Dr. ing. C. Hernandez Ganan (TUD), RAPID

English scientific summary

Despite the benefits of the widespread deployment of diverse Internet-enabled devices such as IP cameras and smart home appliances - the so-called Internet of Things (IoT) has amplified the attack surface that is being leveraged by cyber criminals. While manufacturers and vendors keep deploying new products, infected devices can be counted in the millions and spreading at an alarming rate all over consumer and business networks. The objective of this project is twofold: (i) to explain the causes behind these infections and the inherent insecurity of the IoT paradigm by exploring innovative data analytics as applied to raw cyber security data; and (ii) to promote effective remediation mechanisms that mitigate the threat of the currently vulnerable and infected IoT devices.

By performing large-scale passive and active measurements, this project will allow the characterization and attribution of compromise IoT devices. Understanding the type of devices that are getting compromised and the reasons behind the attacker's intention is essential to design effective countermeasures. This project will build on the state of the art in information theoretic data mining (e.g., using the minimum description length and maximum entropy principles), statistical pattern mining, and interactive data exploration and analytics to create a casual model that allows explaining the attacker's tactics and techniques. The project will research formal correlation methods rooted in stochastic data assemblies between IoT-relevant measurements and IoT malware binaries as captured by an IoT-specific honeypot to aid in the attribution and thus the remediation objective.

Research outcomes of this project will benefit society in addressing important IoT security problems before manufacturers saturate the market with ostensibly useful and innovative gadgets that lack sufficient security features, thus being vulnerable to attacks and malware infestations, which can turn them into rogue agents. However, the insights gained will not be limited to the attacker behavior and attribution, but also to the remediation of the infected devices. Based on a casual model and output of the correlation analyses, this project will follow an innovative approach to understand the remediation impact of malware notifications by conducting a longitudinal quasi-experimental analysis. The quasi-experimental analyses will examine remediation rates of infected/vulnerable IoT devices in order to make better inferences about the impact of the characteristics of the notification and infected user's reaction. The research will provide new perspectives, information, insights, and approaches to vulnerability and malware notifications that differ from the previous reliance on models calibrated with cross-sectional analysis. This project will enable more robust use of longitudinal estimates based on documented remediation change. Project results and methods will enhance the capacity of Internet intermediaries (e.g., ISPs and hosting providers) to better handle abuse/vulnerability reporting which in turn will serve as a preemptive countermeasure. The data and methods will allow to investigate the behavior of infected individuals and firms at a microscopic scale and reveal the causal relations among infections, human factor and remediation.

English public summary

Despite the benefits of the widespread deployment of diverse Internet-enabled devices such as IP cameras and smart home appliances, the Internet-of-things has amplified the attack surface that is being leveraged by cyber criminals. Millions of IoT devices are infected and being misused for malicious purposes. The RAPID project aims at explaining the causes behind these infections; and promoting effective remediation mechanisms.

Dutch public summary

Naast de voordelen van de wijdverbreide inzet van diverse internet-compatibele apparaten zoals IPcamera's en slimme huishoudelijke apparaten, heeft het Internet-of-Things tevens het aanvalsoppervlak vergroot dat wordt gebruikt door cybercriminelen. Miljoenen IoT-apparaten zijn geïnfecteerd en worden misbruikt voor criminele doeleinden. Het RAPID-project is gericht op het verklaren van de oorzaken van deze infecties; als ook het bevorderen van effectieve herstelmechanismen.