ERNW
providing security.

IoT IT Security and Secure Development Life Cycle

Security BSides Ljubljana, 2015

By Christopher Scheuring, ERNW Germany

/whoami

- Christopher Scheuring
- Security Analyst @ ERNW
- Since 2010 IT Security Architect and Analyst
- Before: 8 years software development
- Email: cscheuring@ernw.de

ERNW GmbH

- ERNW provides vendor independent security services to support our customers' business.

- Established 2001
- 35 employees
- Vendor Independent
- We understand corporate
- Deep technical knowledge
- Structured (assessment) approach
- Business reasonable recommendations
- Customers predominantly large/very large enterprises

Agenda

- The Big Question:
  IoT – how secure we are?

- IT-Security in IoT – we need it!
- The SDLC and IoT - and why it becomes difficult.
- The challenges and problems with IoT.

ERNW
providing security.

What IoT means – what do we talk about?

IoT

- Internet of Things
  - Sounds cool ;-)
- Other Buzz Words
  - Industry 4.0
  - Connected Cars
  - Smart Home
  - Cloud Apps
  - Yadda-yadda-yadda

IoT – The Idea

- Everything becomes accessible from every where.
  - Your fridge generates the shopping list.
  - Systems detect wear and tear to order new parts.
  - Robots order 3rd party parts for the next product they will build.
  - Your smartphone switch of the lights or open your home door.
  - Cars tell other cars the current traffic situation and control the traffic flow.

IoT – The Problems

- Everything becomes accessible from everywhere which means:
- Everything **needs** to be connected to the Internet at any time:
  - Your smart TV (with smart cam)…
  - Your home automation with door-opening-capability…
  - Your car with GPS so you could find it easier or open doors remote…
  - The industrial system to interact with 3rd party partners – perhaps in booth direction…
  - -Yadda-yadda-yadda ;-)

IoT – The Real Live

- Did you ever pentest or perform a security analysis for “IoT” devices?
  - Smart home components
  - Industrial components (robots, switches, welding machines, sensors and actors…)
  - Cars (inside buses or the GSM connectivity – think about WiFi)
  - The network infrastructure
  - Your smartphone…
- If yes – you know how secure they are!

IoT – What we're Talking

- We are talking about systems designed to work in an autonomous and secure environment.
- The communication infrastructure origin was designed for safety and availability (like RS486, Fieldbus, CAN…)
- No needs to secure theme in an IT-Security point of view.
- They are secure by dedicated connection matrixes.

IoT – Becomes Real Live

- Those systems now are connected to the Internet or company WANs.
- By just applying TCP/IP interfaces.
- Following the rapid development needed for IoT.
- And forgot the IT Security needs…
- Systems designed for an autonomous and secure environment become reachable all over the world.

Why SDLC becomes important for IoT

SDLC

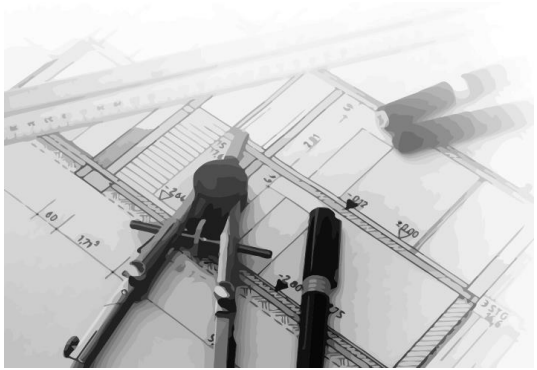
Secure Development Life Cycle

- Is the inclusion of IT security belongings into the (software) Development Live Cycle.
- Focus is checking:
  - Company policies
  - Legal requirements
  - Technical IT-Security requirements
  - Efficacy of security measures

IoT and SDLC

- Let's talk about IoT and SDLC.
- E.g. a small and cute home automation system.
- Something really everyone needs because we can do it:
  - Check our temperature and window stats by our smart phone.

Our Design



- Cool and smart mobile app – very important!
- Using whatever cloud service for data exchange – because it's easy to develop.
- Cheap and easy programmable hardware (like an Arduino – its cool for developing smart projects).

Our Infrastructure

- Seems to be isolated – everything is inside our home.
- The only connection to the world is by a **dedicated one way** communication to the cloud service.
- Our smart phone only talks to the cloud service end displays the temperature and state of the windows.
- Everything is fine – implement it :-)

Our Project Goes Live

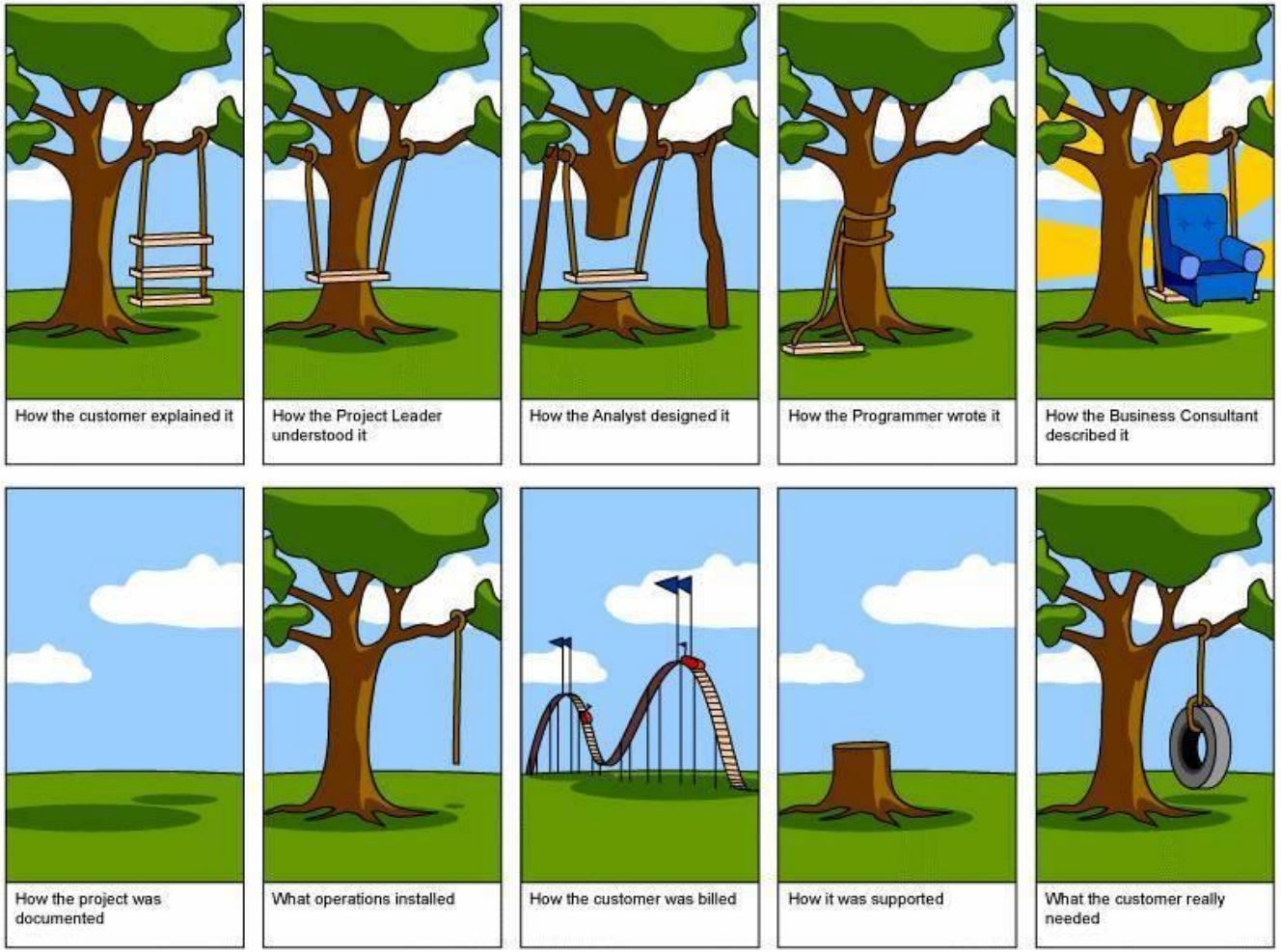
- Cool Arduino with a real cheap WiFi module, temperature and window sensors (costs some less EURs).
- Easy software development because there are a lot of cool stuff available from the internet (GPL or free).
- Finding a usable cloud service is also an easy step.
- Rapid development in real live: Everything works after 1,2-3 days.

Our Project Grows...

- We feel like the king of the hill.
- Eyes glow and new ideas are sparkling:
  - Open the front door.
  - Change the temperature.
  - Switch the lights.
  - Yadda-yadda-yadda
- And control all cool features by smartphone.
- OK – you turn back to a child... ;-)

Small IoT RL Excursion

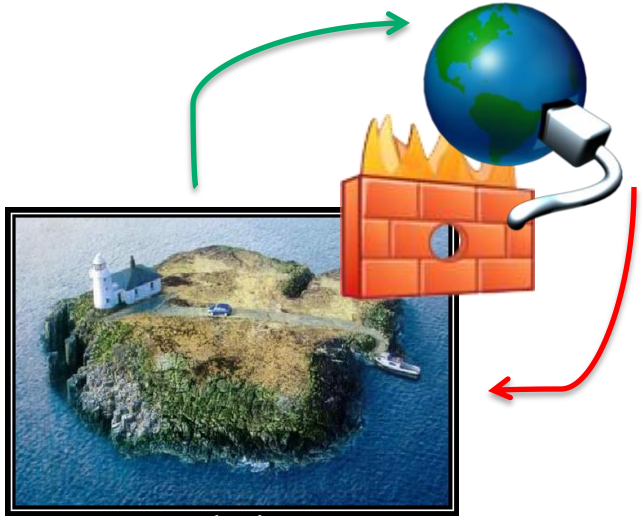
- The guys selling the IoT / smart home application feel like king of the hill.
- Eyes glow and new ideas are sparkling:
  - Open the front door.
  - Change the temperature.
  - Switch the lights.
  - Yadda-yadda-yadda
- And control all cool features by smartphone.
- OK – they got Dollar signs in the eyes… ;-)



ERNW
providing security.

Keep in mind the real live of software development ;-)

What Now Happens…



- Your isolated environment gets connected to the world – in both ways!
- The origin design was only specified for a one-way connection initiated from inside your isolated environment into the Internet.
- Your concept becomes broken in a view of security point…
- Your now need a back connection…

Unfortunately…

- Point of view sales man:
  - What's the problem?
  - You could open your front door even if you forgot your key at home!
- You remember the BMW hack?
  - Maybe some one could get access to your home – unauthorized caused by a bug?

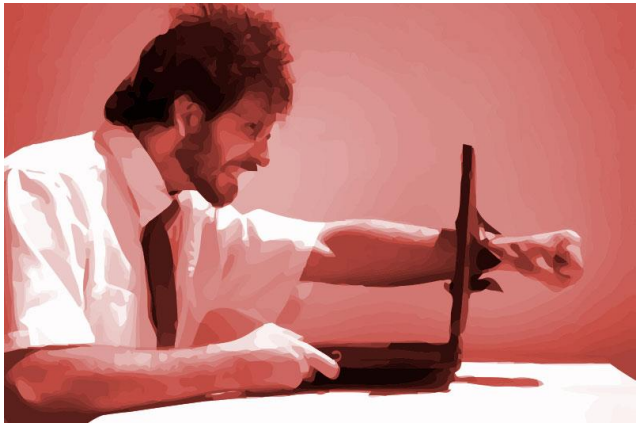
ERNW
providing security.

Here we go and deal with the new challenge.

IoT & The Challenge

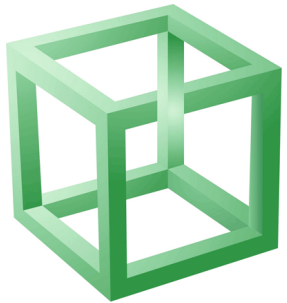
- Changing our way of life using IoT also means knowing the threats.
- And (possible) vulnerabilities caused by new connectivity and being connected every time.
- And therefore it's very important using SDLC measures in the early project phase.
- Think about what would be the unbelievable feature and include it into your SDLC process :-)

The Threats



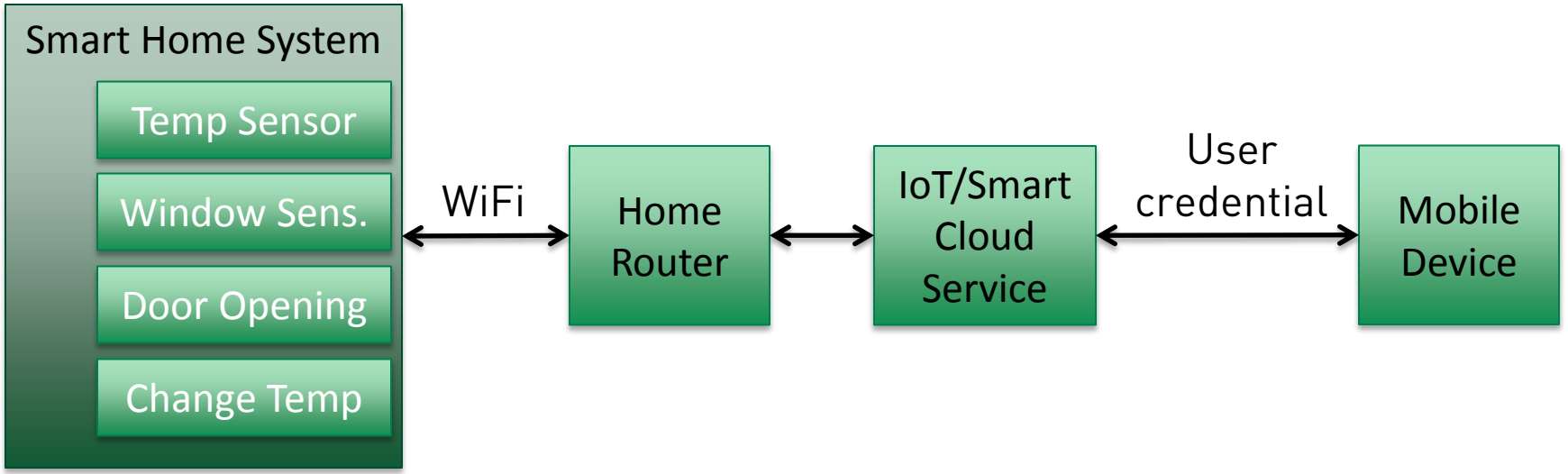
- Surprise – the already known ;-)
- E.g. STRIDE
  - Spoofing user identity
  - Tampering Data
  - Repudiation
  - Information disclosure (privacy breach or data leak)
  - Denial of service (DoS)
  - Elevation of privilege

Our IoT Project



- It was designed to use in ideal world.
- After enhancing we need to check for possible/new threats.
- And if there are any vulnerabilities concerning to the threats.
- This will be a security analysis process inside the DLC => Secure DLC.

Big Picture



Attacks

• Exploits against the system • Local attacks • Attacks against WiFi	• Default credentials • Exploits against the router	• Web-App Hacking • Brut-forcing	• Malware • MitM • Eaves-dropping	• Theft • Un-kown access

Are you vulnerable? Yes, You Are Vulnerable!

Our Smart IoT App Vulns

- Weak encryption for storage of the user credentials inside the smartphone app.
- Easy to brutforce user credentials of the used cloud server because of missing measures.
- Hard coded cloud credentials inside the Arduino app code.
  - Becomes a serious problem – we want to open the front door…
- Hard coded encryption key for WiFi
  - Could leak your WiFi key by the source-code and you need a way to handle changing the key…

Like The Reality?

- Are their any existing vulnerabilities?
  Yes – of course :-)
- It's like at any known application.
- Plus extra spread over different communication partners and systems.

Some known Vulns (2)

- CVE-2014-3344:
  - Cisco Transport Gateway for Smart Call Home framework multiple cross-site scripting (XSS) vulnerabilities.
  - Allows remote attackers inject arbitrary web script or HTML.
- CVE-2014-9557:
  - Smartwebsites SmartCMS Multiple XSS (Cross-Site Scripting) Security Vulnerabilities.

Some known Vulns (1)

- CVE-2014-4892:
  - uControl Mobile App no X.509 SSL certificate verification.
  - Allows Man-in-the-Middle attacks like accessing sensible data or trigger action.
- CVE-2014-3346:
  - Cisco Transport Gateway for Smart Call Home DOS vulnerability in framework.
  - Allows breaking the availability.

Some known Vulns (3)

- Loxone Smart Home 2015.02.28:
  - Multiple vulnerabilities found by SEC Consult Vulnerability Lab like:
    - Cross-site request-forgery (XSRF)
    - Multiple reflected cross-site scripting (XSS) vulnerabilities plus stored.
    - Denial of service (DoS) by simple synflood.
    - Credential Leakage because of storing in cleartext.

Automation could harder

- Want to have more fun?

- Go performing penetration tests on automation components.
- Yes for sure – only in a test lab environment ;-)
- And you will get ICSA-Numbers from the ICS-Cert…

War Story
Scalance Switch

- ICSA-12-102-04: Siemens Scalance X Buffer Overflow Vulnerability
- Found by performing a brutforce stability test.
- Missing password length check in web GUI causes a reboot of the switch.
- What leads to a **safety stop**!

War Story
Siemens CP 1604/1616

- ICSA-13-084-01: Siemens CP 1604/1616 Improper Access Control
- Found by performing a security test of a robot.
- Accessible **remote** debugging port.
- While “playing” with the debugging port – the card crashes…
- What leads to **not** any more **controllable** robot (needed to restart)!

War Story
BTW Robots...

- Sorry... not public...
- So only in the talk ;-)

SDLC for IoT is necessary!

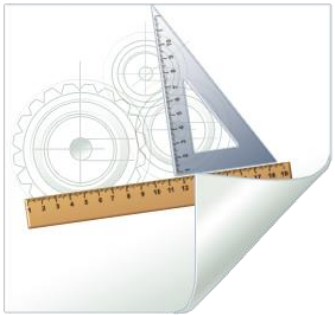
IoT & Threats & SDLC (1)

- Start thinking like a hacker to understand threats and why possible vulnerabilities could become a serious problem.
- Understand possible IT security problems at the IoT environment and all involved 3rd party systems.
- Identify weakness inside your concept – in every phase of you development live cycle.
- React as soon as possible – this makes live a lot easier and more secure :-)

IoT & Threats & SDLC (2)

- And the biggest challenge:
- The Life Time!
- IoT, Automation Components, Smart Home Device etc. will run longer than your smartphone.
- Where talking about 10 up to 30 years!
- Remind it for your IoT SDLC.

SDLC & IoT (1)



- A complete/holistic SDLC for IoT is necessary.
- Security should be taken into consideration in each phase of application/system development.
- Existing SSDLC methodologies focus on Governance, Construction, Verification and Deployment business functions and their relevant security activities.
- And for Operation!

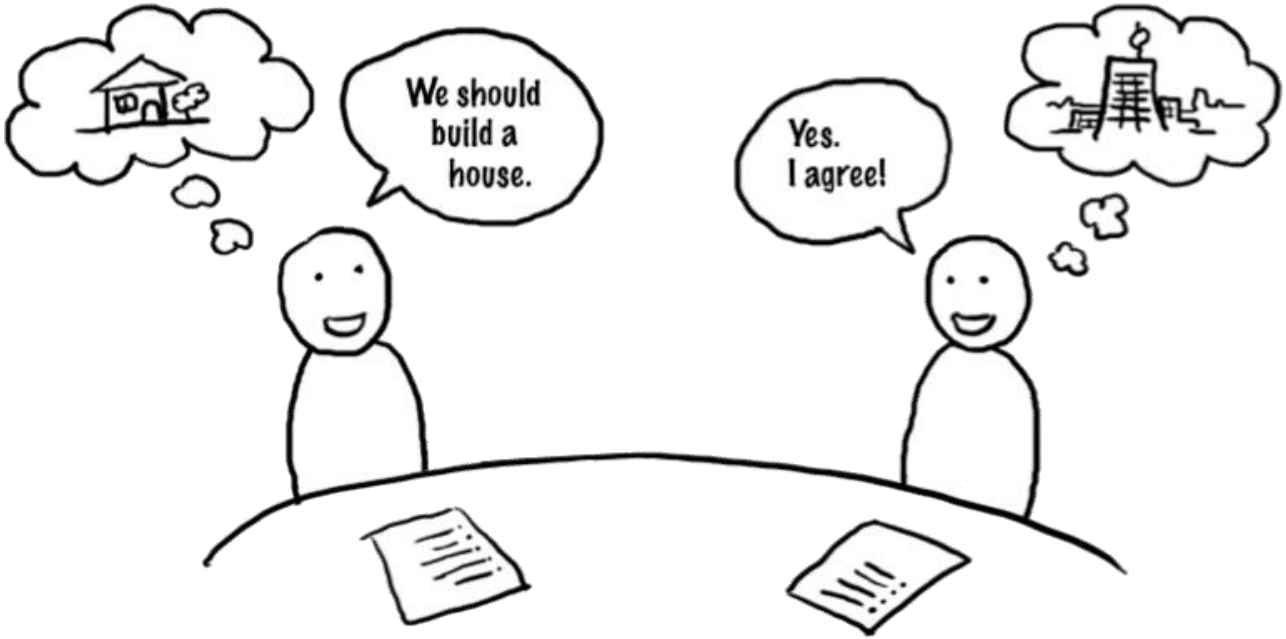
SDLC & IoT (2)

- Use Software Assurance Maturity Models e.g.
  - OpenSAMM [http://www.opensamm.org]
  - BSIMM (Building Security In Maturity Model) [www.bsimm.com]
- These methodologies can help to improve security of IoT systems and applications.
- Don't forgot to include all involved partners and used communication links into your analysis.

Conclusion

- Smart and IoT systems will be widely spread in the future.
- They will cover a lot of our daily work and live.
- So they need to be designed to protect our privacy and our safety.
- And they will run longer as expected.
- Smart and IoT should not become an acronym for unsecure…

Thanks a lot for you attention :-)



Questions

www.TROOPERS.de