Analyzing the Impact of Botnet Infection on Networked Systems using Timed Automata

Alvi Jawad, Luke Newton
Systems and Computer Engineering Department
Carleton University, Ottawa, Canada
{alvijawad, lukenewton}@cmail.carleton.ca

Abstract— **The Internet of Things (IoT) has stimulated the creation of a new era with the promise of ubiquitous connectivity. Recent years have seen a proliferation of cheap IoT devices, many of which employ energy-efficient designs, mandating low computational resources that preclude the use of rigorous security mechanisms. Furthermore, many deployed IoT devices continue to use default vendor passwords, and many others tend to have weak credentials. Adversaries in IoT exploit these security vulnerabilities to create their own army of connected IoT devices, known as botnets, only to be used later to perform various malicious attacks on the network. In this project, we aim to model and simulate the dynamic behavior of a botnet as a networked timed automata using the modeling tool UPPAAL to gain insight into the botnet infection process in diverse system configurations. Additionally, we aim to analyze the impact of the infection process on the modeled network by implementing existing security mechanisms and assess the feasibility of such measures.**

Index Terms—**Internet of Things (IoT), Botnets, Network Security, Modeling, Timed Automata, UPPAAL**

I. Introduction

The Internet of Things (IoT) refers to the interconnected network of the vast number of internet-enabled physical objects around the world. In recent years, the increased availability of low cost, low power sensors, and enhanced communication methods has caused an explosion in the number of IoT devices [1]. With this increased communication, data collection, and analysis, IoT has the potential to improve many facets of society, including, but not limited to, healthcare, infrastructure, supply chains, and the general home and office environments. Unfortunately, due to the relatively low computational resources available for typical IoT devices and the rushed production of many such devices, the IoT infrastructure has become vulnerable to a number of security threats [2].

Botnets are one of the major security issues faced in the current IoT landscape [3]. Botnets are a network of devices corrupted by malware that are ready to be instructed by a botmaster through some Command and Control infrastructure. Once in control of a large enough botnet, botmasters may either use or trade the attacking capabilities in exchange for money to perform targeted attacks on websites [4]. The relatively low computational resources of cheap IoT devices imply the lack of built-in measures to protect against malware [5]. Furthermore, IoT devices are often deployed with weak and/or default credentials, and the embedded nature of the devices can make it challenging, and often impossible, to patch vulnerabilities. All this comes together to make IoT devices ideal candidates for botnet infection.

While bots in an IoT botnet do not individually present a threat, a large enough botnet can cause catastrophic impacts. One such example is the Mirai botnet, first identified in 2016, that launched Distributed Denial of Service (DDoS) attacks against security blog KrebsOnSecurity and French cloud computing company OVH, with malicious traffic peaking at 620 Gbps and 1.1 Tbps respectively [4]. More recently, the largest ever DDoS attack was targeted at Amazon Web Services in February 2020, which saw sustained traffic at 2.3 Tbps [6]. While the majority of the botnet exploits involve DDoS attacks, they are not limited to DDoS attacks only. The following lists several malicious capabilities of botnets:

1) DDoS: The most common botnet attack. A large enough botnet can flood network endpoints or links with enough traffic to severely degrade or completely disallow legitimate traffic through the targeted location [3].
2) General bot traffic: Continuous communication and propagation consumes network bandwidth and often results in decreased performance in infected devices.
3) Spam or Malware dissemination: Rather than sending all bot traffic to one location like in a DDoS attack, botnets can also be used to distribute malicious payloads to a wide variety of targets [3].
4) Firmware corruption: Botnets like BrickerBot can, once commanded, access and destroy a device's firmware [4].

Research on botnets has surged in popularity after the emergence of the Mirai Botnet, and our research intends to build on top of these efforts.

The rest of this proposal is structured as follows. Section II explores the motivation behind our study and presents our research objectives. Section III outlines how we plan to approach our proposed modeling and analysis through various stages of the project. Finally, Section IV describes our envisioned expected outcomes from the project.

II. Problem Statement

The botnet infection process has been studied in great detail and modeled using several modeling formalisms, including epidemiological, stochastic, and economic models [7], as well as Petri Nets [8]. As countermeasures, patching vulnerable devices, frequent rebooting, and even the use of innocuous botnets have been suggested to reduce the botnet infection rates [8]. However, these studies do not consider different classes of IoT devices that exhibit varying behaviors, and as such, ignore the presence of the heterogeneity inherently present in the massive IoT infrastructure.

In this project, we aim to model a Mirai-like botnet infection process using timed automata and observe the impact of the infection on the simulated network in varying system configurations. The timed automata mathematical model allows us to formally model and analyze the real-time behavior of botnets and its individual components, and observe the behavioral changes in the botnet due to behavioral changes in individual entities within the network [9]. The high decidability of timed automata allows us to exhaustively check the model for reachability properties such as whether in each simulation scenario, the botnet is capable of infecting all the devices within the entire network, and if not, why. Another consideration would be identifying the percentage of devices that can consistently be infected within a certain time in each system configuration, and how implementing existing security mechanisms impact those figures.

Possible variations in the system configuration include the type and number of such types of devices connected to the network, the capability to reboot and frequency of reboots, vendor patching, and the inclusion of randomness in device behaviors. If feasible, possible extensions to the study may include different network topologies and the modeling of different classes of botnets.

III. Work Plan

The Work Plan for the project is intended to outline the envisioned timeline to achieve the objectives set out for this project. The timeline is subjective to change based on the progress made and feedback received in the earlier stages of our research.

For modeling purposes, we will be using the integrated tool environment UPPAAL that allows for the modeling, verification, and validation of real-time systems modeled as networked timed automata [10]. UPPAAL is freely available only for research purposes[1] within the academia.

The timeline for the project is divided into four primary phases. These phases involve, notably, Literature Review and Initial Testing, System Modeling and Simulation, Data Analysis, and Assessment. Each phase will end with either a discussion with the course instructor or a research presentation and the feedback received from those events will be taken into account in the subsequent phases.

The first phase will focus primarily on identifying additional research questions by an extensive literature review of botnet behaviors and previous attempts to model such behavior using various modeling techniques. Concurrently, we will explore the capabilities of the UPPAAL modeling tool, create an initial system model to perform some initial simulations to meet the instructor for a detailed discussion two weeks before the progress presentation. The progress made up until that point, coupled with the feedback from the discussion, will direct our future activities and, if necessary, a shift in research focus.

Phase two will emphasize enhancing model accuracy and experimentation. We should be fairly certain about our final research goal at this point, which will be reflected by a more concentrated literature search closely aligning with our final goal. This phase ends with the progress presentation in early November.

In the third phase, we will prioritize analyzing the experimental results and verifying some of the reachability properties of the system. The results from this stage might also engender modified experiments and small changes in the model to accommodate those modifications. This phase will also end with a discussion with the instructor, determining if an extension of the scope is feasible before the presentation of the results in early December.

The final phase will focus almost exclusively on the writing and finalizing the assessment of our experimental results to provide feasible recommendations. Additionally, this phase will include rigorous scrutiny of each group member's written work by the other to deliver a high-quality piece of work by the end of the project deadline.

IV. Expected Final Outcome

The anticipated final outcome of this project is a close inspection of the botnet infection process through modeling and simulation and observation of how variations in the system configuration affect the process. Additionally, we intend to gain insights into the effectiveness of existing security mechanisms and provide recommendations for the feasibility of such measures based on our experimental data and analysis.

References

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[2] F. A. Alaba, M. Othman, I. A. T. Hashem, and F. Alotaibi, "Internet of things security: A survey," *Journal of Network and Computer Applications*, vol. 88, pp. 10–28, 2017.

[3] S. S. Silva, R. M. Silva, R. C. Pinto, and R. M. Salles, "Botnets: A survey," *Computer Networks*, vol. 57, no. 2, pp. 378–403, 2013.

[4] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "Ddos in the iot: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, 2017.

[5] E. Bertino and N. Islam, "Botnets and internet of things security," *Computer*, vol. 50, no. 2, pp. 76–79, 2017.

[6] Cloudflare, "Famous ddos attacks — the largest ddos attacks of all time."

[7] P. Wainwright and H. Kettani, "An analysis of botnet models," in *Proceedings of the 2019 3rd International Conference on Compute and Data Analysis*, pp. 116–121, 2019.

[8] H. Tanaka, S. Yamaguchi, and M. Mikami, "Quantitative evaluation of hajime with secondary infectivity in response to mirai's infection situation," in *2019 IEEE 8th Global Conference on Consumer Electronics (GCCE)*, pp. 961–964, IEEE, 2019.

[9] R. Alur and D. L. Dill, "A theory of timed automata," *Theoretical computer science*, vol. 126, no. 2, pp. 183–235, 1994.

[10] G. Behrmann, A. David, and K. G. Larsen, "A tutorial on uppaal," in *Formal methods for the design of real-time systems*, pp. 200–236, Springer, 2004.

[1] http://www.uppaal.org/