Smart-home Security

Michael Sonntag

September 2015

INSTITUTE
OF NETWORKS
AND SECURITY

JKU
JOHANNES KEPLER
UNIVERSITY LINZ

Smart Homes

- What is a “Smart Home”?
  - Not merely replacing AC wires by a bus system
  - “Activities” can be combined: Switch A results in several results, e.g. dim lights, close shutters, switch on TV
  - Autonomy: Some things happen “on their own”
    - Depending on the weather forecast (or simply date & time) heating, ventilation, shutters etc are controlled and regulated
    - Simulation of persons during holidays
- Reality: Smart homes are currently very dumb
  - Everything has to be pre-defined in detail
  - Few combinations and very little autonomy
- Still, even not-so-smart homes can be helpful!
- But potential problems exist too: Privacy, security, lifetime, safety etc

Attacker model

- To secure something we must know what/whom to secure it against: Knowledge, resources, capabilities…
- Attacker model for smart homes (private houses/flats):
  - Complete knowledge of:
    - Model & manufacturer of all elements, their properties and functions
      - Observation, datasheets available, easy to be bought
    - Limited knowledge about placement and interconnection
      - Observation, public plans, presumptions (“useful”, accepted approaches etc)
    - All devices are commercially available; internal hardware modification/replacement possible; adding devices possible
      - Just buy & modify and place them, e.g. as a guest
    - Access to the communication medium: Wires, radio transmissions
      - “Evil maids”, external devices, incomplete shielding
  - Assumption: Whole system under control of a single entity or completely separated
    - Potential problem: Door communication in multi-tenant homes

Security elements: Physical, Power

- Physical elements: Important, but often impossible
  - Some devices are outside; if they contain a key, it can almost always be extracted or “transplanted” to another device
  - Evil maid and guests can add devices on the inside too
  - Result:
    - Tamperproof hardware, at least for keys (→ chipcards)
    - Security may not depend on “no physical access”
- Power: What happens in case of a power failure?
  - Some things will not work; e.g. UPS for central system, but for all external devices too? Externally accessible → Bleeding it!
  - Startup state and transient states: How will devices be configured (default= off → alarm systems?) or react (e.g. open&close fully for end position detection!)?
  - Partial power loss? Central server has longer boot time!
  - Result: Indiv. configuration of startup state and power-off state

Security elements: Keys, Interconn.

- Password/Keys: Distribution&assignment is difficult
  - Typically keys are "built-in" in the hardware
    - Getting hold of the device → Key is accessible!
  - Even if custom keys are distributed, they can be extracted
    - Chipcards don't help → They could be switched to another device!
  - Key rollover: Communication black-outs, interruptions etc.
- Interconnection security: Many vendors/items
  - Conflicting standards, often also varying communication means
  - Everyone can talk with everyone? Or one central instance?
  - Some elements are less secure → Reduced security for whole?
  - Example of gas meter command released into the electricity meter network → Whole Austrian Grid was endangered!
- Updates: Smart-phones are updated rarely, but they "live" only 24 month. Smart-home: 10-20 years!
  - And who is going to update his 20-50 "light switches"???

Security architecture requirements

- Star architecture: Central server with “sensitive” data/full control + “dumb” devices (→ compromise “harmless”)
  - No distribution → Single point of failure (DoS attacks)!
  - Simpler trust: Device know the server; server knows everyone
  - Reachability: Every device must be able to communicate with it
    - Signal strength, repeaters, mesh networks, …
  - No broadcasts: Source authentication
    - Breaking one device gets access to this device and its capabilities only
  - Reliable bidirectional communication: Acknowledgement
    - Prerequisite for useful encryption&authentication! Else: Delay, replay, DoS
  - Intranet/Internet reachability: View/Control from afar; updates
    - Strong separation and secure communication needed (enc. + sign.)
    - Connections between buildings/locations
  - “Translation” service: From one system/manuf. to another
    - Avoids N^2 translation requirements!
    - Includes architecture translations (distributed like KNX)

Security model for smart-homes

- Currently: Installed by professionals; “one system”
- Future: Self-installed/non-experts
  - Mixed elements over time (extensions, replacement)
  - No professional “maintenance” can be expected
- Security functionality needs to be integrated
  - Currently available for professional & expensive (KNX) system: Data logger, blocking obviously incorrect/unknown addresses, preventing reprogramming of devices
  - Nothing “serious” like a firewall/IDS is commercially available
- Security must be self-configuring (non-experts!)
  - “Learning mode” for one day/week with assumption “secure”
  - Feedback by users: “intentional” → later modifications, erroneously learned; but user mainly think “I want it to work”
    - Multiple levels of response: Taking note, increased observation, warning, request/wait for human repeat, blocking

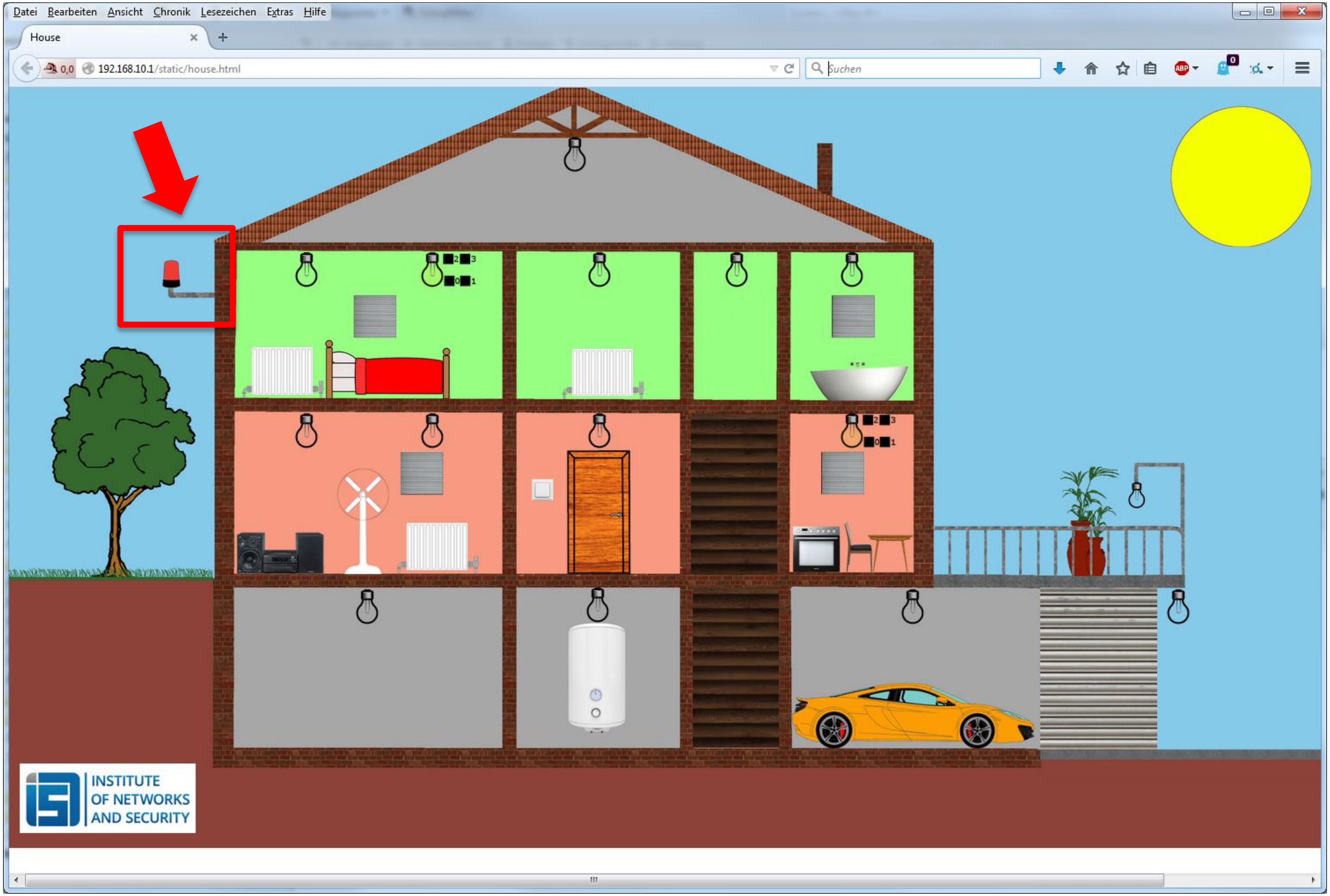
Intrusion detection

- Becomes useful with a central server → Located there
  - Access to all of the various communication mediums
  - Complete knowledge of the system, as every command goes through here (problematic with distributed systems!)
  - Receives every sensor value/command issued → Holistic view
- Requires (but also produces!) a system documentation
  - What exists, how they communicate, when are they active
- Typical problem of IDS: False positives
  - Here the environment is extremely static and usage is regular
    - If nobody is at home, switches don't send commands
  - Changes lead to alarms → Update of the "documentation"
    - Important for changes to be incremental (no replacement) to avoid having to relearn everything
    - May also integrate "lost" (e.g. replaced) devices → removed from config.
- Note: IDS will not protect against spying (=passive)!

Intrusion detection: KNX example

- For the home-automation system OpenHAB an IDS for KNX was developed at the institute
  - Not on the “Internet” side, but directly for the KNX bus
  - At the moment: Explicitly defined definitive problems are recognized (= already more than commercial systems do!)
- Currently in progress: Learning mode
  - “Static” mode completed: Comparison to “abstracted” past
  - “Dynamic” mode: Learning combinations of events
    - When A than B: B without A → suspicious; A without B → Error/attack
  - Problems:
    - Activities depend not only on commands, but also lots of external data (example: Person A at home = Light on → depends on the time of the year and the weather too!)
    - Many things are extremely regular (e.g. heating), but everything involving humans is more unpredictable. Still quite good, but “rule chains” have to start with human actions and end “sometimes later”

KNX example: Visualization



Conclusions

- Smart-Homes are a bit earlier than cars today: Features are built in without security, and because of public hacks expensive retro-fitting has to be done
  - Increased responsibility of manufacturers would improve the situation, but this would require world-wide regulation
- Until then (so probably for a long time ☺):
  - Add security devices on the “outside”, e.g. Internet connection
  - Add security to inside devices, esp. central servers
  - When designing new systems/extensions: Make sure that security is at least possible, if not built-in by default
- Insurance companies: Require official certification or licensed technicians or no compensation if this at least contributed to the damage

Thank you! Questions?

Thank you!

Any questions?

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

INSTITUTE
OF NETWORKS
AND SECURITY
https://www.ins.jku.at