RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Internet of Things... Promising but Let's Not Forget Security Please!

SESSION ID: STU-M05A

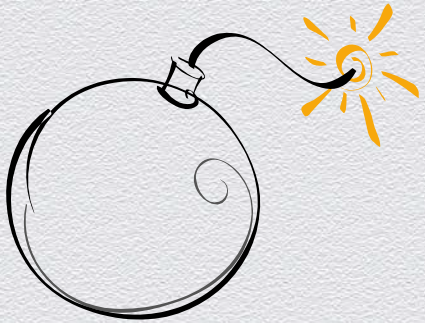
Eric Vyncke
Distinguished Engineer
Cisco
@evyncke

RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

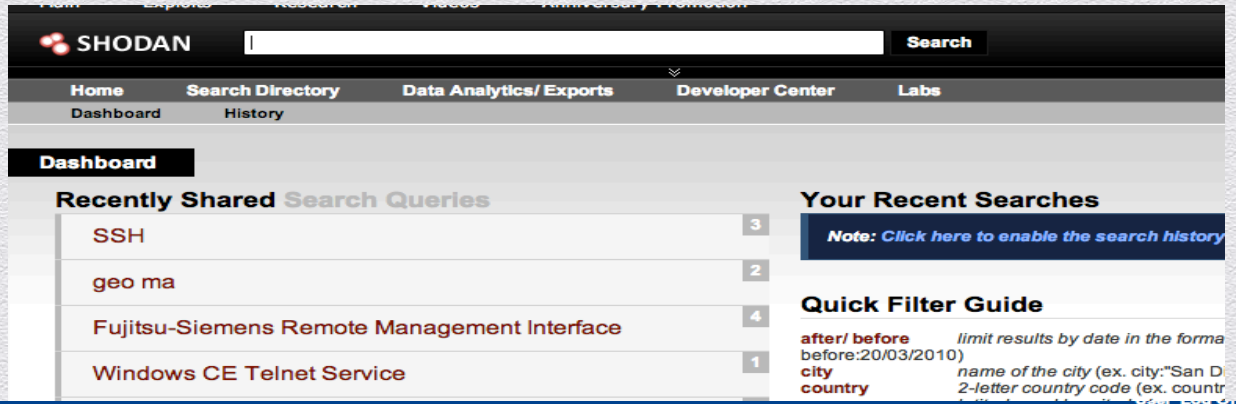
Internet of Things: Threats

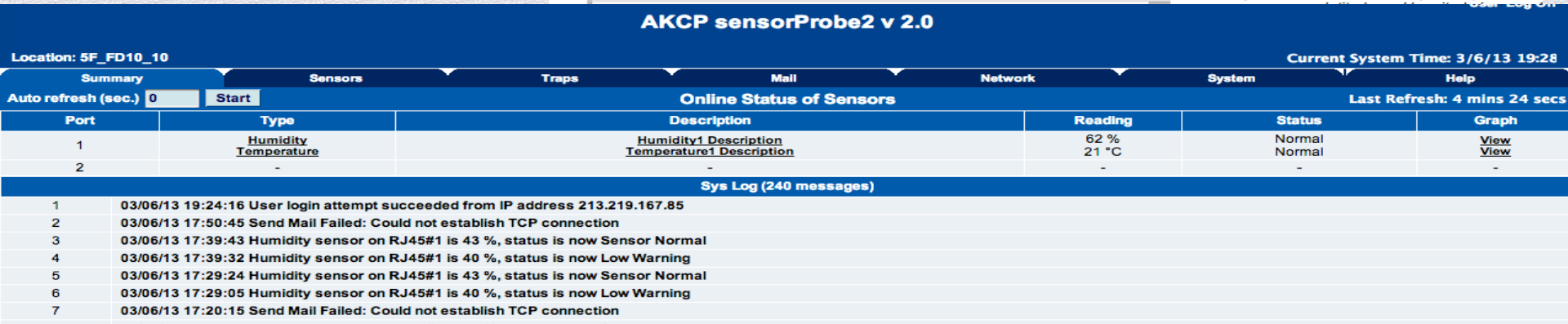
What are the threats?
Too many of them

- Plain worms escaping the plain IT world into the IoT?
  - Limited to ‘things’ running a consumer OS: Windows, Linux, iOS, Android, ...
- Script kiddies or other targeting at random residential IoT
  - Unprotected webcams
  - Stealing content
  - Having ‘fun’ with heating system
- Organized crime
  - Access to intellectual property
  - Sabotage and espionage
  - See also further
- Cyber-terrorism
  - Against nuclear plants, traffic monitoring, railways, ... (critical infrastructure)



Shodan





- http://www.shodanhq.com/ a IPv4 scan of the Internet
- Do not believe that IPv6 will help....

Risks to Industrial Control Systems

Application of Security patches

Natural or Man-made disasters

Worms and viruses

Theft

Sabotage

Safety

Denial of Service

Unauthorized access

Unauthorized actions by employees

Unauthorized remote access

Unintended employee actions

Unaddressed risks increase potential for disruption to control system's uptime and safe operation

Privacy even for residential

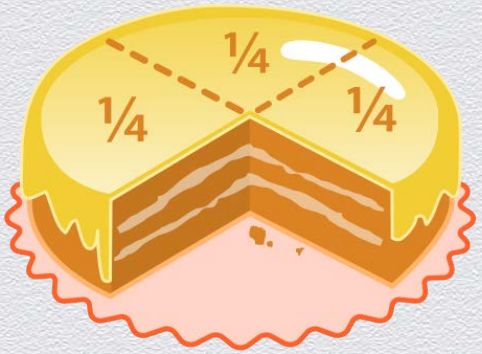
- Example: smart metering
  - Using this example simply because it is easy to understand, deployed and could be fixed (if not yet done)
- In case of unauthorized access:
  - Less consumption as usual => nobody at home, let's break into it!
  - 5-min interval consumption meter => can guess the TV channel!
  - http://events.ccc.de/congress/2011/Fahrplan/events/4754.en.html

Source: wikimedia.org

RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

A System Approach to IoT Security

System Approach to IoT Security?



Source: wikimedia.org

- Too many IoT to do security analysis for all use cases
- Let's cut the big cakes in smaller edible pieces
- Let's focus on generic properties of IoT
  - Property can be: mobile vs. fixe, tamper-proof
  - And derives threats on each properties
  - Then, design mitigation techniques or risk managements (work in progress...)

Lifetime: cost vs. crypto resistance

- Example: smart metering?
  - How old it your house?
  - How old is your electricity meter?
- Compare with lifetime of DES
  - 1977: published by US FIPS
  - 1999: EFF breaks it in 22 hours
  - 2005: removed by US FIPS
  - Guess: crypto has a limited lifetime of 20-30 years...
  - Compare with above...
- Even public key cryptography could be defeated with quantum computer...
  - OK, not within 10 years probably
  - Search also for ‘post quantum cryptography’

Source: wikimedia.org

Device identity vs. group membership?

- Any can handle access control
- Device identity/authentication
  - Smart meter to get your own bill
  - Actuators (and even)
  - Smart vehicles
  - But, scalability issue...
- Group membership
  - Array of sensors for physical environment, what is important is location not individual identity
  - Actuators: all bulbs in the same room
  - Easier to scale

Multi-Party Networks...

- Use case: smart metering, home surveillance, ...
  - Where the residential network (operated by SP/subscriber) is shared
- Availability?
  - Quality of Service is an obvious must
  - VLAN separation can also help
  - But shared/unmanaged CPE???
- Threat: Man-in-the middle attack to be assumed
  - Impact on confidentiality & integrity => crypto could help
- Provisioning? Vendor? Service Provider? Owner?
- Liability?

Mobility

- If a ‘thing’ is mobile, then it can be moved maliciously, i.e. stolen
- If a ‘thing’ is fixed, then a move could still be physically possible but undetectable

- Pick your devil!

Source: wikimedia.org

Always on?

- Always on:
  - Removal/loss detection is immediate
  - High rate of poll makes man-in-the-middle more complex
- Periodic poll:
  - Wait until next poll before detecting removal/loss
  - Balance between cost/energy and security
- On-event push:
  - Removal/loss detection is impossible

Source: wikimedia.org

Wisdom of the crowd

- Assuming cheap ‘things’, then one lost thing is not a major issue
  - Loss in the sense of physically destroyed (availability) or owned (integrity)
  - Averaging the surrounding sensor measurements (temperature, ...)
  - Could also be applicable to actuators such as parallel electrical switch
  - Proven technique: using 3 ‘things’ and using a majority vote on the outcome. The voting system could be sheer dumb electronics

Summary

Summary

- IoT is a broad term covering
  - Different vulnerabilities: software, crypto, can be stolen, ...
  - Different risks: national critical infrastructure vs. home heating system
- Let's be pragmatic and cut the problem is smaller pieces
- Work in progress ☺, not all solutions are available yet
  - This is normal
  - Let's focus on the problem statement first

- What can we trust in Internet of Thing?
  - The network that we know or things to be built?

Thank You