LISA: Predicting the Impact of DoS Attacks on Real-World Low Power IoT Systems

Luca Arnaboldi
School of Computing, Newcastle University
Email: l.arnaboldi@ncl.ac.uk

Charles Morisset
School of Computing, Newcastle University
Email: charles.morisset@ncl.ac.uk

Organizations and researchers alike have widely recognised the multiple advantages of adapting Network Intrusion Detection Systems (NIDS) as the norm to monitor against DoS attacks on their systems [1]. Standard approaches used to train NIDS include using a database of known attacks (*misuse detection*) and testing systems to create a "benchmark" behaviour and flag any anomaly as a potential attack (*anomaly detection*) [2].

Implementing a NIDS within an Internet of Things (IoT) network however faces multiple challenges. Firstly, it is usually challenging to establish a benchmark behaviour in dynamic IoT systems as devices may constantly shift, new devices might join and behaviours might change [3], which might prevent using anomaly detection. Secondly, protocols can vary from one network to another, which necessitates data collection to be bespoke to an individual system [4]. Thirdly, a misuse detection can be time consuming to enforce, since collecting data unique to a system and for each attack is time consuming [2] and some system changes can require to collect the data or part of the data from scratch (e.g. interactive smart homes where devices can change frequently [5]).

To address the second and third challenges, we present a novel modelling approach LISA (Lightweight IoT System under Attack). In a nutshell, a LISA model consists of a collection of Markov Decision Processes (MDP), representing the IoT network, the attackers, and some processes monitoring the security metrics under consideration. A trace of the LISA model (corresponding to a sequence of actions of the different MDPs) should match a trace of the actual system, and conversely, such that it becomes possible to train a NIDS for the actual system on the traces of the LISA model. The main strengths of our approach is the ability to easily represent various configurations for the IoT network as well as multiple types of attackers.

Using LISA, one can simulate different power of attacks (e.g. a botnet with multiple devices), as a factor of messages sent and predict the impact on the system (e.g., decrease in throughput, time to system failure). Each MDP component of the LISA model is based on measurements from the actual system (e.g. the time required by a specific device to process a message). The task of the model is twofold 1) represent key characteristics of an IoT device to infer specifics of a real world system e.g. time to drain of battery under a specific attack and 2) generate traces of behaviour of the system under attack. The specifics in question for the devices are memory and battery power, since each device will have unique battery levels and memory that could easily be overwhelmed by an attacker. The attacker MDPs are manually defined to match the behaviour of real world attacks. A particular strength of our approach is the ability to find the optimal path of attack through an *MDP adversary* [6] (although we still need for all possible attacks to be modelled first).

To model low power IoT devices we make the following assumptions: at the communication layer low power IoT devices capabilities are generally limited to reading/receiving and passing on/distributing data [3] independent of the protocol used, that the bandwidth is independent of the device, and that the battery drainage is linear in respect to current [7]. The action labels of the MDP are used in to represent the behaviour of a device and to synchronize with other parts of the system. The device has an associated monitor that synchronizes on each action and guards for the current values of battery and memory. In a LISA a monitor is non blocking, the calculations for battery are based on increase in Amperes at time T based on processing of messages. The larger the inflow of messages (due to attacker processing power) the larger the drain on the battery [7], [8], [9]. The monitor allows to calculate traces of executions that lead to battery drainage and/or memory exhaustion of the devices.

An attack synchronizes with a subset of actions of the device, when an attacker synchronizes on the device, the monitor will synchronize on that action and calculates the drainage. The monitor keeps track of all these measurements for its respective device. Implementing a LISA model in a tool like PRISM allows us to make use of Probabilistic Control Tree Logic (PCTL) [10] to calculate matching behavior between the system and the model, to compute the optimal attack path, and to simulate traces of actions we can use the verified model to create a synthetic data set of network behaviour.

Preliminary results on a simple system of interconnected sensor devices shows that LISA enables the accurate prediction of how long it will take to take down the real world device. We have used attack traces generated from the MDPs to train NIDS to detect DoS attacks on the real world system, and the ongoing results are encouraging. We believe that LISA will enable system designers to test their system before implementing it and to make accurate security decisions about systems of IoT devices.

References

[1] D. Lin, “Network intrusion detection and mitigation against denial of service attack,” 2013.

[2] P. Mell, V. Hu, R. Lippmann, J. Haines, and M. Zissman, “An overview of issues in testing intrusion detection systems,” 2003.

[3] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, “Internet of things (iot): A vision, architectural elements, and future directions,” *Future generation computer systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[4] E. Guillen, J. Sánchez, and R. Paez, “Inefficiency of ids static anomaly detectors in real-world networks,” *Future Internet*, vol. 7, no. 2, pp. 94–109, 2015.

[5] “Beolink smarthome.” [Online]. Available: https://www.bang-olufsen.com/en/solutions/beolink-smarthome

[6] M. Kwiatkowska, G. Norman, and D. Parker, “Markov decision process.” [Online]. Available: http://www.prismmodelchecker.org/lectures/biss07/04-mdps.pdf

[7] “Calculating battery life in iot applications.” [Online]. Available: http://uk.farnell.com/calculating-battery-life-in-iot-applications#calculator

[8] L. Arnaboldi and C. Morisset, “Quantitative analysis of dos attacks and client puzzles in iot systems,” in *Security and Trust Management - 13th International Workshop, STM 2017, Oslo, Norway, September 14-15, 2017, Proceedings*, 2017, pp. 224–233.

[9] Z. Abbas and W. Yoon, “A survey on energy conserving mechanisms for the internet of things: Wireless networking aspects,” *Sensors*, vol. 15, no. 10, pp. 24 818–24 847, 2015.

[10] C. Baier, J.-P. Katoen, and K. G. Larsen, *Principles of model checking*. MIT press, 2008.