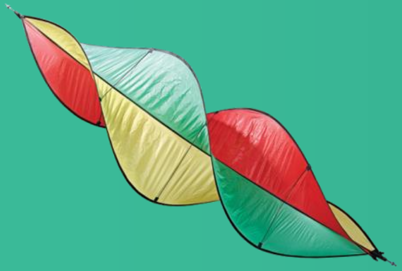
KU LEUVEN

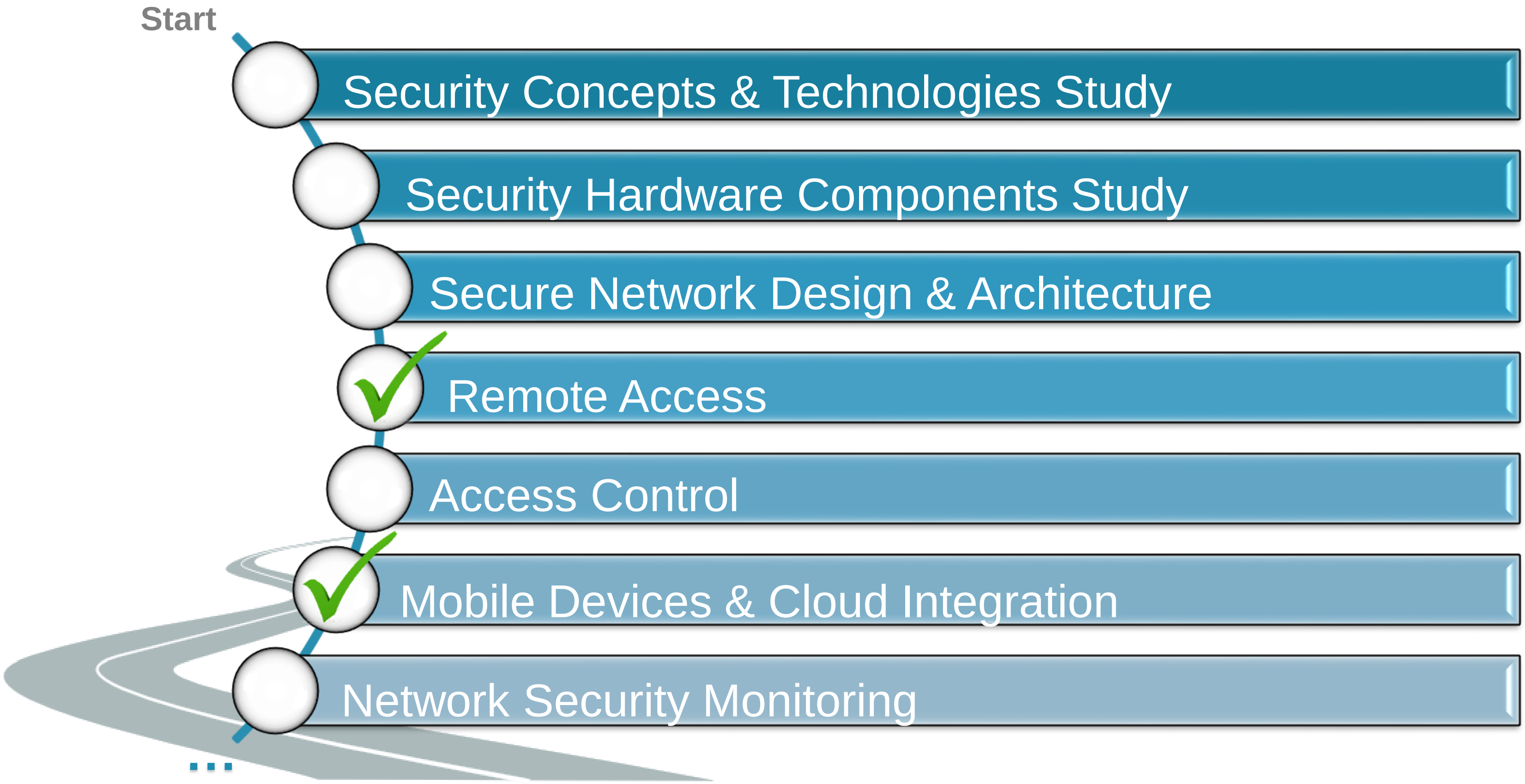
TECHNOLOGIECAMPUS GENT



Secure Remote Access to Control Systems Using Mobile Devices

Laurens Lemaire
Lisa Eggermont

Project Roadmap



Start

- Security Concepts & Technologies Study
- Security Hardware Components Study
- Secure Network Design & Architecture
- ✓ Remote Access
- Access Control
- ✓ Mobile Devices & Cloud Integration
- Network Security Monitoring

...

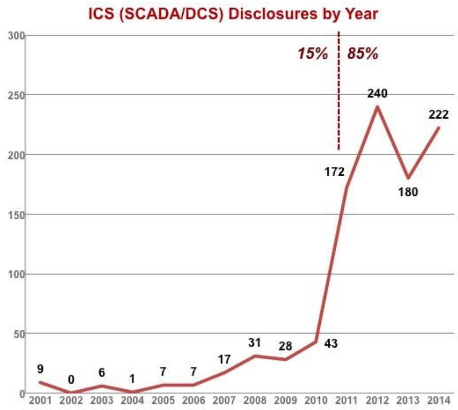
Problem Statement

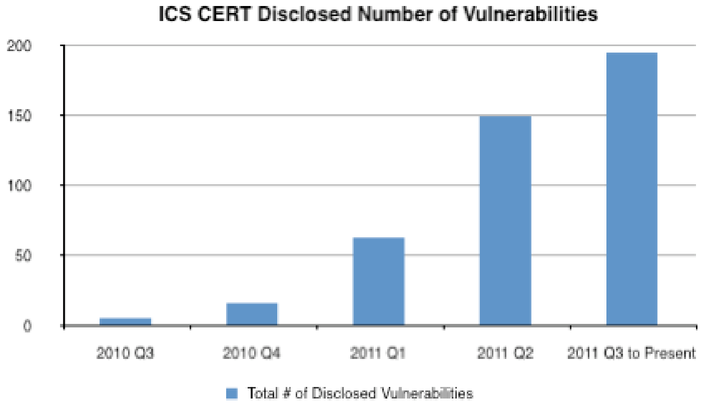
- Past:
  - Industrial Control Systems isolated
  - Security low priority
    - Sufficient to prevent physical access

- Present:
  - Evolution of IT affects ICS
  - Systems connected to company networks/internet
    - Easier to use
    - **Easier to attack!**

Problem Statement

- Several attacks on ICS in recent years
  - Stuxnet
  - Potentially disastrous consequences





Goal

- Design and compare different architectures for secure remote access of Industrial Control Systems
- Test one architecture on a real case study

Case Study

- iGenerator at Technology Campus Ghent
  - Burns rapeseed oil to generate electricity
  - Contains InteliLite NT MRS

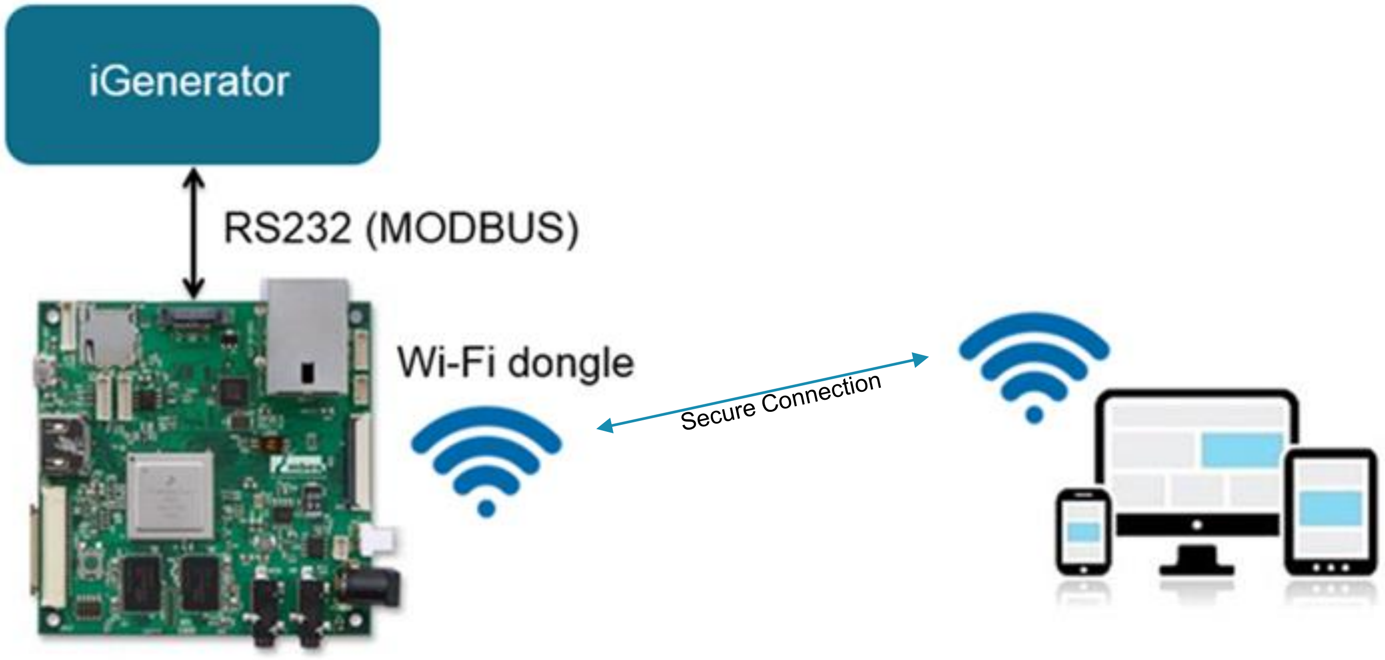
Case Study

- Company rents out iGenerator + Mobiles
  - Construction sites, festivals, …
- 2 User profiles:

	Manager	Employee
View parameters	✓	✓
Modify parameters	✓	✗
Start/stop iGenerator	✓	✗

Setup

- SABRE Lite development board
  - Jetty Server



Alternatives

- pfSense
- Industrial routers
- Cloud

- Role-based access control
  - Access restrictions to specific devices
  - No control over commands
- Requires external power source
- Default security
  - VPN
  - Industrial-grade firewalls

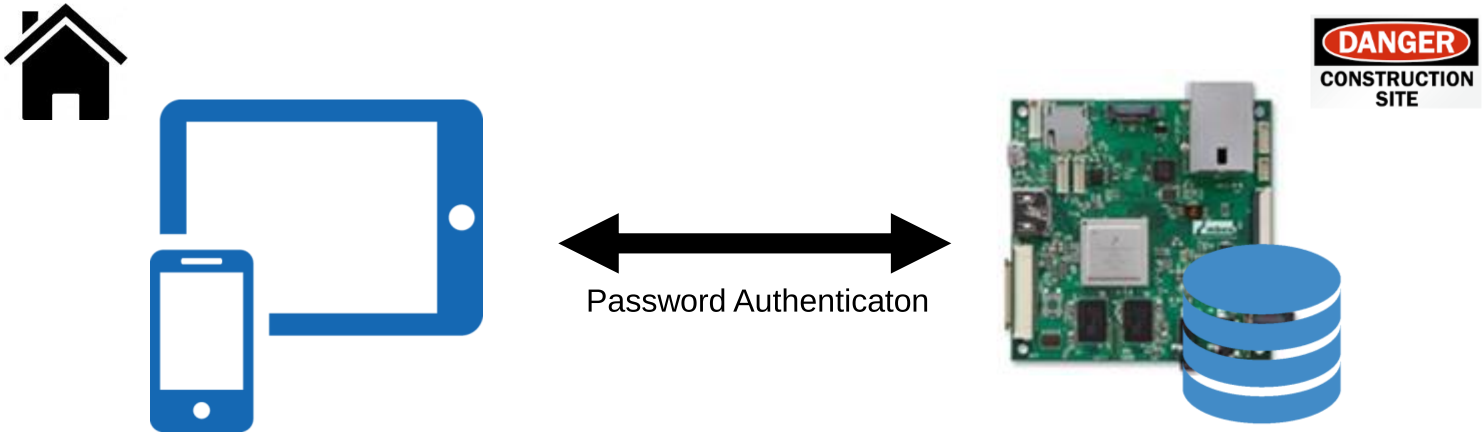
Evaluation Criteria

- Two factors
  - Security requirements
    - Authentication
    - Access control
  - Possible attacks
    - Attacks on the communication link (active and passive)
    - Database attacks
    - Social engineering

Design

- 4 Different approaches to achieve security

- Architecture 1: basic setup

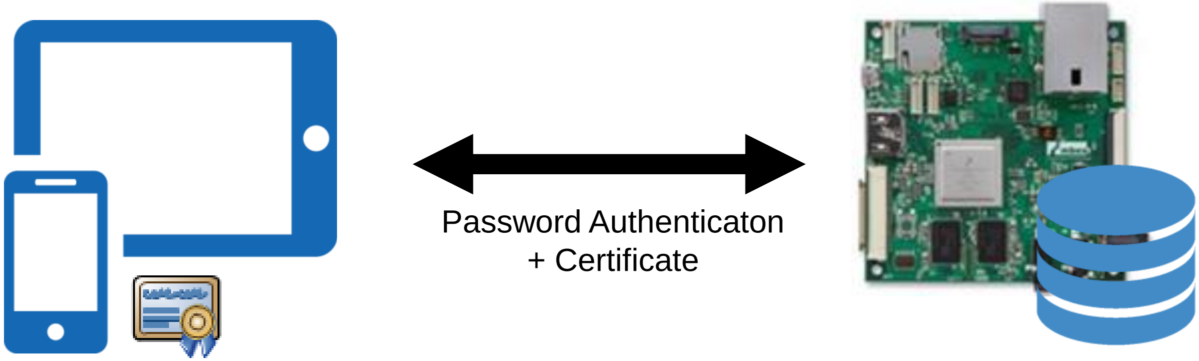


Password Authenticaton

- Password database maintenance
- Only user authentication
- Database/truststore easy to access for attackers

Design

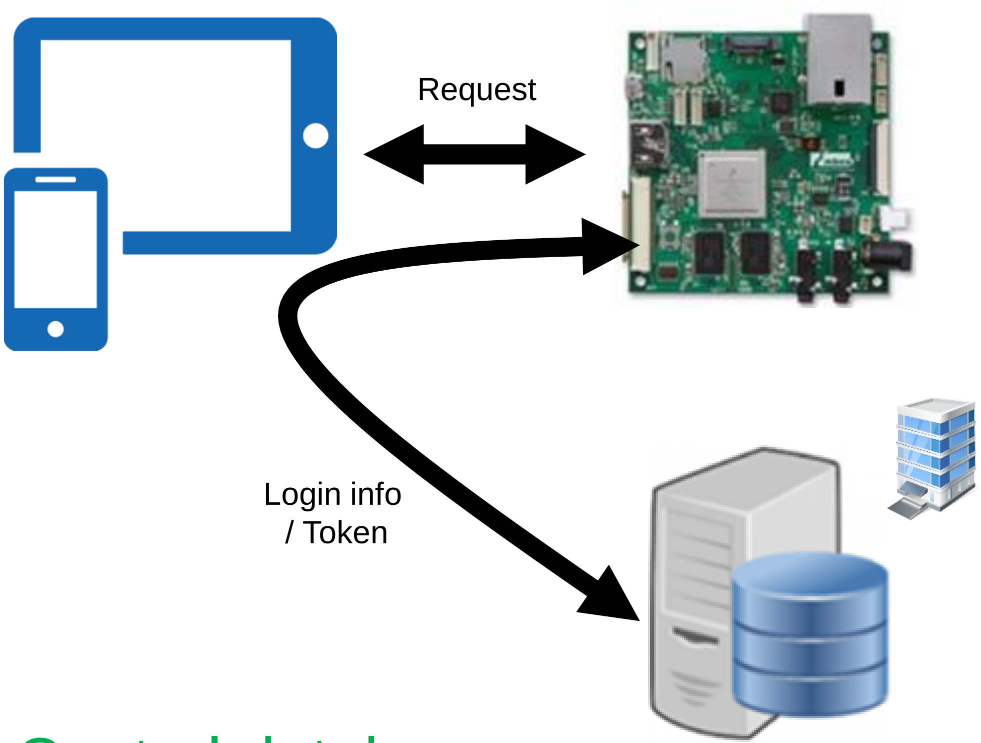
- Architecture 2: Device authentication



- Device + user authentication
- Password database/truststore maintenance
- Database/truststore easy to access for attackers

Design

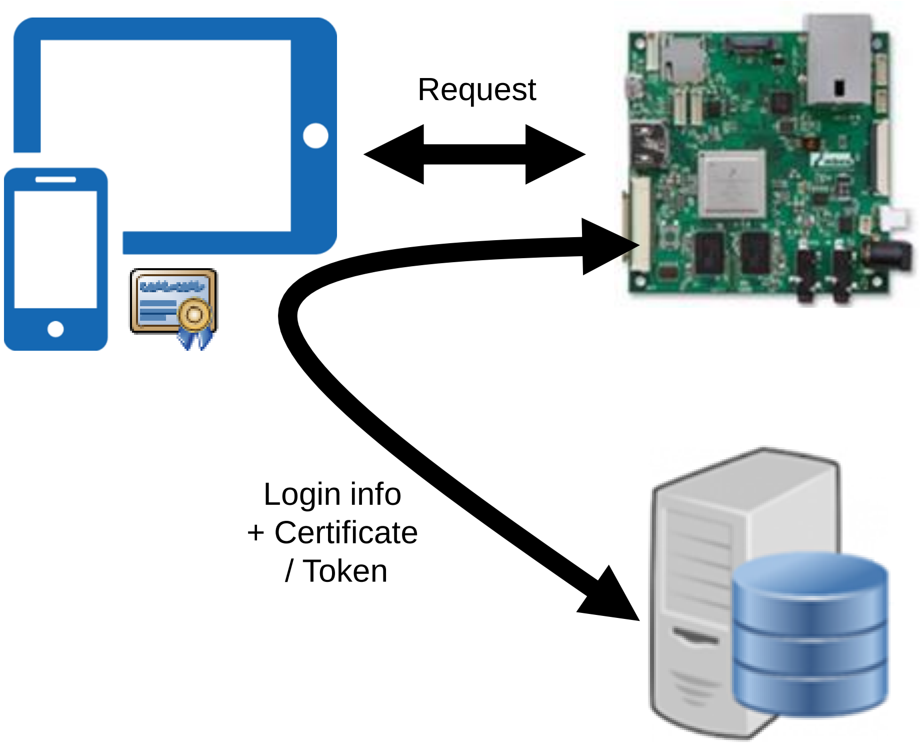
- Architecture 3: Authentication server



- Central database management
- Database harder to access for attackers

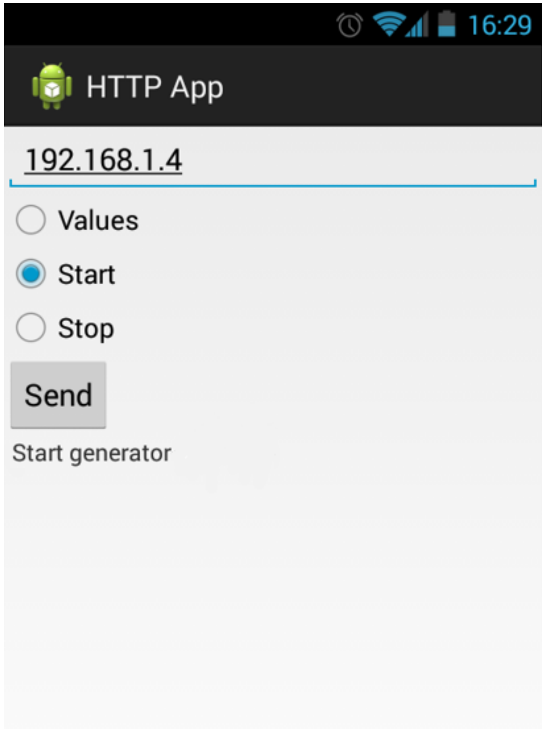
Design

- Architecture 4: Combination of 2 & 3



Implementation Prototype

- Implemented second architecture
  - Two parts: Basic setup & Security
- Basic setup:
  - Serial communication
    - Contacting iGenerator (C#)
    - C# → Java (JNI)
  - Jetty server
  - Android application



16:29

HTTP App

192.168.1.4

○ Values

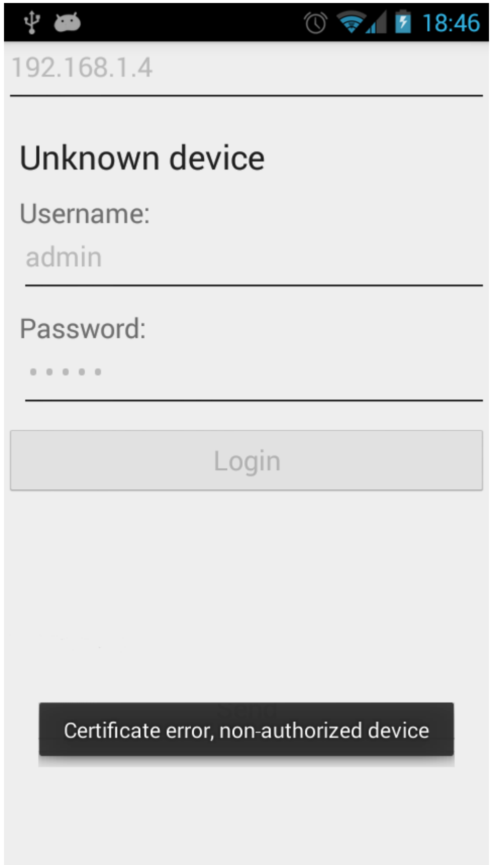
● Start

○ Stop

Start generator

Implementation Prototype

- Security:
  - SSL connection
  - User authentication
    - Hashed database with credentials
  - Device authentication



192.168.1.4

Unknown device

Username:

admin

Password:

•••••

Certificate error, non-authorized device

Conclusion

- Architectures for secure remote access
  - Embedded device
  - No VPN
  - One implemented: Device authentication

- Future work:
  - Replace Wi-Fi by 3G/4G
  - IP address?
    - Fixed IP SIM cards

Questions?