CYSEC Cybersecurity TU Darmstadt | System Security Lab | TECHNISCHE UNIVERSITÄT DARMSTADT

Bachelor / Master Thesis in IoT Sicherheit

Erkennung von Privatheitsangriffen und infizierten IoT-Geräten im Smart Home

IoT-Geräte wie z.B. smarte Kaffeemaschinen, intelligente Beleuchtungssysteme sowie virtuelle Assistenten wie Amazon Alexa sind in Smart Homes mittlerweile weit verbreitet. Die Sicherheit und Vertraulichkeit von Benutzerdaten in Smart Homes sicherzustellen ist aber nach wie vor eine große Herausforderung. In diesem Projekt untersuchen wir Privatheitsaspekte der Datenverarbeitung von IoT-Geräten, welches eines der wichtigsten Anliegen von Smarthome Benutzern ist. IoT-Geräte erzeugen täglich große Mengen an Daten, die in direktem Zusammenhang mit Nutzern stehen. Diese können, z.B. Videoaufnahmen aus IP-Kameras, Audiodaten von Voice Assistenten, Fitnessdaten aus Fitness Trackern oder Benutzeraktivitäten von Smart Home-Sensoren umfassen. Obwohl die Daten kritische sensible Informationen über den Benutzer offenbaren können, ist es oft nicht klar wie die Daten verarbeitet, übertragen, gespeichert und verwendet werden. Unseriöse IoT-Anbieter können unter Umständen insgeheim Daten unbefugterweise verwenden, z.B. ohne Genehmigung des Nutzers an Dritte verkaufen. Auch seriöse aber unaufmerksame IoT-Anbieter können Prozessdaten in einer Art und Weise verarbeiten, welches von Angreifern ausgenutzt werden kann.

Das Ziel dieser Arbeit ist die Entwicklung einer Methodik zur Ermittlung potenzieller Datenschutzlücken und Sicherheitsrisiken im Zusammenhang mit IoT-Geräten und zugehörigen IoT-Diensten, indem eine eingehende Analyse der von IoT-Geräten erzeugten Verkehrsmuster in typischen Smart Home-Szenarien durchgeführt wird.

Aufgaben

- Durchführung von Experimenten in einem Smart Home-Labor und Erfassung von Netzwerkverkehr von IoT-Geräten (Unser Laboraufbau umfasst mehr als 50 verschiedene IoT-Geräte.)
- Analyse des generierten Netzwerkverkehrs um Kommunikations- und Verhaltensmuster von IoT-Geräten zu verstehen und privahtheitsrelevante Informationen zu Identifizieren
- Verständnis darüber aufbauen, wie IoT-Daten verarbeitet und gespeichert werden, um potenzielle Sicherheitsprobleme zu identifizieren
- Einen Bericht über die Untersuchungsergebnisse in Form eines B.Sc. / M.Sc. Thesis verfassen

Voraussetzungen

- Gute Kenntnisse in Netzwerken, Protokollen sowie IT-Sicherheit und Privacy
- Erfahrung mit Python
- Gute analytische Fähigkeiten
- Motivation und Fähigkeit zur selbstständigen Arbeit sowie Bereitschaft zu Teamarbeit

Kontakt

Wenn Sie sich für dieses sehr aktuelle Thema interessieren, wenden Sie sich bitte an Thien Nguyen (ducthien.nguyen@trust.tu-darmstadt.de) oder Markus Miettinen (markus.miettinen@trust.tu-darmstadt.de) per Mail, um mehr zu erfahren. Bitte fügen Sie einen kurzen Überblick über Ihre bisherigen Studienleistungen und Notenspiegel bei.

AK Professor Dr.-Ing. Ahmad-Reza Sadeghi
Gebäude S4|14 (CASED Gebäude)
Mornewegstraße 30
64293 Darmstadt
https://www.trust.informatik.tu-darmstadt.de

April 2019

CYSEC Cybersecurity TU Darmstadt | System Security Lab | TECHNISCHE UNIVERSITÄT DARMSTADT

Bachelor / Master Thesis in IoT Security
Identifying privacy leaks and malicious IoT devices in smart homes

IoT devices ranging from home appliances like smart coffee machines, smart lighting systems to virtual home assistants like Amazon Alexa are being widely deployed in smart homes. However, assuring the security and privacy of user data in smart homes is a big challenge. In this project, we investigate the privacy aspects of data processing by smart home IoT devices, which is one of the most important concerns of smarthome users. IoT devices generate massive amounts of data related to smart home users on a daily basis. These data can be, e.g., video footage from IP cameras, audio from voice assistants, user's health-related information from fitness trackers or user activity data from smart home sensors. Although the data potentially reveal critical sensitive information about the users, it is often not clear how the data are processed, transmitted, stored and used. Dishonest IoT vendors might stealthily use the data, e.g., sell it to a third party without the user's approval or even being aware or of this. Non-malicious but careless IoT vendors might also process data in an insecure way which may be exploitable by an adversary.

The goal of this thesis assignment is to develop a methodology for identifying potential privacy leaks and security risks related to IoT devices and related IoT services by performing in-depth analysis of traffic patterns generated by IoT devices in typical smart home settings.

Tasks

- Perform experiments in a Smart Home lab setup and collect network traffic of real-world IoT devices (Our lab setup includes more than 50 different IoT devices.)
- Analyze network traffic generated by IoT devices to find and understand network traffic patterns and communication behaviours and potentially related privacy-relevant information
- Investigate how IoT data are processed and stored to identify potential privacy and security problems
- Report the findings in the form of a B.Sc. / M.Sc. thesis

Prerequisites

- Good knowledge in computer networks, network protocols as well as computer security and privacy
- Experience with Python
- Good analytical capabilities
- Motivation and capability to perform independent work as well as readiness to work in a team

Contact

If you are interested in this highly trendy topic, contact Thien Nguyen (ducthien.nguyen@trust.tu-darmstadt.de) or Markus Miettinen (markus.miettinen@trust.tu-darmstadt.de) via mail to learn more about it. Please include a brief overview of your study background and a transcript of records.

AK Professor Dr.-Ing. Ahmad-Reza Sadeghi
Gebäude S4|14 (CASED Gebäude)
Mornewegstraße 30
64293 Darmstadt
https://www.trust.informatik.tu-darmstadt.de

April 2019