Data Exfiltration in IoT Protocols

Daniel Uroz [1] Ricardo J. Rodríguez [1]

[1]Distributed Computing Group (DisCo), Universidad de Zaragoza, Spain

Instituto Universitario de Investigación en Ingeniería de Aragón
Universidad Zaragoza

IX Jornada de Jóvenes Investigadores del I3A

Introduction

Data exfiltration: unauthorized transfer of information

- Adversaries mask transferences using **covert channel** techniques to bypass defense mechanism (such as a firewall)
- Covert channel: any communication to transfer information violating the systems security policy

Internet of Things (IoT) networks: sensors, objects and smart nodes capable of communicating with each other without human intervention

- Generate continuous information, lately sent to an outside network responsible of recollection and processing
- Rely on **IoT protocols**, specially design for constrained devices

Characteristics of Protocol Exfiltration

1. **Packet type**: defined by a protocol, tailored for a specific purpose:
   - *Payload*: data able to carry in a single packet
   - *Overhead*: every byte not representing the actual data to exfiltrate
2. **Transport**: connectionless or connection-oriented transport protocols
3. **Error detection**: checksum redundancy mechanism to spot errors on received data

Studied Protocols

Traditional Protocols

- Internet Control Message Protocol (ICMP)
- Network Time Protocol (NTP)
- Domain Name System (DNS)

IoT Protocols

- Constrained Application Protocol (CoAP)
- Message Queuing Telemetry Transport (MQTT)
- Advanced Message Queuing Protocol (AMQP)

Experimentation

We developed the **Python library `chiton`** to exfiltrate data encapsulating the data into IoT protocol's packets:

`https://github.com/duroz/chiton`

We tested how IoT protocols perform for **different types of data varying from 1, 10, 100, 1000, 10000 to 100000 KiBs**

Results and Discussion

The results are plotted in Figure 1. A big time difference is shown between CoAP protocol and the MQTT and AMQP protocols, motivated by:

- The CoAP protocol needs to send more packets for the same amount of data. We kept IP packets under the 1280 bytes length limit, due to the TCP/IP network. However, there is a lack of knowledge about the maximum transmission unit used in the network
- Depending of the network configuration, nodes may apply more priority to TCP traffic over UDP

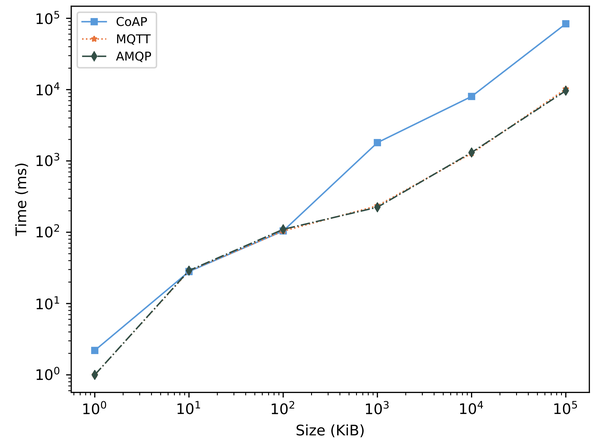

Figure 1. Comparison of data exfiltration times by IoT protocol

Conclusions

- **First study to extensively compare these IoT protocols from the point of view of data exfiltration**, focusing on characteristics such as overhead and useful payload for every available packet
- We **empirically measure and compare the time necessary to exfiltrate files of different data size**

References

[1] Daniel Uroz.
Data Exfiltration in IoT Protocols.
Master's Thesis, University of León, Spain, September 2020.
Online; `https://webdiis.unizar.es/~ricardo/files/TFMs/Exfiltracion-Datos-Protocolos-IoT_TFM_ULE.pdf`. Accessed on December 10, 2020.