IN4253IN Applied Security Analysis

- The Hacking Lab Mantra:
  Take it apart and see how it works

- Small teams of 2-4 students
  Evaluate the security of a system, show the vulnerabilities and make it better

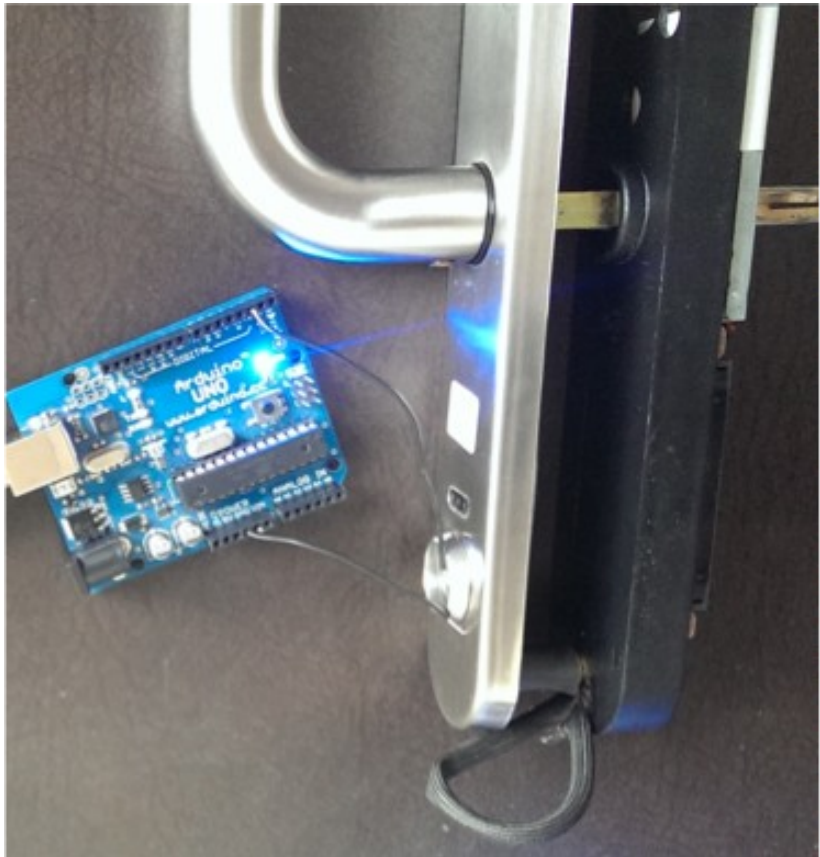
- Q3, but most students extend their project into Q4

TU Delft

IN4253IN Applied Security Analysis

Recent example projects:

Door Lock Security



TU Delft

IN4253IN Applied Security Analysis

Recent example projects:

Security and Supply Chains:
The Evil Networking Card

IN4253IN Applied Security Analysis

Recent example projects:

App Security

TU Delft

IN4253IN Applied Security Analysis

- Keep in mind:
  - **This is not a course on “how to hack”**
  - Instead of lectures, we will have weekly coaching sessions
    most of your time will be spent code analysis, programming, debugging
  - Crypto and (advanced) network security knowledge is recommended
  - Not easy (you will work on state of the art systems), but rewarding

ET4397IN Network Security

- 16 Lectures covering vulnerabilities and security practices of every OSI layer.
  - **Physical layer:** intercepting traffic on copper cables, fiber optics, wireless systems, satellite, microwave, building resilient topologies
  - **Link Layer:** Traffic hijacking, ARP, VLANs, MPLS, WiFi, telecom networks, port-based network access control (802.1X)
  - **Network Layer:** best practices security network design, switch design/attacks, threat intelligence, IP security, DNS/DNSSec, secure/covert tunnels, firewalls/diodes, routing attacks, intradomain security
  - **Transport Layer:** TCP attacks, TLS/SSL ecosystem, side-channels
  - **Application Layer:** NG-Firewalls, honeypots, botnets, real-time communication security
  - **System security:** meta-data analysis, anonymizing proxies

TU Delft

ET4397IN Network Security

- 16 Lectures with demos covering every OSI layer.
  - **Physical layer:** tapping into a copper cable, wireless systems interception
  - **Link Layer:** MITM, malicious GSM network
  - **Network Layer:** protocol specification attacks, poisoning attacks
  - **Transport Layer:** session hijacking, retrieving keys by side-channels
  - **Application Layer:** botnets, threat intel using TUDelft's telescope
  - **System security:** identify people through meta data, build a backdoor into a PRNG to decode SSL in real-time

ET4397IN Network Security

- Focus on concepts, no programming knowledge required
- Grading:

40% homework (conceptual questions)
60% final exam

OR

40% homework (conceptual questions)
60% mini project (software/hardware)

More information, list of content, tentative schedule on
www.networksecuritycourse.nl

TU Delft

IN4402 *Advanced* Network Security

- Advanced Network Security takes you down the rabbit hole
- Runs in parallel to Network Security and deepens the material
- We will
  - experiment in labs with networking hardware
  - look at vulnerabilities in detail
  - implement real attacks and write tools to defend against them
  - data-mine network traces to find the bad guys
  - run a red-team/blue-team cyber defense

Labs: Wireless signal interception and recovery, VLAN/STP attacks, DDoS attack mitigation, AES key recovery through network side channels etc.

IN4402 *Advanced* Network Security

- You need **strong** programming skills (self-score test online)
- Advanced Network Security is 10 EC, you follow the 2 lectures of ET4397IN, plus have additional in-depth lectures and labs
- After this, you know the security of networks inside out.

CS4120 Methods in Cyber Security

- Preparation program for MSc thesis
- Q3 and Q4, every two weeks

- Learn how to
  - Setup **your** MSc project
  - Design a suitable research question
  - Review of techniques for cyber security research

TU Delft