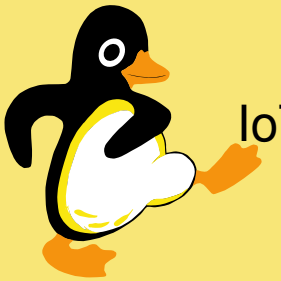


IoT Security and Privacy

Dr. Ralf Schlatterbeck
Open Source Consulting

Email: office@runtux.com
Web: http://www.runtux.com
Tel. +43/650/621 40 17

IoT

→ Internet of Things
- Haustechnik (Home Automation)
- Smart City
- Smart Grid: Stromzähler
- Industrielles Internet (Industrie 4.0)
- Auto
- Medizintechnik
- Einzelhandel
- . . .

Safety vs. Security

- Im Englischen: Sicherheit: Safety oder Security
- Safety: Schutz vor unwahrscheinlichem Ereignis das zu Gefahr der Verletzung o.ä. führen kann

→ „Gegner“ ist die Physik

- Security: Schutz vor Bedrohung

→ „Gegner“ ist ein Mensch (!) „Adversary“
- Confidentiality (Geheimhaltung) → u.a. Privacy!
- Integrity (Integrität von Daten oder Zuständen)
- Availability (Verfügbarkeit)
  keine „Denial of Service Attack“

PWNAGE

- Frage: Wem „gehört“ ein Gerät
- Who „owns“ the Device: ownage or PWNAGE
- Bedeutet: Wer *kontrolliert* das Gerät
- De facto, nicht de jure Besitz
- Gilt natürlich auch für Daten
- Wem „gehören“ die Daten in der Cloud?
- Cloud: another word for other peoples computers!

- In der Folge *pwned* als Wortschöpfung

Beispiel Skype

- Skype ist verschlüsselt
- Frage: Wer hat den Schlüssel?
- Wer den Schlüssel hat, hat Zugang zur Kommunikation

→ PWNED

Kurt Sauer, Skype: „Wir stellen eine sichere Kommunikationsmöglichkeit zur Verfügung. Ich werde Ihnen nicht sagen, ob wir dabei zuhören können oder nicht.“ [Eve07]

Data Leaks

- Impressive List of Data-Leaks Wikipedia [Wik17]
- $>$ 200 cases with up to several million datasets each
- „Lost“ Data (Euphemism for „stolen“)
- Health-Care
- Financial (and Credit-Card data)
- Email
- Dating Sites
- ...

→ Now imagine Home-Automation + IoT

Influences on “Real World”

- Møller-Maersk:
  Largest Container-Shipping Company
- NotPetya (allegedly Russian) worm
- Used vulnerability developed by NSA: “EternalBlue”
- Original Target was Ukraine
- “it was the equivalent of using a nuclear bomb to achieve a small tactical victory”[Gre18]
- Estimated $300,000,000 just for Møller-Maersk
- Downtime: Several Days
- Good Story in Wired [Gre18]

IoT: Nicht nur Daten

- IoT Geräte kontrollieren ihre Umwelt!
- Sensoren zur Erfassung von Messwerten
- Aktuatoren zur Beeinflussung der Umwelt
- Beispiel: Türschloss
- Beispiel: Heizung
- Ransomware?

→ Was passiert wenn ein IoT-Device *pwned* wird?

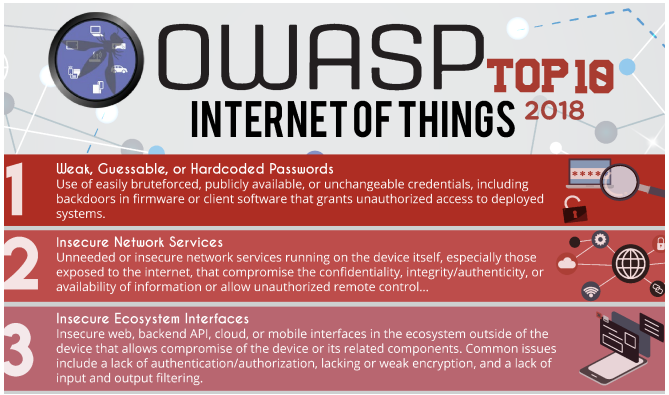
→ Verfügbarkeit (Availability) wird wichtiger

→ Integrität wird wichtiger [Sch17]

An Internet-sized Robot

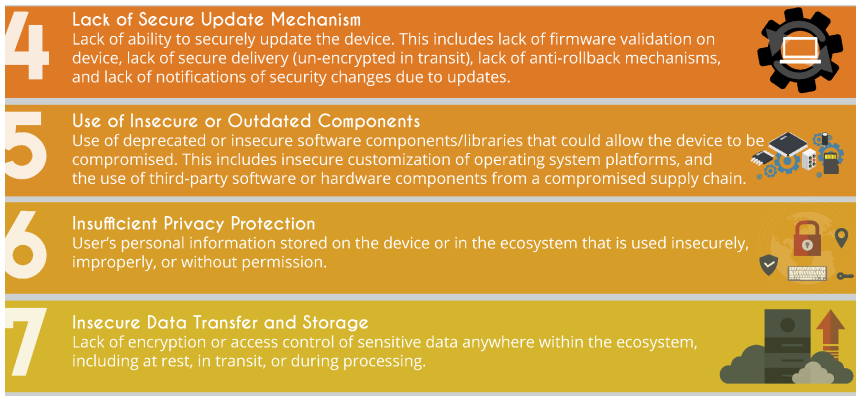
„You can think of the sensors as the eyes and ears of the internet. You can think of the actuators as the hands and feet of the internet. And you can think of the stuff in the middle as the brain. We are building an internet that senses, thinks, and acts.
This is the classic definition of a robot. We're building a world-size robot, and we don't even realize it.
[. . .] Give the internet hands and feet, and it will have the ability to punch and kick.“ [Sch17]

Open Web Application Security Project



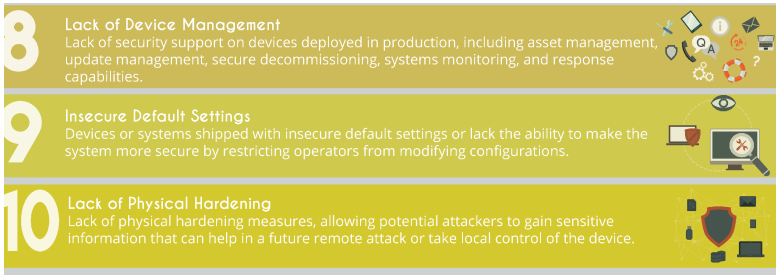
[OWA18]

Open Web Application Security Project



[OWA18]

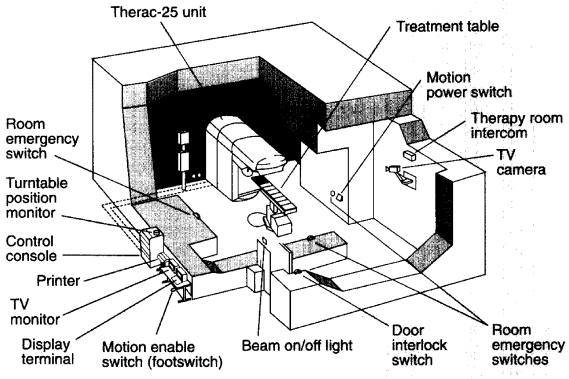
Open Web Application Security Project



[OWA18]

Failures Pre-Internet: Therac-25

1980er computerisierte Bestrahlungseinheit [LT93]



Nehmen wir ein Netzwerk dazu

- Netzwerk macht Angriffe schlimmer
- Economy of Scale
- Gleicher Angriff auf Millionen von Geräten
- 2016: Angriff auf Brian Krebs, Security Blogger
- . . . Mit *pwned* Web-Cams
- Bis dahin nicht gesehene Bandbreite 620 Gbps

→ Was kann man sonst noch mit einer *pwned* Web-cam tun? Wer hat eine im Wohnzimmer?
→ Neue, „kreative“ Angriffe möglich!

Marktversagen

- Weder der Käufer noch der Verkäufer interessiert sich für Security
- Der Käufer der Web-Cam weiss nicht dass diese für Angriffe verwendet wird
- Der Verkäufer ist nur an Features interessiert, und an kurzer „Time to Market“
- Die Betroffenen sind weder Käufer noch Verkäufer

→ Staatliche Regulierung???
→ [Sch17]

Bruce Schneier: Truisms

- On the internet, attack is easier than defense
- Most software is poorly written and insecure
- Connecting everything to each other via the internet will expose new vulnerabilities
- Everybody has to stop the best attackers in the world
  Via network everyone can reach everywhere
- Laws inhibit security research
  USA: Digital Millenium Copyright Act, Germany: Hacking Tools

→ [Sch17]

Constrained Device

- Kilobyte nicht Gigabyte
- Megahertz nicht Gigahertz
- Moores Law nicht für Leistungssteigerung
- . . . sondern niedrigeren Stromverbrauch + kleiner
- Typischerweise verbunden über Funk
- Nicht WLAN, langsamer, energiesparender
- Netzwerk: ZigBee oder 6loWPAN
- Auch Bluetooth (low energy)

Constrained Device

- Contrained Devices heute in vielen Geräten
- Waschmaschine, Backofen, Herd, Spülmaschine, Heizung, Fernseher, Videorecorder. . .
- Aber heute oft noch kein Netzwerk
- *Viel* mehr Devices als Webcams
- Nehmen wir ein Netzwerk dazu: Waschmaschine ans Internet
- Fernseher hats schon: Spracherkennung in der Cloud [Har15]
- Update-Problem durch geringe Bandbreite!
- Für viele Devices keine Update-Möglichkeit!

Beispiel Philips Hue

- „Intelligente“ Glühbirne
- Farbige LEDs mit Einstellmöglichkeit
- Kommunikation über Funk (ZigBee)
- Typisches „Constrained Device“
- Basisstation kommuniziert mit Lampen
- Basisstation verbunden mit Philips Cloud
- Fernsteuerung möglich
- Programmierung *nur* über die Cloud
- Lampen von anderen Herstellern tw. möglich
- Aber ging dann plötzlich nicht mehr

IoT-Worm Paper

- Security-Researcher Weizmann Institute
- Mehrere Schwachstellen in Philips Lampen
- Pairing mit Basisstation
- . . . normalerweise nur auf <1m Entfernung

→ war auf Funkentfernung möglich

→ damit kann ich die Lampe des Nachbarn *pwnen*

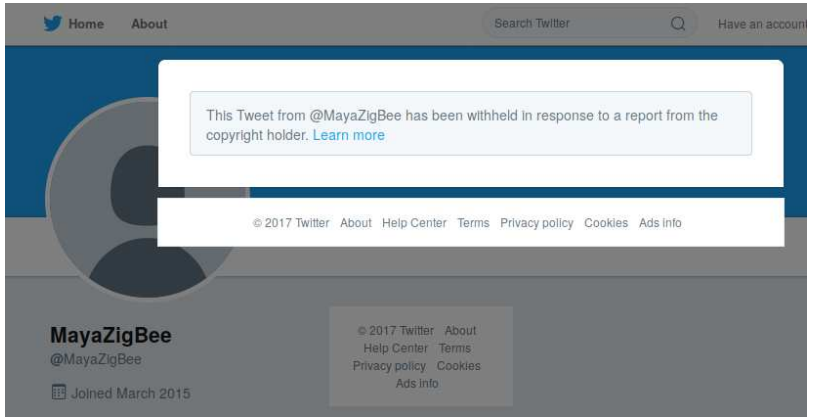
- . . . und schlimmeres
- Pairing Keys sind in jedem Gerät gleich
- Waren ursprünglich geheim aber sind inzwischen bekannt
- . . . Pairing-Vorgang ist abhörbar [ROSW16]

IoT-Worm Paper

- Philips Lampen können Software-Upgrade (gut!)
- Dafür ist ein Schlüssel nötig
- . . . der in jeder Lampe steckt
- Dieser Schlüssel ist nicht einfach auszulesen
- Aber die Angreifer konnten es trotzdem
- Sidechannel-Angriff [ROSW16]
- . . . Strommessung am Microcontroller
- . . . Lässt Rückschlüsse auf den Key zu
- Inzwischen ist der Key auf Twitter geleakt

Twitter

Naive Suche nach ZigBee Key auf Twitter



Zahnpasta geht nicht zurück in die Tube

Symmetrische vs. Asymmetrische Schlüssel

- Symmetrisch: Gleicher Schlüssel beim Hersteller und im Gerät – kann, wie wir gehen haben, aus dem Gerät geholt werden
- Asymmetrische Schlüssel: Privater Schlüssel beim Hersteller
- Public Key im Gerät

- Funktioniert leider nicht für initialen Schlüsselaustausch: Henne-Ei Problem
- Out-of-Band für Pairing ist besser
- . . . aber braucht zusätzliche Ressourcen

Wurm

→ Pairing in Funkreichweite
→ Software-Upgrade Key
- Alle Zutaten für einen Wurm
- . . . der sich von Lampe zu Lampe ausbreitet
- Pairing: Auf Funkreichweite
- Reset to Factory Default
- Software Upgrade
- Die neu infizierte Lampe infiziert *alle Lampen in Funkreichweite*
- In einer Stadt wie Paris: Abdeckung gut genug dass *alle* Lampen infiziert werden [ROSW16]

What to do with pwned Lamp?

- Licht aus!
- Neue „kreative„(?) Angriffe möglich!
- photosensitive Epilepsie: 0.8% aller Kinder
- Auslösung durch Lichtblitze
- Bei Kontrolle von vielen Lampen:
- Alle gleichzeitig ein- ausschalten
- . . . Angriff auf Stromversorgungs-Infrastruktur
- „Information Exfiltration“ [RS16]

Informationsübertragung

Informationsübertragung durch intelligente Glühbirne [RS16]

Extended Functionality Attacks

Attack deviates from normal Functionality [RS16]
- Ignoring the functionality
  → Botnet of WebCams
- Reducing the functionality (Denial of Service)
  → No Light, Ransomware
- Misusing the functionality
  → photosensitive Epilepsy
- Extending the functionality
  → Information Exfiltration
  Different and unexpected physical effect (!)
  MacGyver. . .

Andere Beispiele

→ Stromzähler: Abschaltung eingebaut,
geringe Bandbreite für Updates
Gefahr eines Blackout
→ Auto: Angriff auf Unterhaltungselektronik
von dort auf CAN-Bus → *Bremse* (!)
→ Medizinische Geräte oft unsicher
Zertifizierung verhindert Updates
→ Viele Geräte funktionieren *nur* mit Cloud
Google Revolv Smart Home [Fin16]
Philips Hue
. . . *pwned* . . .

Agile vs. Certified

Two approaches to safety & security

1. Get it right the first time and certify
2. Make your security agile

- With 1 we get secure design & engineering, government approval. Known from Safety world (planes, medical devices).
- With 2 getting it wrong is ok if you can respond fast enough

These worlds are colliding, need to make them work together [Sch17]

Agile vs. Certified

- We know how to get it right with safety (physics!)
- We do not know how to get it righ with security (human adversary!)
- From previous examples we see that creativity plays a major role in discovering new exploits
- . . . that when developing nobody thought about
- Is the number of exploits limited or unlimited?
- Given enough time & development:
Do we eventually get a secure system?
- Or will we discover new exploits as time goes on?
- At least attacks never get worse!

Agile *and* Certified?

- Use certification for safety
- Re-certification must be *fast*
- Use automated tests for re-certification?
- More costly during development but re-certification is cheaper!
- In case of security problems: re-run tests
on modified system
- Do we need a security certification?
- Security is a *process*!

Connect Everything to the Net??

“That’s a lot of different security requirements, and the effects of getting them wrong range from illegal surveillance to extortion by ransomware to mass death. My guess is that we will soon reach a high-water mark of computerization and connectivity, and that afterward we will make conscious decisions about what and how we decide to interconnect. But we’re still in the honeymoon phase of connectivity. [. . .] mantra for the internet today might be: ‘Connect it all.’ ” [Sch17]
Regulation? How do we ensure we get something that works?

Contents

Contents

Contents

Bibliography

[Eve07] Joris Evers. Telefonieren übers Internet: Wie sicher ist Skype wirklich? News article, NetMediaEurope Deutschland GmbH, February 2007. Accessed 2017-10-21.

[Fin16] Klint Finley. Nest's hub shutdown proves you're crazy to buy into the internet of things. News article, Wired, May 2016.

[Gre18] Andy Greenberg. The untold story of NotPetya, the most devastating cyberattack in

Bibliography

history. *Wired*, August 2018.

[Har15] Shane Harris. Your Samsung SmartTV is spying on you, basically. News article, The Daily Beast, May 2015.

[LT93] Nancy G. Leveson and Clark S. Turner. An investigation of the Therac-25 accidents. *IEEE Computer*, 26(7):18–41, July 1993.

[OWA18] OWASP internet of things top 10 2018. Security recommendation, Open Web

Bibliography

Application Security Project, December 2018.

[ROSW16] Eyal Ronen, Colin O'Flynn, Adi Shamir, and Achi-Or Weingarten. IoT goes nuclear: Creating a ZigBee chain reaction. Technical report, Weizmann Institute of Science, November 2016.

[RS16] Eyal Ronen and Adi Shamir. Extended functionality attacks on IoT devices: The case of smart lights. In *1st IEEE Euro-*

Bibliography

pean Symposium on Security and Privacy, pages 3–12, Saarbrücken, Germany, March 2016. Invited paper.

[Sch17] Bruce Schneier. Security and the internet of things. Blog post, Bruce Schneier Blog, February 2017.

[Wik17] List of data breaches. Wikipedia, Wikipedia, October 2017. Accessed 2017-10-21.