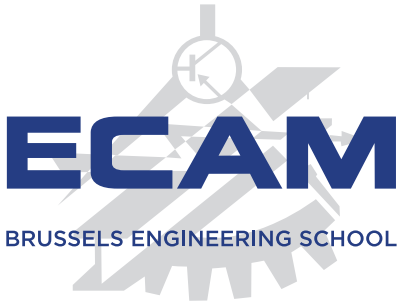


I5020 Computer Security

Session 8

Database, Cloud and IoT Security

Sébastien Combéfis

Fall 2019

Database Security

Database Security

- Sensitive information concentrated in organisational database

  Should be accessed by customer, partner, employee, etc.

- Database security has not kept pace with increased reliance
  - Imbalance between DBMS complexity and security techniques
  - SQL is a sophisticated interaction protocol
  - Lack of full-time database security personnel in companies
  - Heterogeneous mixture of databases platforms in companies

DBMS

- Database is a structured collection of data stored

  Data are used by one or more applications

- Database Management System (DBMS) is a suite of programs
  - Construct and maintain the database
  - Offer ad hoc query facilities to multiple users/applications
- Efficient access to large volumes of data
  - Vital to the operation of many organisations
  - Security requirements beyond capabilities of OS-based security
  - Should be able to control access to records in file

SQL Injection Attack

- Most frequent and dangerous network-based security threats

  Many attacks covered by the literature are SQLi

- Designed to exploit the nature of web application pages
  - Dynamic pages ask for information (location, credit card, etc.)
  - Dynamic content transferred to and from back-end databases
  - SQLi tries to send malicious SQL command to database server

- Several kinds of attacks can be done through SQLi

  Dump, modify/delete data, launch DoS attack, etc.

Injection Technique

- Prematurely terminate text string to append a new command

  Add comment mark -- to ignore subsequent text

```
"SELECT * FROM Orders WHERE ShipCity = '" + shipcity + "'"
```

↓

```
shipcity = "Redmond'; DROP TABLE Orders--'"
```

↓

```
"SELECT * FROM Orders WHERE ShipCity = 'Redmond'; DROP
TABLE Orders--'"
```

SQLi Attack Avenue

- Various final targets of SQLi attacks

  Directly attacking data in the database or outside it

- Five main avenues of SQLi attack can be identified
  - Provide suitable crafted user input sent to the web application
  - Corrupting server variables (used for HTTP header, etc.)
  - Second-order injection based on already existing information
  - Altering cookies sent from the client to the server
  - Physical user input generating dangerous barcode, RFID, etc.

SQLi Attack Type

- Various ways of retrieving the result of the attack

  Result retrieved directly or indirectly by the attacker

- Three main types of SQLi attacks can be identified
  - **Inband**: same communication channel than injection
  - **Inferential**: reconstruct information by observing results
  - **Out-of-band**: different channel to retrieve results

SQLi Attack Countermeasure

- A single countermeasure is insufficient

  Necessary to use an integrated set of techniques

- Three main types of countermeasures to deploy
  - **Defensive coding**: parametrised query insertion, SQL DOM
  - **Detection**: detect SQLi vulnerabilities in code/ongoing attack
  - **Run-time prevention**: check queries at runtime

Database Access Control

- DBMS typically provide an access control capability

  Assuming the computer system has authenticated each user

- DBMS typically support three range of administrative policies
  - **Centralised**: small number of privileged users for the DBMS
  - **Ownership-based**: table owner (creator) for the table
  - **Decentralised**: owner for other users (DAC)

```
GRANT SELECT ON ANY TABLE TO martin

REVOKE SELECT ON ANY TABLE FROM julian
```

Database Encryption

- Database protected by multiple layers of security

  Firewall, authentication, access control, DB access control, etc.

- Additional measure required in case of sensitive data
  - Database encryption is warranted and often implemented...
  - ...and used as the last line of defence
- Two disadvantages to database encryption
  - Authorised users must have access to decryption key
  - It becomes more difficult to perform record searching


Cloud Security

Cloud Security

- Substantial loss of control with cloud computing for enterprise

  Over resources, services and applications

- Several main cloud-specific threats have been identified
  - Attackers are abusing cloud computing to lead attacks
  - Exposed interface/API may be insecure (weak authentication)
  - Risk for client data loss or leakage
  - Credentials can be stolen for account/service hijacking
  - ...

Cloud Data Protection

- Many ways to compromise data with cloud computing

  Deletion/alteration of records, unlinking record, encoding key loss

- Two models for database environments for cloud computing
  - **Multi-instance** model

    Unique DBMS running on VM instance for each cloud subscriber
  - **Multi-tenant** model

    Predefined environment for the cloud subscriber with tagging

Cloud Security as a Service

- Security as a Service (SECaaS) package of security services

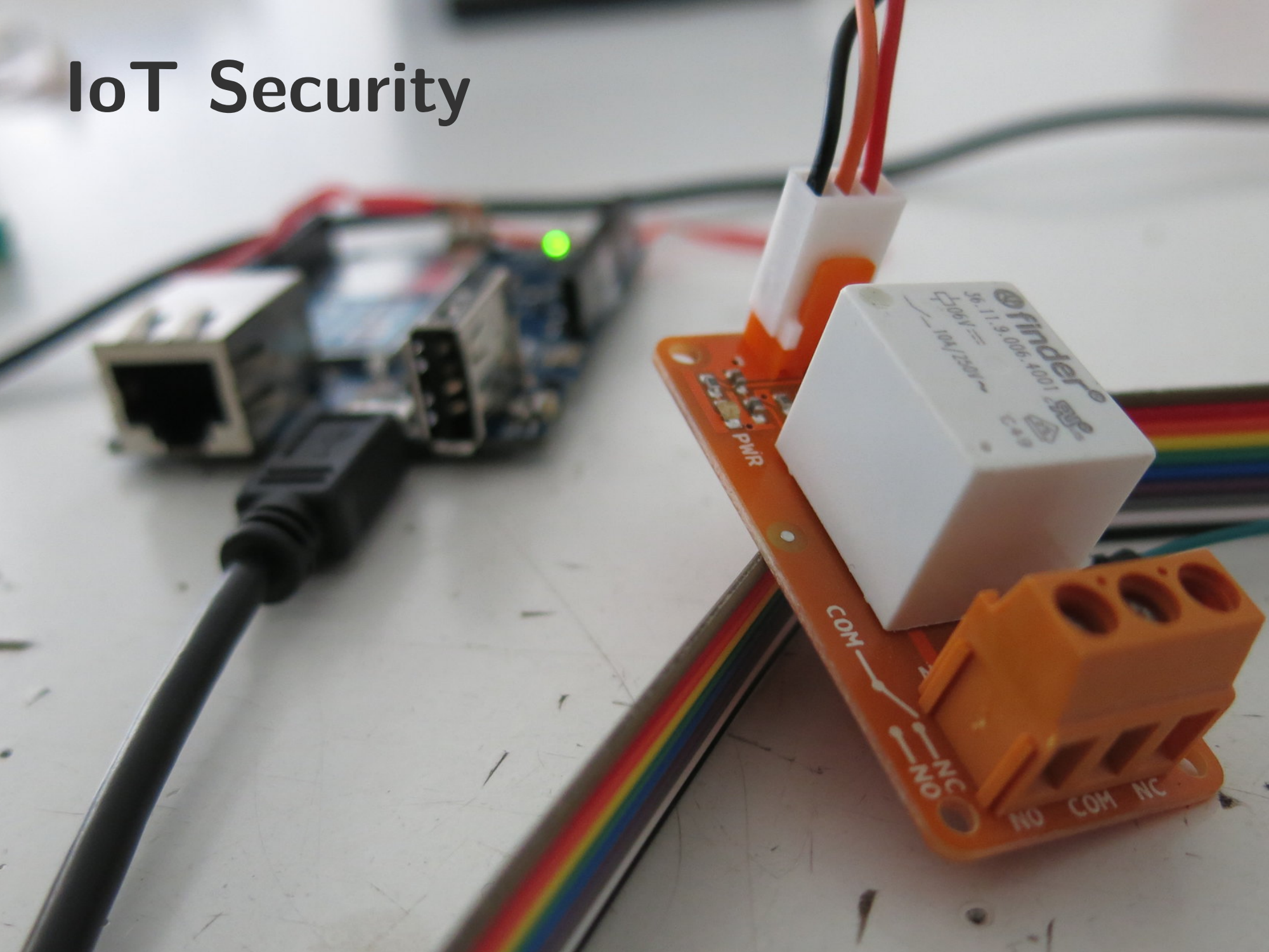
  Offload security responsibility from entreprise to service provider

- Several security services can be offered by SECaaS

  Authentication, anti-virus/malware/..., intrusion detection, etc.

- Three main categories related to cloud-based infrastructure
  - Identity and Access Management (IAM)
  - Data Loss Prevention (DLP)
  - Web security

IoT Security



IoT Security

- IoT security thought about as for any computer system

  Taking into account the potential limited computational resources

- Four main elements specific to IoT applications
  - Device authentication to confirm true and unique identity
  - Secure connection to protect data in motion
  - Secure code execution to protect data in use
  - Secure storage to protect data at rest

Layer Architecture

- IoT applications have three different operational layers

  Each of which with different functionalities and threats

- Three main layers common to IoT systems can be identified
  - **Perception layer** collects the data

    Protect the device from damaging or malicious input data
  - **Application layer** is the most diverse layer

    Data access permission, protection and recovery, etc.
  - **Network layer** transmits the data

    Same problems as TCP/IP (DoS, integrity damage, MitM, etc.)

Threat Vector

- Several ways for attacker to penetrate into an IoT device

  Attack surface can be very large and weak in IoT applications

- Three main attack categories specific to IoT systems
  - **Communication attack** over network or in IoT environment

    DoS, DDoS, spoofing, MitM, network injection, etc.
  - **Physical attack** through wired/wireless medium, or directly

    Reverse engineering, jamming, tampering, etc.
  - **Application/Software attack** issues on code

    SQLi, XSS, misconfiguration, etc.

Trust in IoT

- Trust in IoT can be divided into four different levels

  IoT user, application, network and physical layers

- Sacrifice for value is a big problem with IoT

  IoT device working for desired purpose and affordable is enough

- Three different security classes must be considered
  - **Privacy**: data about you can be collected by companies
  - **Availability**: must be available and powered to complete task
  - **Reliability**: transmitted and received data must be correct

Compliance in IoT

- Compliance is vital to security and security operations

  Help companies organising security operations

- Three different security classes must be considered
  - **Policy control**: typically regarding users
  - **Governmental oversight**: allowing them access to data
  - **Non-gov. oversight**: alliance, security professionals, etc.

References

- Douglas R. Stinson, & Maura B. Paterson, *Cryptography: Theory and Practice* (Fourth Edition), CRC Press, 2017. (ISBN: 978-1-138-19701-5)
- Syed Rizvi, Joseph Pfeffer III, Andrew Kurtz, & Mohammad Rizvi (2018). *Securing the Internet of Things (IoT): A Security Taxonomy for IoT*, 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications.

Credits

- Bob Mical, December 3, 2013, https://www.flickr.com/photos/small_realm/11189803153.
- Dennis Amith, December 17, 2012, https://www.flickr.com/photos/kndynt2099/8281891497.
- WeMake Milano, April 12, 2014, https://www.flickr.com/photos/wemake_cc/13848292804.