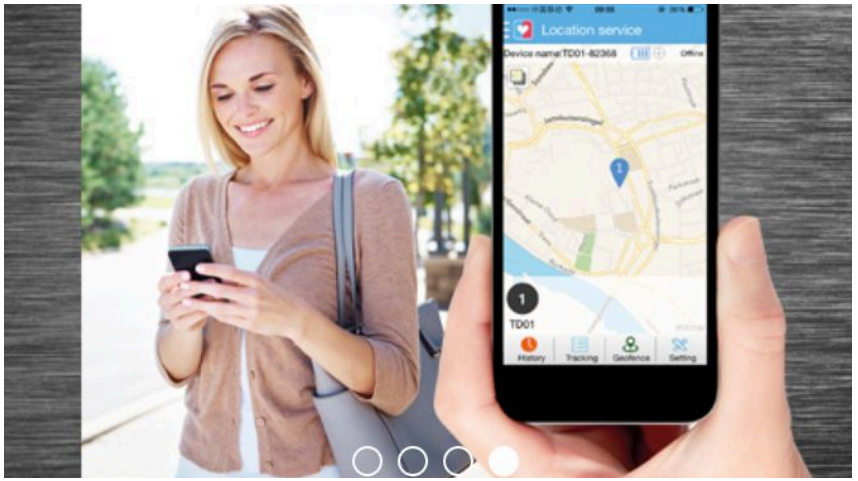
The sustainability of safety, security and privacy

Ross Anderson

Cambridge

Darmstadt, September 2019

EU RAPEX A12/0157/19



- Enox's 'Safe-Kid One' was recalled on Saturday 1 Feb
- "Unencrypted communications with its backend server … enables unauthenticated access"
- Hackers can track and call kids, change device ID…
- Doesn't comply with Radio Equipment Directive

How does IoT change safety?

- The EU regulates safety of all sorts of devices
- In 2015, they asked Éireann Leverett, Richard Clayton and me to examine what IoT implied
- 2016 report (WEIS 2017): once there's software everywhere, safety and security get entangled
- (The two are the same in the languages spoken by most EU citizens – sicurezza, seguridad, sûreté, Sicherheit, trygghet…)
- How will we have to update safety regulation (and safety regulators) to cope?

Background

- Markets do safety in some industries (aviation) way better than others (medicine)
- Cars were dreadful until Nader's 'Unsafe at Any Speed' led to the NHTSA
- In the EU, we have broad frameworks such as the Product Liability Directive 85/374/EES, Framework Directive 2007/43/EC on type approval, plus many detailed rules
- Over 20 EU agencies (plus UNECE) in play

When cars get hacked

When cars get hacked (2)

- 2011: Carshark needed physical access
- 2015: Charlie Miller and Chris Valasek hacked a jeep Cherokee via Chrysler's Uconnect
- So now we just need your IP address!
- Suddenly people cared…
- Chrysler recalled 1.4m vehicles for software fix

When cars get hacked (3)

Darmstadt, September 2019


CareFusion
Alaris® PC
PRIMARY INFUSION
RATE
VTBI
Press START


Options
Total Volume
Occlusion Alarm Setting
Primary
Secondary Bolus
Rate
Volume to be Infused
Run
Hold
On Off Charge
Battery
Silence
GRASEBY
500


P Bag Vol: 250ml
Volume Left 246.9
A Infused 3.1
Press OK to start
START OK
STOP NO
BOLUS
ON OFF
BodyGuard 545


DOOR OPEN CLOSE CLAMP
ALARM PUMPING ALERT
BACK LIGHT
SILENCE
125
1000
CLEAR TOT VOL
TIME
STOP
ON OFF CHARGE
OPTIONS


SILENCE
STOP
START
POWER
ABBOTT
GEMSTAR
ON / OFF
BACK-UP
CHANGE
OPTIONS
PURGE
HELP
NO
YES ENTER
1-800-241-4002


1 SELECT mg/mL
2 SELECT µg/mL
3 SELECT mL
HOSPIRA
aim plus
OPTIONS
STOP
START
HELP
BACKUP
CHANGE
SILENCE
PRIME
NO
YES ENTER


Epidural
A:Bupivicaine/Fentanyl
500ml
Rate :
0 mL/hr
Pt Bolus 0
mmHg 0 720
ON OFF
info
STOP NO
START OK
PRIME BOLUS
cme medical
BODY GUARD 545

Background (2)

- Research by Harold Thimbleby: hospital safety usability failures kill about 2000 p.a. in the UK, about the same as road accidents
- Safety usability ignored – incentives wrong…
- But attacks are very much harder to ignore – a wifi tampering demo in 2015 led the FDA to blacklist the Hospira Symbiq infusion pump
- 2017: recall of 450,000 St Jude pacemakers
- What should Europe do?

Background (3)

- The Medical Device Directives have been revised: reg 2017/745 comes into force 2020 requiring post-market surveillance, a risk management plan for each device, ergonomic design …
- Reg 17.2: ‘for devices that incorporate software… the software shall be developed … in accordance with the state of the art taking into account the principles of development life cycle, risk management, including information security, verification and validation’

Background (4)

- 18.8 ‘Devices shall be designed and manufactured in such a way as to protect, as far as possible, against unauthorised access that could hamper the device from functioning as intended’.
- It’s still not perfect (there’s wriggle room on ergonomics, network security assumptions…) but it’s a huge improvement!

Background (5)

- Electricity substations: 40-year lifecycle, protocols (DNP3) don't support authentication
- IP networking: suddenly anyone who knows a sensor's IP address can read from it, and with an actuator's IP address you can activate it
- Only practical fix: re-perimeterise!
- Have one component that connects you to the network and replace it every 5 years (harder for cars which have multiple RF interfaces)

Broad questions include…

- Who will investigate incidents, and to whom will they be reported?
- How do we embed responsible disclosure?
- How do we bring safety engineers and security engineers together?
- Will regulators all need security engineers?
- How do we prevent abusive lock-in? Note the US DMCA exemption to repair tractors …

Policy recommendations included

- Requiring vendors to self-certify, for their CE mark, that products can be patched if need be
- Requiring a secure development lifecycle with vulnerability management (ISO 29174, 30111)
- Creating a European Security Engineering Agency to support policymakers (now: ENISA)
- Extending the Product Liability Directive to services
- Updating NIS Directive to report breaches and vulnerabilities to safety regulators and users

The punch line

- Phones, laptops: patch them monthly, but make them obsolete quickly so you don’t have to support 100 different models

The punch line

- Phones, laptops: patch them monthly, but make them obsolete quickly so you don't have to support 100 different models
- Cars, medical devices: we test them to death before release, but don't connect them to the Internet, and almost never patch

The punch line

- Phones, laptops: patch them monthly, but make them obsolete quickly so you don't have to support 100 different models
- Cars, medical devices: we test them to death before release, but don't connect them to the Internet, and almost never patch
- So what happens to support costs now we're starting to patch cars?

The trilemma

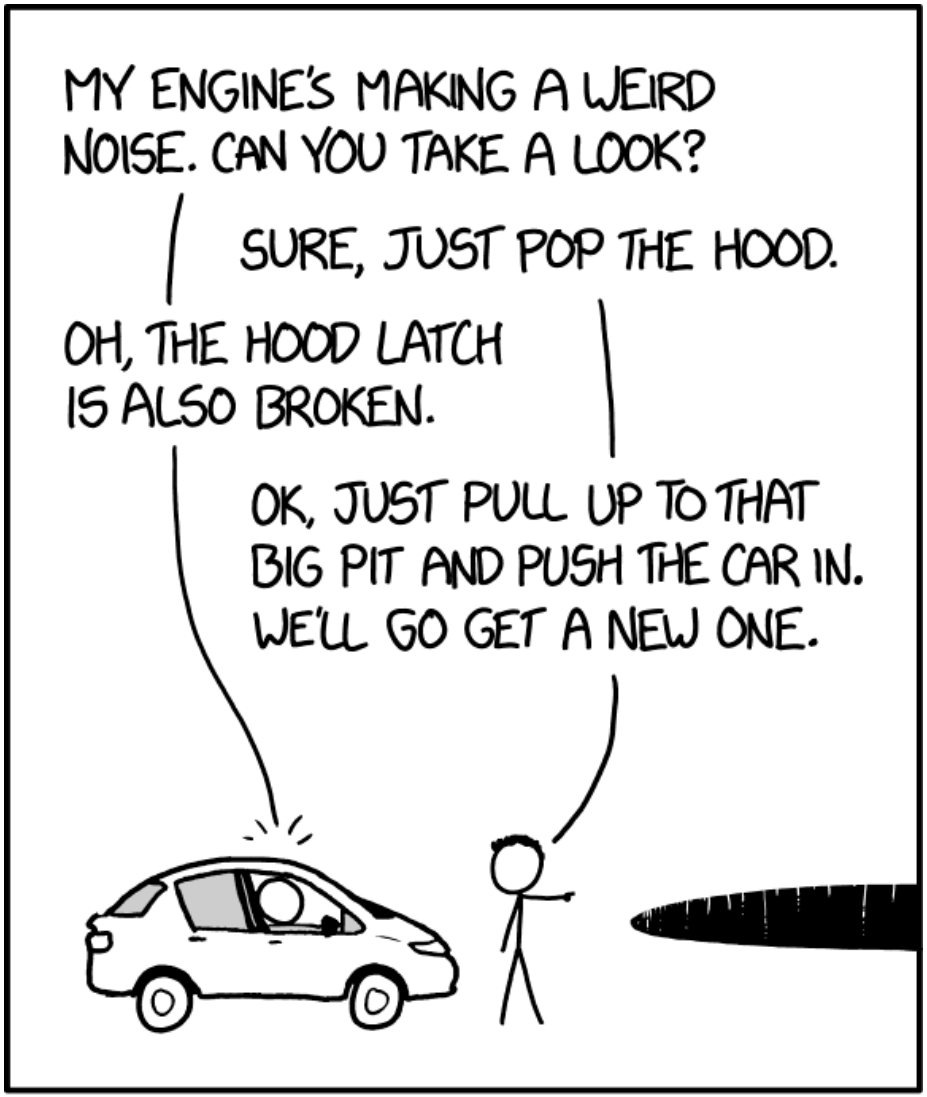
- Standard safety lifecycle, no patching -> safety + sustainability -> go online, get hacked
- Standard security lifecycle, patching -> breaks safety certification
- Patching plus redoing safety certification with current methods -> costs of maintaining safety rating can be sky high
- So: can we get safety, security and sustainability at the same time?

The right to repair

- The Centennial Light has been burning since 1901
- In 1924, a cartel of GE, Osram and Philips agreed to reduce average bulb lifetimes from 2500h to 1000h
- Many firms make it hard or even illegal to fix products
- Shortening product life a crime in France (Apple is being investigated)

Vehicle lifecycle economics

- Vehicle lifetimes in Europe have about doubled in 40 years
- Average age at scrappage in UK now 14.8y
- Some vehicle makers want to say “scrap it after 7 years and buy a new one!”
- But the embedded CO_2 cost of a car often exceeds its lifetime fuel burn
- And what about Africa, where most vehicles are imported second-hand?



I'M SURE THE ECONOMICS MAKE SENSE, BUT IT STILL FREAKS ME OUT HOW QUICK COMPANIES ARE TO REPLACE COMPUTING DEVICES INSTEAD OF TRYING TO FIX THEM.

What is a reasonable design lifetime?

- Cars: maybe 18 years (10 years from sale of last product in a model range)
- Domestic appliances: surely 10 years because of spares obligation, plus store life … 15?
- Medical devices: if a pacemaker has a 10-year in-service life, then surely 20
- Electricity substations: maybe 40 years
- WEF “circular vision for electronics”

2019 Consumer Protection Upgrade

- 2019/771: EU directive on smart goods
- Buyers of goods with digital elements are entitled to necessary updates for two years, or a longer period of time if this is a reasonable expectation of the customer
- We expect this will mean at least 10 years for cars, ovens, fridges, air-conditioning…
- Trader has burden of proof in first two years

The grand challenge for research

- If the durable goods we're designing today are still working in 2038 then things must change
- Computer science = managing complexity
- The history goes through high-level languages, then types, then objects, and tools like git, Jenkins, Coverity …
- What else will be needed for sustainable computing once we have software in just about everything?

New directions…

- Research topics to support 20-year patching
  Include a more stable and powerful toolchain
- Crypto teaches how complex this can be
- Cars teach: how do we sustain all the test environments?
- Control systems teach: can small changes to the architecture limit what you have to patch?
- Android teaches: how do we motivate OEMs to patch products they no longer sell?

Implications for research and teaching

- Since 2016–7 I've been teaching safety and security together in the same course to first-year undergraduates
- We're starting to look at what we can do to make the tool chain more sustainable
- For example, can we stop the compiler writers being a subversive fifth column?
- Better ways to communicate intent might help ('What you get is what you C')

Micro-scale sustainable security

- Laurent Simon, David Chisnall and I worked on compiler support for crypto
  - Easy problem 1: zeroising sensitive variables
  - Easy problem 2: constant time loops
- Can we do these properly, with compiler annotations that make intent explicit?
- Answer: yes, but doing it right is nontrivial!
- EuroS&P paper ‘What you get is what you C’

Macro-scale sustainable security

- The airline industry has infrastructure to learn from accidents and fix stuff
- But the car industry?
  - Safety agency would demand access to 100m lines of software, which even the OEMs don't see now
  - Who gets to see which the accident reports?
  - What happens with a 737Max scale incident?
  - Order 300m license holders to retrain and test?
- This will take 20 years to fix, plus incentives!

My other car's a...

Paefgen has given the world the £110,000 Bentley Continental GT, but prefers to drive a good old Morris Minor

The top dogs of the motor industry don't necessarily drive their own glitzy products ... something much humbler can do them just fine, reports **Andrew Frankel**

Dr Franz-Josef Paefgen is a very important man. As boss of Audi, he set the company on course for the success it enjoys today. Now he is the chairman and chief executive of Bentley, where he has overseen the

with only 40,000 miles on the clock, and not previously restored, which is

Mercedes-Benz SLR McLaren. He has several slices of exotica in his

having to worry, and use it as a true utilitarian car."

admit they drive the cars they wish they had designed, rather than the ones they actually did. Julian Thompson, director of advanced product design at Jaguar and the man who styled the original Lotus Elise, has driven a Ferrari Dino 246GT for

More …

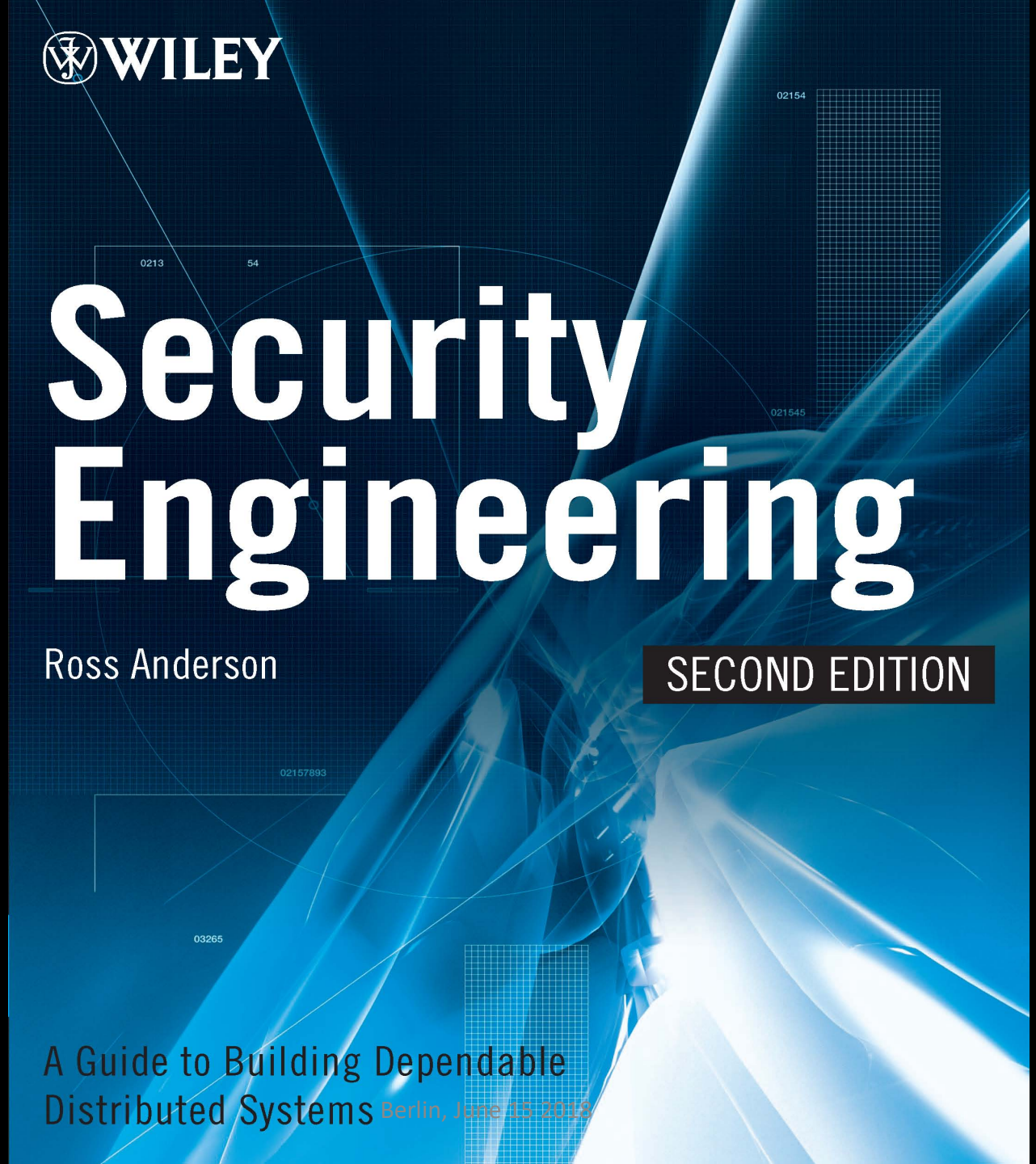
- Our paper "Standardisation and Certification in the Internet of Things" is on my web page

  http://www.cl.cam.ac.uk/~rja14/

- Or see "When Safety and Security Become One" on our blog

  https://www.lightbluetouchpaper.org

- Workshop on the Economics of Information Security, Brussels, June 15–16 2020


WILEY
02154
0213
54
Security
Engineering
021545
Ross Anderson
SECOND EDITION
02157893
03265
A Guide to Building Dependable
Distributed Systems
Berlin, June 15 2018