Cyber Security

Michael Sonntag
Institute of Networks and Security

MOTIVATION

- Cyber Security is getting important: Pervasiveness of IT devices
  - You car: It can be hacked (especially if it is autonomous!)
  - Your radio/alarm clock: Too late for work
  - Routers (Cisco): Zero-day exploits known for years by NSA, which got hacked and the problems were published
  - Cloud systems: Too many problems to list here!
- Important distinction: Routers/cloud are managed by professionals, which are (hopefully) able to rapidly respond to problems
  - But who is going to update the light switches (or the home routers: e.g. recently the default passwords of routers were shown to be trivially breakable)?
- Assumptions for smart homes/end users:
  - They are not security professionals
  - They won’t pay for use restrictions, potentially causing problems
  - They are unwilling to insure against damages to third persons

SOLUTION (?): AUTOMATING SECURITY

- Two fundamental issues:
  - Authentication: Who is it? Is it the persons claiming to be? Is someone there at all?
    - Note: For many end-users the “person” might be a device, as there is no longer exclusive human→ device interaction. Devices will interact with each other
      - E.g. allowing a drone to deliver a package inside the house, but only in the first room (opening door/window)
  - Authorization: We know who it is → Which permissions to assign?
    - What is a “guest” allowed to do?
    - Who (=security group!) is the boyfriend of the daughter?
- A matter of trust: Human → Device, but also Device → Device
- We can do this manually, of course, but who is going to do it?
  - Also note: For security we have false positive/negative problems
    - Unlocking the door: Very few false positives → many false negatives!

AUTOMATIC IDENTIFICATION

- Humans: Facial recognition, gait identification, fingerprint sensors, RFID badges/devices carried etc
  - Are we identifying the person (e.g. mobile phones do get stolen)?
  - Explicit interaction required (light switches/handles/knobs could integrate fingerprint sensors)?
    - Do we need signs notifying users of this (like video surveillance)?
- Devices: How can they be identified?
  - And what does that mean? Unique identity? Owner?
  - “Biometrics” at least in theory possible, e.g. small imperfections in production process; unchangeable long unique ids, …
  - Assigning IDs, distributing certificates etc: End-users are not going to do this.
    - One possibility “enrolment”: Once registering (simple!) is acceptable
  - Big problem: How to prevent devices from acquiring an arbitrary new identity?

AUTOM. ASSIGNMENT OF PERMISSION

- Technically easy, but who should received what?
- A suitable metaphor is needed, which also renders assignment (non-technically!) easy
- Various options:
  - Learning: Difficult for devices, constant feedback needed
    - In contrast to human children devices do not live long enough!
    - How to trust other devices to learn from them? Are their rules suitable for the new device (e.g. toaster → fridge)?
  - Central server: Registration is already needed for identification
    - With varying degrees of centrality: State, neighbourhood, household
  - Default fallback:
    - Everything allowed: Customers are satisfied, no security
    - Everything forbidden: Good for learning, customers are annoyed
  - Configuration by customers: Would they really know how/what?
  - Configuration by experts: Who will pay for this?

SUGGESTION: HOUSEHOLD METAPHOR

- Pre-configuration of devices according to a household metaphor:
- Pros:
  - Easily understood even by lay persons
  - Suitable for humans
  - Suitable for devices representing humans
    - They represent someone from a specific group
  - Preconfiguration by manufacturer possible
  - Sorting persons/devices into groups doable for non-experts
- Cons:
  - Not perfect security
    - Sometimes too many permissions
    - No perfect fit to standard groups for every device/person
  - Different according to society
    - A “household” in western Europe might differ from those in Asia
  - Difficult to improve security if desired
  - Standardization between manufacturers required

THE PERMISSION SYSTEM

- Permissions are kept simple, so users can understand them
  - They need not manually create rules, assign permissions etc, but they must be able to understand why something is allowed/denied!
- Four “permissions” exist:
  - Which roles (humans and devices) may receive data?
    - Someone is asking a device → Should it hand out the information?
  - Which roles can be represented by devices to obtain data?
    - Whom can the “fridge” impersonate? The owner (→ read calendar for expected guests) or a guest (→ ask for temperature/weather forecast)?
  - Which roles (humans and devices) may issue commands?
    - Requesting actions from devices → Who may do this?
  - Which roles may be represented by devices to issue commands?
    - Fridge: Owner (→ autonomously order food) or family (→ alarm because something nears expiration date)?
- Note: Devices “impersonate” humans and command other devices
  - Humans don’t impers. humans, devices don’t command humans

THE SMART HOME SCENARIO

- An example for the household metaphor
  - See e.g. the “fridge”: How to classify it?
    - Data production = “family member”
      - Only persons with role “family member” can retrieve data, but e.g. vendors or guests cannot
      - Why? Typically only “family members” would be allowed to inspect it!
    - Data consumption (=impersonation) = “family member”
      - Who is expected to be present, what food is planned, general environmental information (current supply, temerpature)
    - Accepting commands = “owner”, “utility provider”
      - Kids should not be able to turn it off or order lots of ice cream, but the smart meter may do the first
    - Issuing commands = “owner”, “family member”
      - For ordering supplies or adding diary entries for shopping
  - Problems: Child adds “party with 20 other kids” in calendar → fridge buys food, utility provider can turn it off (erroneously) and spoil the food, …

SYSTEM OVERVIEW

- Several roles are needed at least:
  - Owner: May do everything
  - Partner: Very wide permissions, but not everything
  - Family: Lots of commands, but privacy restrictions; may introduce other persons (→ guests) and devices (→ new things)
  - Medical doctor: Access to medical information
  - Craftsmen: Temporary physical access, detailed technical data
  - Utility provider: Permanent access but only electronically
  - Guest: Temporary physical access, use of general devices, but nothing private (= more command than data access)
- Devices can be preconfigured → Who may switch on a radio can be set in the factory (owner, partner, family, guest), with automatic individualisation of roles
  - The “family” in house A is similar but not the same as in house B
- Only assigning persons to roles needs to be done individually

IMPLEMENTATION

- What is needed technically?
  - Identification of users: Username/password on devices + tracking their movement, carried devices, explicit (fingerprints) or partial/implicit identification (TV child protection code), obtaining from other devices
  - Identification of devices: Public/private key cryptography
  - Central server for directory of devices, persons, and their roles: May be replicated to all devices (few&slow changes), including the permissions (all or only applicable ones)
  - Standardized communication between devices
- Organizational requirements:
  - Enrolment of devices upon “installation”: pairing to central server
  - Assigning unknown persons to groups (easy) and their identification assets (more difficult)

SUMMARY AND OUTLOOK

- While the approach presented will not produce perfect security, it is still much better than the current state of potentially very good, but actually nonexistent security
  - Focus on acceptability and understandability
- Requires extensive communication between devices, as not every device has a UI for identifying persons (and users wouldn’t like this)
  - Restriction possible: Devices only, and humans can do everything
- Based on a central server, but could work without, if permanent and reliable communication to several other devices is available
  - Pairing to one device, distribution to others
    - Probably just a question of a few years!

- Realization chances?
  - Technically not that difficult, but standardization is an issue

JOHANNES KEPLER
UNIVERSITÄT LINZ

INSTITUTE
OF NETWORKS
AND SECURITY

https://www.ins.jku.at

THANK YOU FOR YOUR ATTENTION!

Michael Sonntag
michael.sonntag@ins.jku.at
+43 (732) 2468 - 4137
S3 235 (Science park 3, 2nd floor)