

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

Distinguished Engineer
Cisco
[@evyncke](#)

Eric Vyncke

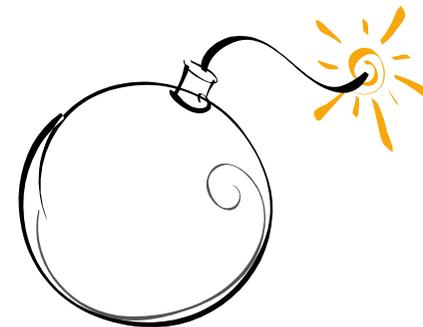
Internet of Things: Threats



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

The screenshot shows the Shodan website dashboard. At the top, there is a search bar with the Shodan logo and a search button. Below the search bar is a navigation menu with links for Home, Search Directory, Data Analytics/Exports, Developer Center, and Labs. The main content area is titled "Dashboard" and features a "Recently Shared Search Queries" section with two entries: "SSH" (3) and "geo ma" (2). To the right, there is a "Your Recent Searches" section with a note: "Note: Click here to enable the search history". At the bottom right, there is a "Quick Filter Guide" link.

The screenshot shows a network management interface. At the top, there is a header with "Location: 5F_FD10_10" and "Current System Time: 3/6/13 19:24". Below the header is a navigation menu with links for Summary, Sensors, Traps, Mail, Network, System, and Help. The main content area is titled "Online Status of Sensors" and contains a table with the following data:

Port	Type	Description	Reading	Status	Graph
1	Humidity	Humidity1 Description	62 %	Normal	View
2	Temperature	Temperature1 Description	21 °C	Normal	View

Below the table is a "Sys Log (240 messages)" section with a list of log entries:

- 03/06/13 19:24:16 User login attempt succeeded from IP address 213.219.167.85
- 03/06/13 17:50:45 Send Mail Failed: Could not establish TCP connection
- 03/06/13 17:39:43 Humidity sensor on RJ45#1 is 43 %, status is now Sensor Normal
- 03/06/13 17:39:32 Humidity sensor on RJ45#1 is 40 %, status is now Low Warning
- 03/06/13 17:29:24 Humidity sensor on RJ45#1 is 43 %, status is now Sensor Normal
- 03/06/13 17:29:05 Humidity sensor on RJ45#1 is 40 %, status is now Low Warning

The screenshot shows a network thermometer interface. The title is "Ethernet Thermometer (Left)" with "s/n: 12941653". The main display shows "Channel 1" and "23.4°C alarm none". To the right of the main display are four buttons: "History .CSV dot", "History .CSV comma", "Mobile web", and "Refresh page".

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

Risks to Industrial Control Systems



Risk to Human Beings

- Implantable Medical Device (such as pacemakers)
- *former Vice President Dick Cheney revealed that his doctor ordered the wireless functionality of his heart implant disabled due to fears it might be hacked in an assassination attempt.*
- *The late Barnaby Jack demonstrated how a certain model of implanted insulin pump could be lethally hacked to administer incorrect dosages from up to 300 feet away.*



<http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheney-s-heart/>

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>

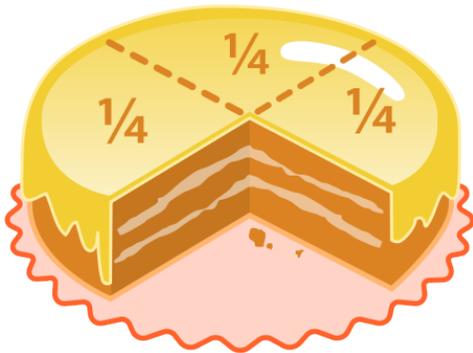


Source: wikimedia.org

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 is your house?
 - How old is your electricity meter?
- Compare with lifetime of DES
 - 1977: published by US NIST
 - 1999: EFF breaks it in 22 hours
 - 2005: removed by US NIST
 - 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](https://commons.wikimedia.org/wiki/File:Rotary_telephone.jpg)

Identity: pre-shared keys are back...

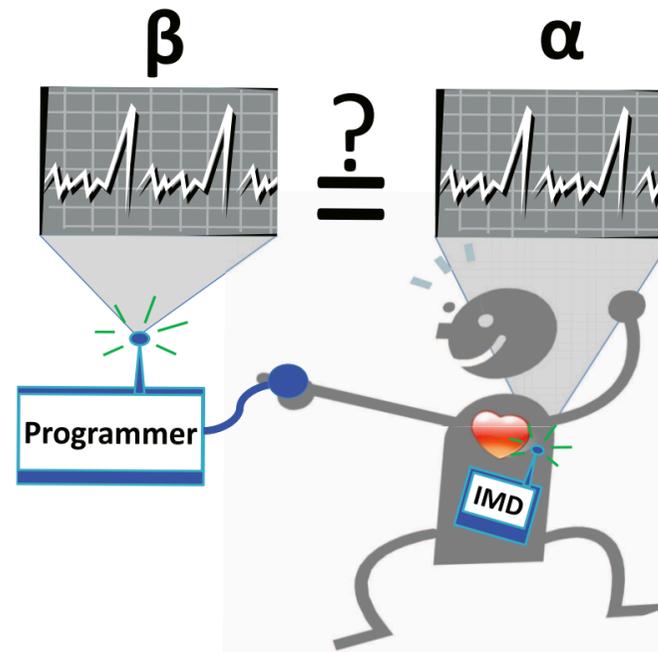
- X.509 Certificates and Public Key Infrastructure
 - Relies on cryptography (see previous slide)
 - Requires a long-term established Certificate Authority
 - Suitable for any to any authentication
- Pre-shared keys
 - Suitable for pre-defined authentication (such as meters to server)
 - Well understood

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

Identity or Proximity?

- Sometimes, no need for real identity of peers
- Heart-to-Heart protocol to give programmatic access to Implantable Medical Device
- Sharing a common physical measurement with enough entropy is enough
- Can also be done with radio wave parameters



<http://www.arijuels.com/wp-content/uploads/2013/09/RJK131.pdf> (Ari Juels & Rice University)

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 (or SDN even?)
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, but can still know its new position
- If a 'thing' is fixed, then a move could still be physically possible but undetectable
- Pick your devil!



Source: [wikimedia.org](https://commons.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

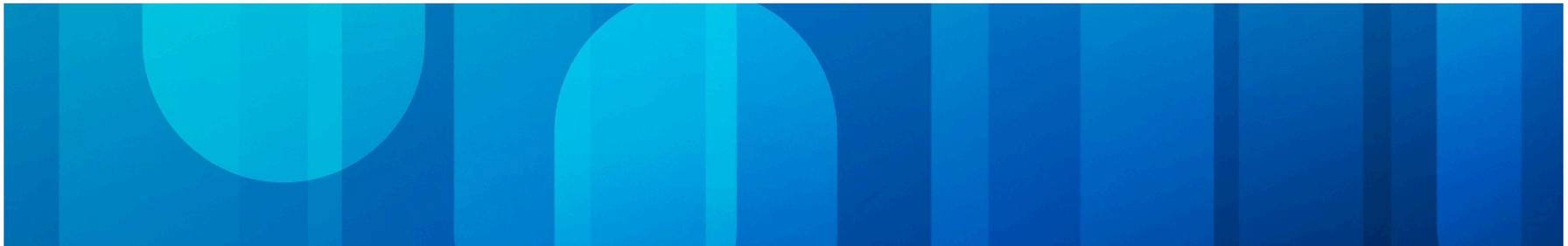
Wisdom of the crowd



- 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
- Example: IoT Grand Security Challenge
 - <http://blogs.cisco.com/security/join-the-challenge-secure-the-internet-of-things/>
- Work in progress 😊, not all solutions are available yet
 - This is normal
 - Let's focus on the problem statement first
 - Solutions exist for specific IoT use cases (smart metering, ...)***
- What can we trust in Internet of Thing?
 - The network that we know or things to be built?

Thank you.

