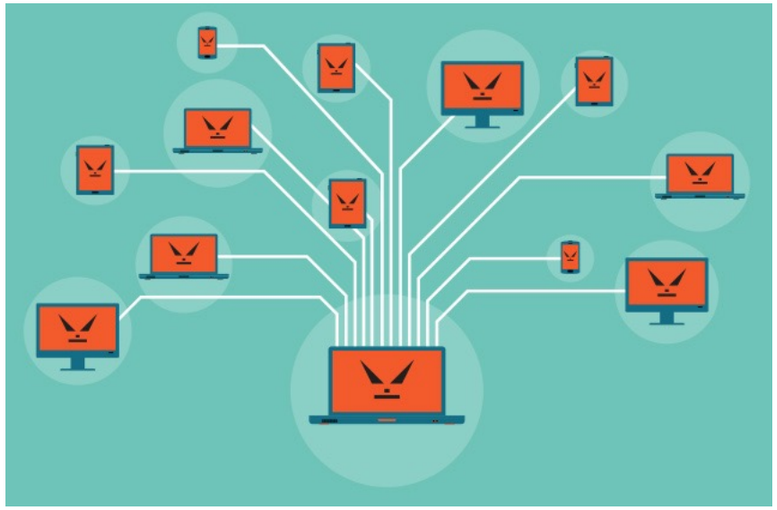
Introduction

The Internet of Things (IoT) is becoming an indispensable part of our daily lives, including health, environment, family, military, etc.

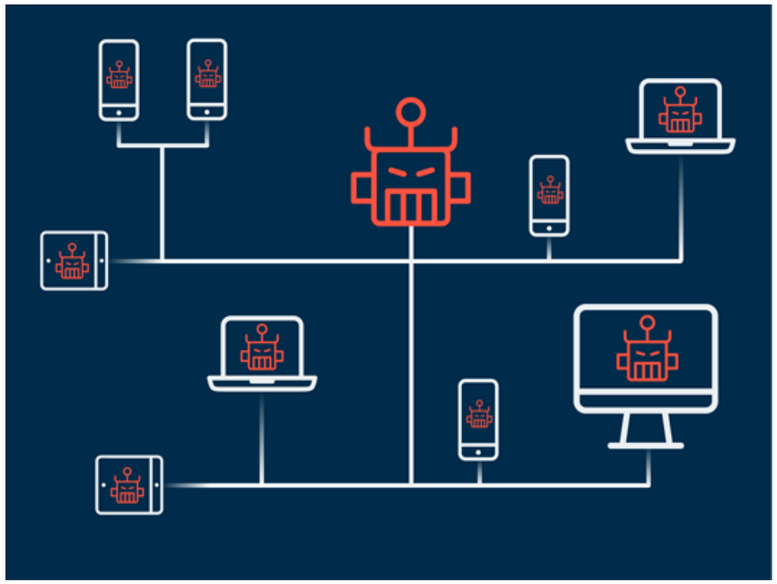
The recent tremendous growth of the Internet of Things for many years has attracted hackers to use their computing and communication advantages to perform different types of attacks.

The main concern is that IoT devices have multiple vulnerabilities. These vulnerabilities can be easily used to form an IoT botnet consisting of millions of IoT devices, posing a major threat to Internet security.

In this case, DDoS attacks originating from the Internet of Things botnet are the current Internet that needs immediate attention.



Source from:
https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.kaspersky.com%2Fblog%2Fbotnet%2F1742%2F&psig=AOvVaw33bsbQAcZXkbCmgVr15Cmv&ust=1620135906225000&source=images&cd=vfe&ved=0CAIQjRxqFwoTCKCWxuPSrfACFQAAAAAdAAAAABAD



Source from:
https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.myrasecurity.com%2Fde%2Fbotnet%2F&psig=AOvVaw33bsbQAcZXkbCmgVr15Cmv&ust=1620135906225000&source=images&cd=vfe&ved=0CAIQjRxqFwoTCKCWxuPSrfACFQAAAAAdAAAAABAJ

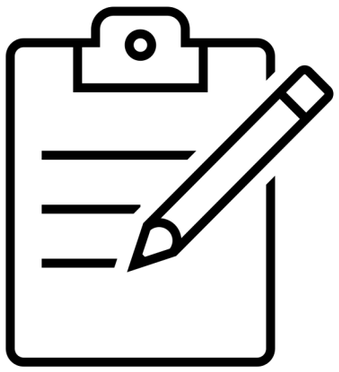
Motivation

Since botnets are so harmful to IoT devices, it is worth studying to understand it and study how to prevent it.

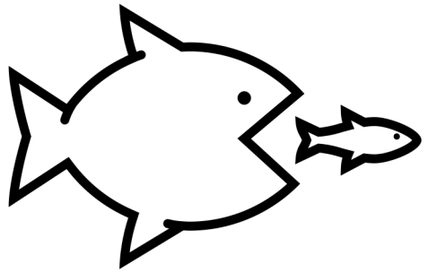
First understand the concept of botnets, understand some forms of botnets, and focus on studying one of them (I use Mirai Boenet as the main example) , to understand how it evolves, how it attacks DDoS, and how it paralyzes IoT devices.

After having a further understanding of botnets, we must understand and analyze how to effectively detect and prevent botnets.

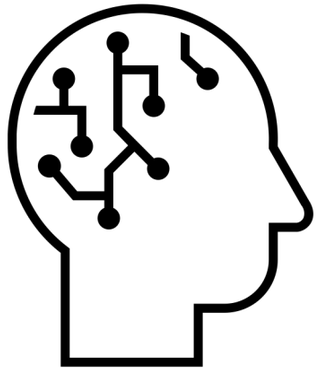
What is it?



How it attacks?

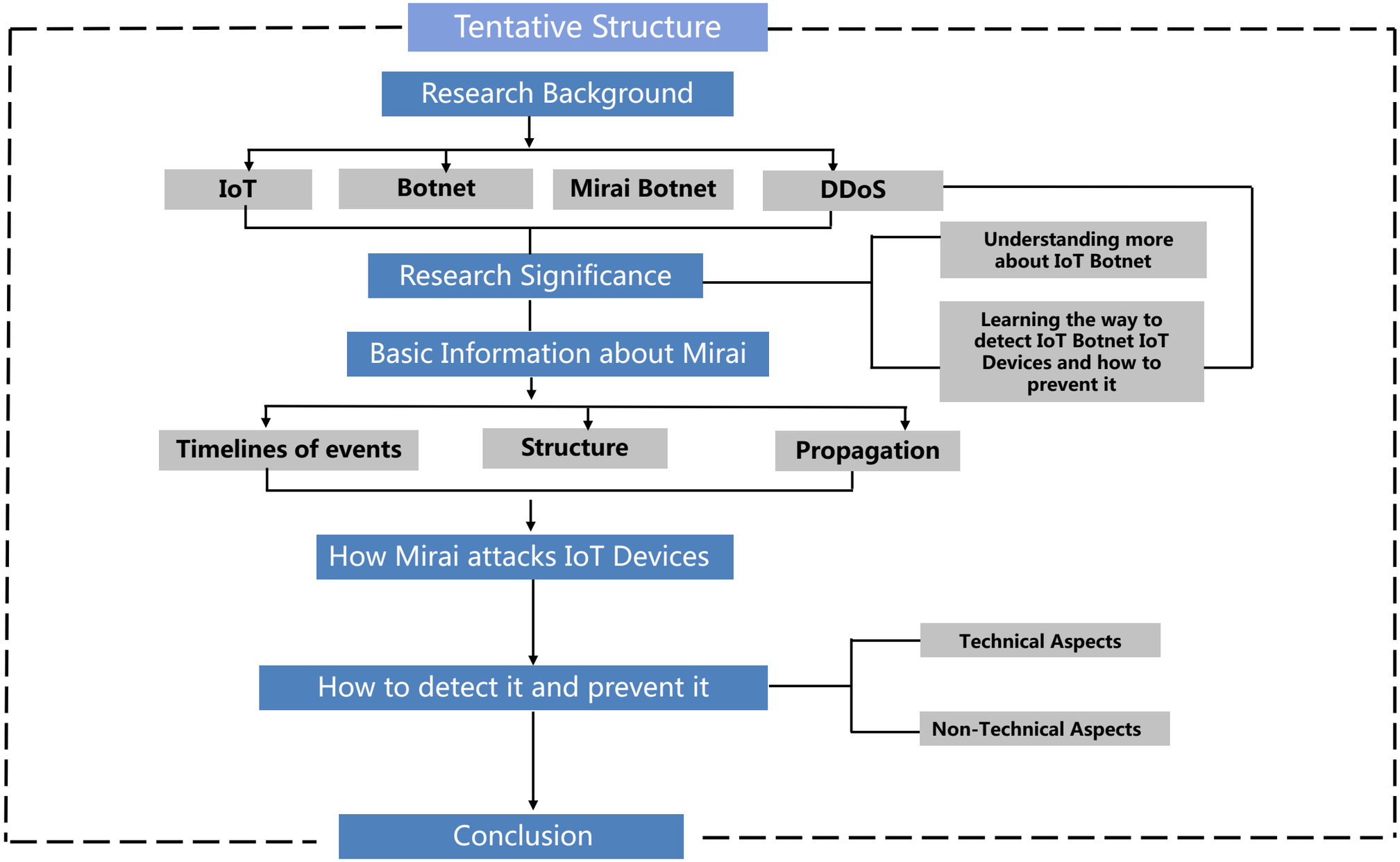


How to detect and prevent it?



Research on IoT Botnet— Use Mirai Botnet as an Example

Tentative Structure



References - General

[1].Manos Antonakakis, Georgia Institute of Technology; Tim April, Akamai; Michael Bailey, University of Illinois, Urbana-Champaign; Matt Bernhard, University of Michigan, Ann Arbor; Elie Bursztein, Google; Jaime Cochran, Cloudflare; Zakir Durumeric and J. Alex Halderman, University of Michigan, Ann Arbor; Luca Invernizzi, Google; Michalis Kallitsis, Merit Network, Inc.; Deepak Kumar, University of Illinois, Urbana-Champaign; Chaz Lever, Georgia Institute of Technology; Zane Ma and Joshua Mason, University of Illinois, Urbana-Champaign; Damian Menscher, Google; Chad Seaman, Akamai; Nick Sullivan, Cloudflare; Kurt Thomas, Google; Yi Zhou, University of Illinois, Urbana-Champaign.**Understanding the Mirai Botnet**. (2017)

[2]. Kishore Angrishi. **Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV) : IoT Botnets**. (2017)

[3]. Artur Marzano, David Alexander, O. Fonseca, E. Fazzion, C. Hoepers, Klaus Steding-Jessen, M. H. P. Chaves, Ítalo S. Cunha, D. Guedes, W. Meira .**The Evolution of Bashlite and Mirai IoT Botnets.** 2018 IEEE Symposium on Computers and Communications (ISCC)

[4]. Basheer Al-Duwairi, Wafaa Al-Kahla, Mhd Ammar AlRefai, Yazid Abdelqader, Abdullah Rawash, Rana Fahmawi. **SIEM-based detection and mitigation of IoT-botnet DDoS attacks.** (2019)

[5]. Huy-Trung Nguyen, Quoc-Dung Ngo, Van-Hoang Le. **A novel graph-based approach for IoT botnet detection**. (2019)

[6]. Stephen Herwig, Katura Harvey, George Hughey, Richard Roberts, Dave Levin. **Measurement and Analysis of Hajime, a Peer-to-peer IoT Botnet.** (2019)

[7]. Xiaolu Zhang, Oren Upton, Nicole Lang Beebe, Kim-Kwang Raymond Choo**. IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers.** (2020)

[8]. Constantinos Kolias, George Mason University, Georgios Kambourakis, University of the Aegean Angelos Stavrou, George Mason University Jeffrey Voas, IEEE Fellow. **DDoS in the IoT: Mirai and Other Botnets**. (2017)

References - General

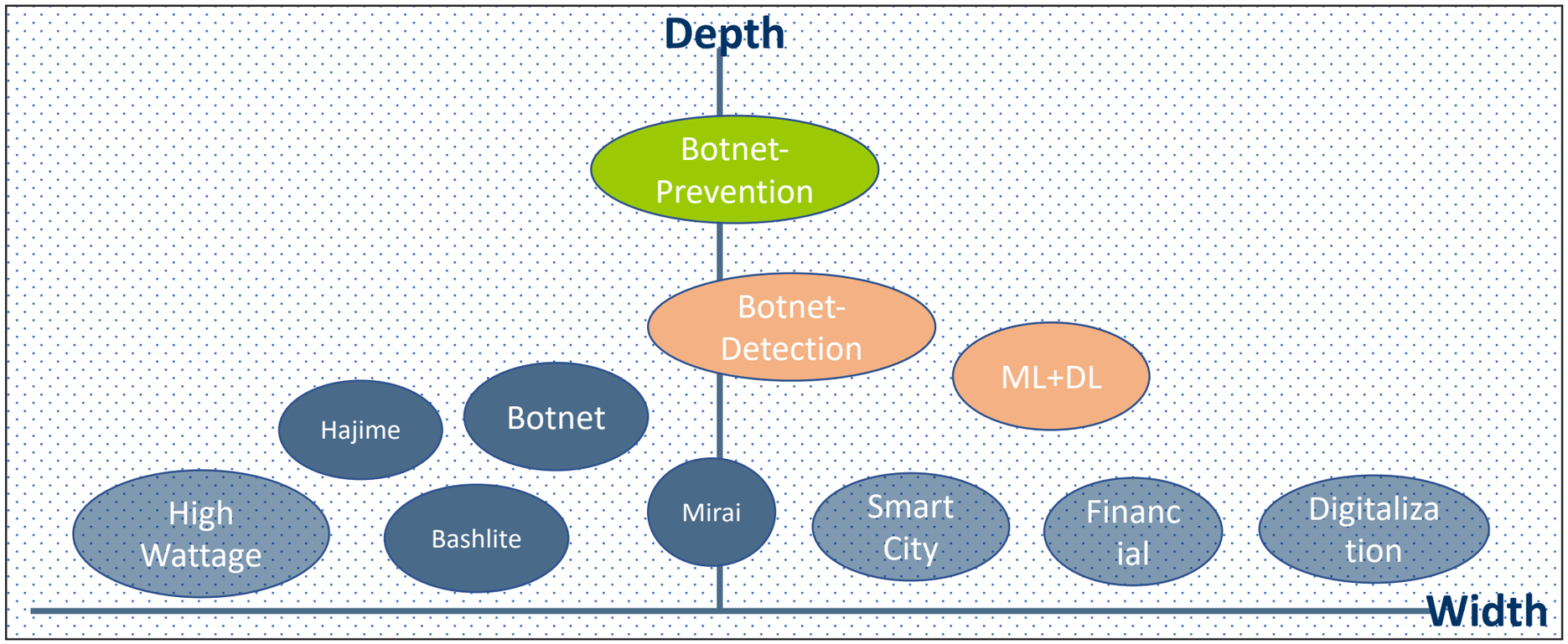
[9]. Priscilla Moriuchi, Sanil Chohan. **Mirai-Variant IoT Botnet Used to Target Financial Sector in January 2018**. (2018)

[10]. Elisa Bertino, Purdue University, Nayeem Islam, Qualcomm. **Botnets and Internet of Things Security.** (2017)

[11]. Saleh Soltan, Prateek Mittal, and H. Vincent Poor, Princeton University. **BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid.** (2018)

[12]. Amaal Al Shorman, Hossam Faris, Ibrahim Aljarah**. Unsupervised intelligent system based on one class support vector machine and Grey Wolf optimization for IoT botnet detection.** (2019)

[13]. Vinayakumar R, Mamoun Alazab Senior Member, IEEE, Sriram S, Quoc-Viet Pham, Soman KP, Simran K. **A Visualized Botnet Detection System based Deep Learning for the Internet of Things Networks of Smart Cities.** (2020)

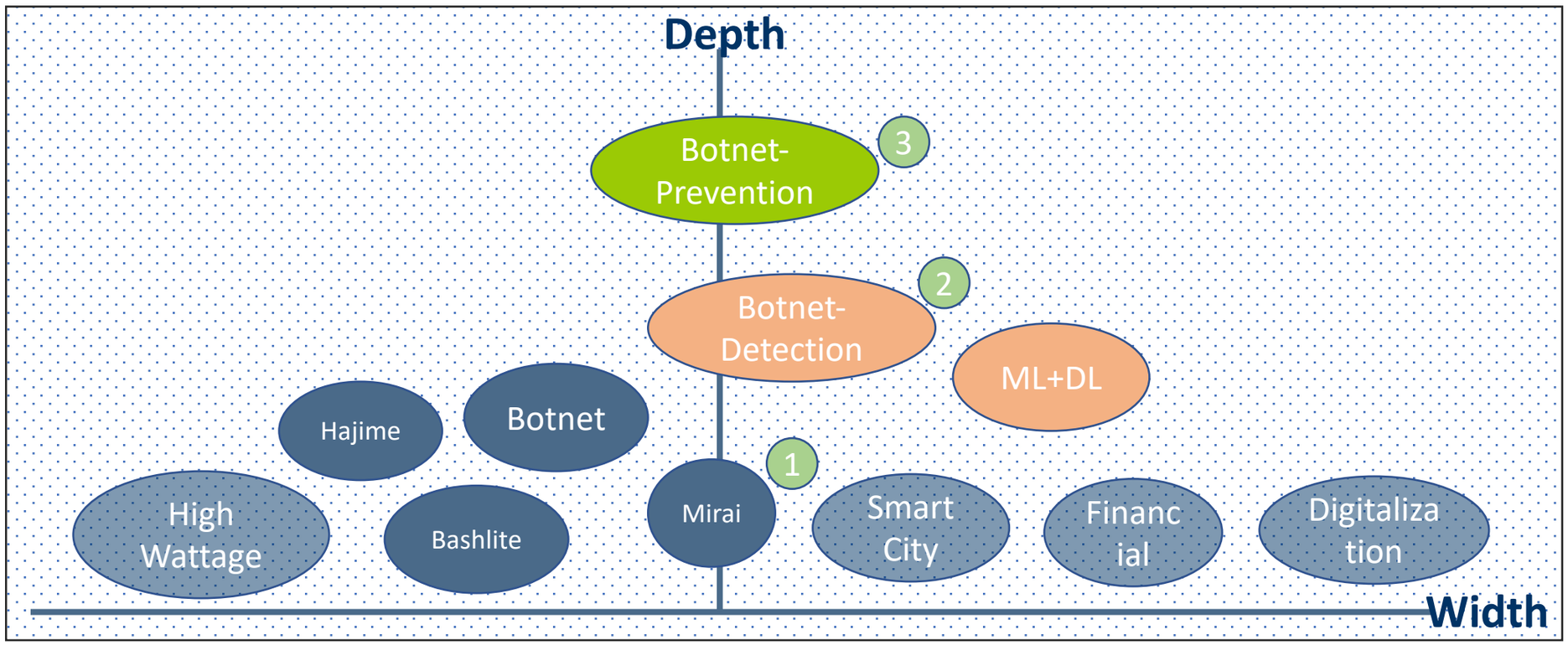


References – The References I Will Focus on

[1].Manos Antonakakis, Georgia Institute of Technology; Tim April, Akamai; Michael Bailey, University of Illinois, Urbana-Champaign; Matt Bernhard, University of Michigan, Ann Arbor; Elie Bursztein, Google; Jaime Cochran, Cloudflare; Zakir Durumeric and J. Alex Halderman, University of Michigan, Ann Arbor; Luca Invernizzi, Google; Michalis Kallitsis, Merit Network, Inc.; Deepak Kumar, University of Illinois, Urbana-Champaign; Chaz Lever, Georgia Institute of Technology; Zane Ma and Joshua Mason, University of Illinois, Urbana-Champaign; Damian Menscher, Google; Chad Seaman, Akamai; Nick Sullivan, Cloudflare; Kurt Thomas, Google; Yi Zhou, University of Illinois, Urbana-Champaign.**Understanding the Mirai Botnet**. (2017)

[2]. Kishore Angrishi. **Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV) : IoT Botnets**. (2017)

[3]. Elisa Bertino, Purdue University, Nayeem Islam, Qualcomm. **Botnets and Internet of Things Security.** (2017



References – The References I Will Not Focus on

[1]. Artur Marzano, David Alexander, O. Fonseca, E. Fazzion, C. Hoepers, Klaus Steding-Jessen, M. H. P. Chaves, Ítalo S. Cunha, D. Guedes, W. Meira .**The Evolution of Bashlite and Mirai IoT Botnets.** 2018 IEEE Symposium on Computers and Communications (ISCC)

[2]. Basheer Al-Duwairi,Wafaa Al-Kahla, Mhd Ammar AlRefai, Yazid Abdelqader, Abdullah Rawash,Rana Fahmawi. **SIEM-based detection and mitigation of IoT-botnet DDoS attacks.** (2019)

[3]. Huy-Trung Nguyen, Quoc-Dung Ngo,Van-Hoang Le. **A novel graph-based approach for IoT botnet detection**. (2019)

[4]. Stephen Herwig, Katura Harvey, George Hughey, Richard Roberts, Dave Levin. **Measurement and Analysis of Hajime, a Peer-to-peer IoT Botnet.** (2019)

[5]. Xiaolu Zhang, Oren Upton, Nicole Lang Beebe, Kim-Kwang Raymond Choo**. IoT Botnet Forensics: A Comprehensive Digital Forensic Case Study on Mirai Botnet Servers.** (2020)

[6]. Constantinos Kolias, George Mason University, Georgios Kambourakis, University of the Aegean Angelos Stavrou, George Mason University Jeffrey Voas, IEEE Fellow. **DDoS in the IoT: Mirai and Other Botnets**. (2017)

[7]. Priscilla Moriuchi, Sanil Chohan. **Mirai-Variant IoT Botnet Used to Target Financial Sector in January 2018**. (2018)

[8]. Saleh Soltan, Prateek Mittal, and H. Vincent Poor, Princeton University. **BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid.** (2018)

[9]. Amaal Al Shorman, Hossam Faris, Ibrahim Aljarah**. Unsupervised intelligent system based on one class support vector machine and Grey Wolf optimization for IoT botnet detection.** (2019)

[10]. Vinayakumar R, Mamoun Alazab Senior Member, IEEE, Sriram S, Quoc-Viet Pham, Soman KP, Simran K. **A Visualized Botnet Detection System based Deep Learning for the Internet of Things Networks of Smart Cities.** (2020)

Tentative Schedule

T0 = **14.04.2021** Introductory session

T0 + 1 week : **21.04.2021** Topic selection

T0 + 3 weeks: **05.05.2021** Midterm Presentation -- （Tentative Structure and Reference)

T0 + 7 weeks : **02.06.2021** deadline to submit alpha version of the report (Complete the structure and try to finish 50%)

T0 + 11 weeks : **30.06.2021** deadline to submit final version of the report

T0 + 12 weeks **: 07.07.2021** Final presentation.

Thank you for your listening!