A performance assessment of network address shuffling in IoT systems

Georg Merzdovnik[1,2], Aljosha Judmayer[1],
Artemios G. Voyiatzis[1,2], and Edgar Weippl[2,1]

[1] SBA Research, Vienna, Austria
{gmerzdovnik,ajudmayer,avoyiatzis,eweippl}@sba-research.org
[2] TU Wien, Vienna, Austria

Networked embedded systems of different forms and shapes are the building blocks for the Internet of Things (IoT). The security of these systems is of paramount importance for the function of the Internet already. Despite the constraints in memory, processing, and power, the network connectivity is often more than ample. IoT devices often have network access interfaces of 100 Mbps or even 1 Gbps. This combined with the exploding number of Internet-connected devices gives rise to new forms of attacks.

The two most severe distributed denial of service (DDoS) attacks ever faced on the Internet, with an aggregate traffic volume of more than 1.1 Tbps occurred in 2016. These attacks became feasible due to the availability of numerous vulnerable and compromised IoT systems, including devices such as digital video recorders (DVRs), IP cameras, and smart thermostats.

The resource constraints of these embedded systems make it difficult to integrate network security mechanisms that are commonplace in enterprise IT environments. Furthermore, the former are often part of smart homes and smart environments. In these settings, the consumers opt for a set-and-forget approach. Software updates and upgrades are in many cases impossible to realize.

In this modus operandi, it is crucial to engineer defenses that are *preventive* in nature. Most of the IoT systems are, from a network perspective, "*sitting ducks*", i.e., they are easily accessible from the network and passively receive all kind of attacks aiming to compromise them.

Moving-target defense (MTD) is an approach to improve the standing of defending information systems in general by breaking this attacker-defender asymmetry [3]. The key assumption for MTD is that the attackers will first perform a reconnaissance to identify possible targets. Then, at a next phase, they launch their (targeted) attack. Under this assumption, MTD dictates to mobilize the available resources, so that the attackers hit wrong or non-existent targets and thus, succeed in defending the systems; collect evidence of their behavior; and provide enough time to deploy network-wide defenses (e.g., honeypots) for further studying their practices and delaying further attacks [4].

While host- and application-level MTDs are hard to realize in embedded systems, network-level ones (e.g., time-varying topology) are considered feasible [2]. IPv6 and IPv4 network address shuffling, i.e., periodically changing the network addresses of the devices in a coordinated way, is an example network-level MTD [1].

In this paper, we augment existing literature by exploring the capability of modern IoT systems to handle network address shuffling. More specifically, we study the performance overhead and the impact of periodically changing network addresses and ports in Linux-based IoT systems (namely, Raspberry Pi and Carambola2) under different probing and network scanning activity scenarios.

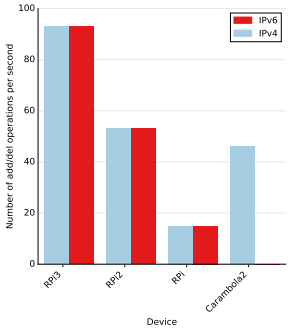

Fig. 1. Address change operations per second and device

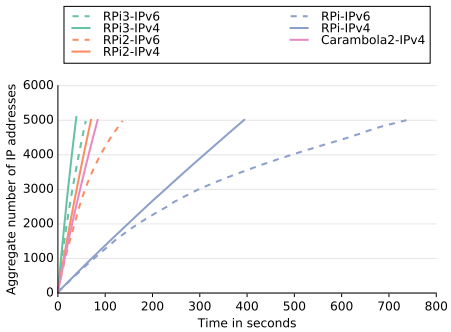

Fig. 2. Total number of IP addresses

Our findings indicate that network address shuffling is feasible in IoT environments. However, special care must be taken when implementing such techniques. The number of possible IP address changes per second varies significantly per device, as depicted in Figure 1. The simultaneous use of multiple IP addresses has an impact in the performance, especially in the case of IPv6, as depicted in Figure 2: the more addresses already in use, the more time to add new ones. Interestingly enough, Carambola2, running OpenWRT with a clock rate of 400 MHz clearly outperforms the *stronger* Raspberry Pi B+ clocked at 700 MHz, reaching the figures of Raspberry Pi 2, which is clocked at 900 MHz and has four cores.

References

1. Cai, G., Wang, B., Wang, X., Yuan, Y., Li, S.: An introduction to network address shuffling. In: 18th International Conference on Advanced Communication Technology (ICACT). pp. 185–190. IEEE (2016)
2. Casola, V., De Benedictis, A., Albanese, M.: A moving target defense approach for protecting resource-constrained distributed devices. In: 14th International Conference on Information Reuse and Integration (IRI). pp. 22–29. IEEE (2013)
3. Jajodia, S., Ghosh, A.K., Swarup, V., Wang, C., Wang, X.S.: Moving target defense: creating asymmetric uncertainty for cyber threats, vol. 54. Springer Science & Business Media (2011)
4. Zhuang, R., DeLoach, S.A., Ou, X.: Towards a theory of moving target defense. In: Proceedings of the First ACM Workshop on Moving Target Defense. pp. 31–40. ACM (2014)