Cybersecurity: safety, privacy, sustainability and liberty

Ross Anderson
Cambridge

CEPS, 2nd December 2020

The Big Picture

- Yesterday the FT leaked the Commission's plan for a 'Transatlantic Agenda for Global Cooperation' on tech, global warming, covid…
- In tech, the EU is the global privacy regulator as Washington and Peking don't care while nobody else is big enough to matter
- The same is happening in safety and in the prevention of market abuses
- Yet security as privacy is getting entangled with security as safety, and both of them with market abuse!

Safety 101

e-mail Sekretariat: info@enoxgroup.de, Website: www.enoxgroup.de

ENOX Group

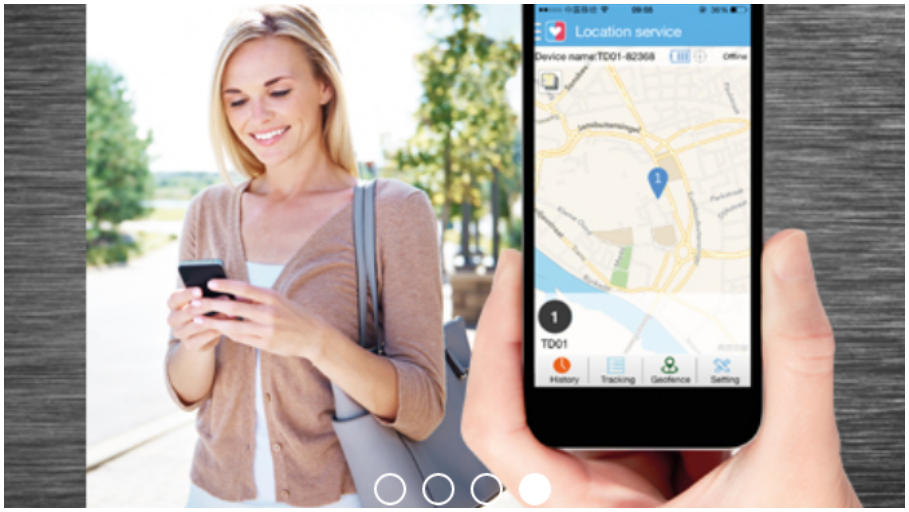
ENOX Production Services GmbH

ENOX SAFE-KID-ONE

A High Tech SIM/GPS Safety and Surveillance Smart Watch for Kids

You can Keep an Eye on, Talk to and Watch over your Kid Everywhere and All the Time

Safety 101



- Enox's 'Safe-Kid One' was recalled Feb 2019
- "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

What about security and safety?

- In 2015, the Commission asked Éireann Leverett, Richard Clayton and me to examine what IoT implied for safety regulation
- 2016 report ‘Standardisation and certification of safety, security and privacy in the Internet of Things’: once there’s software everywhere, safety and security get entangled
- How will we update safety regulation (and safety regulators) to cope?
- We looked at cars, medical devices, and electricity distribution as examples


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
Modular Infusion Pump


Bag Vol: 250ml
Volume Left 246.9
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
TOT VOL STATUS
CLEAR TOT VOL
125
1000
TIME
STOP
ON OFF CHARGE
OPTIONS


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


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


Epidural
11:35
90%
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

Medical Devices

- 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 Wi-Fi 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?

Medical Devices (2)

- The Medical Device Directives have been revised: reg 2017/745 will now come into force in 2021 requiring post-market surveillance, a per-device risk management plan, 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’

Medical Devices (3)

- 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’.
- Similar issues exist in many other sectors, and regulatory action is either underway or needed…
- Not one ‘cybersecurity standard’ but hundreds!

Broader 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 market abuse? Tech is plagued by monopolies large and small…

Sustainability too!

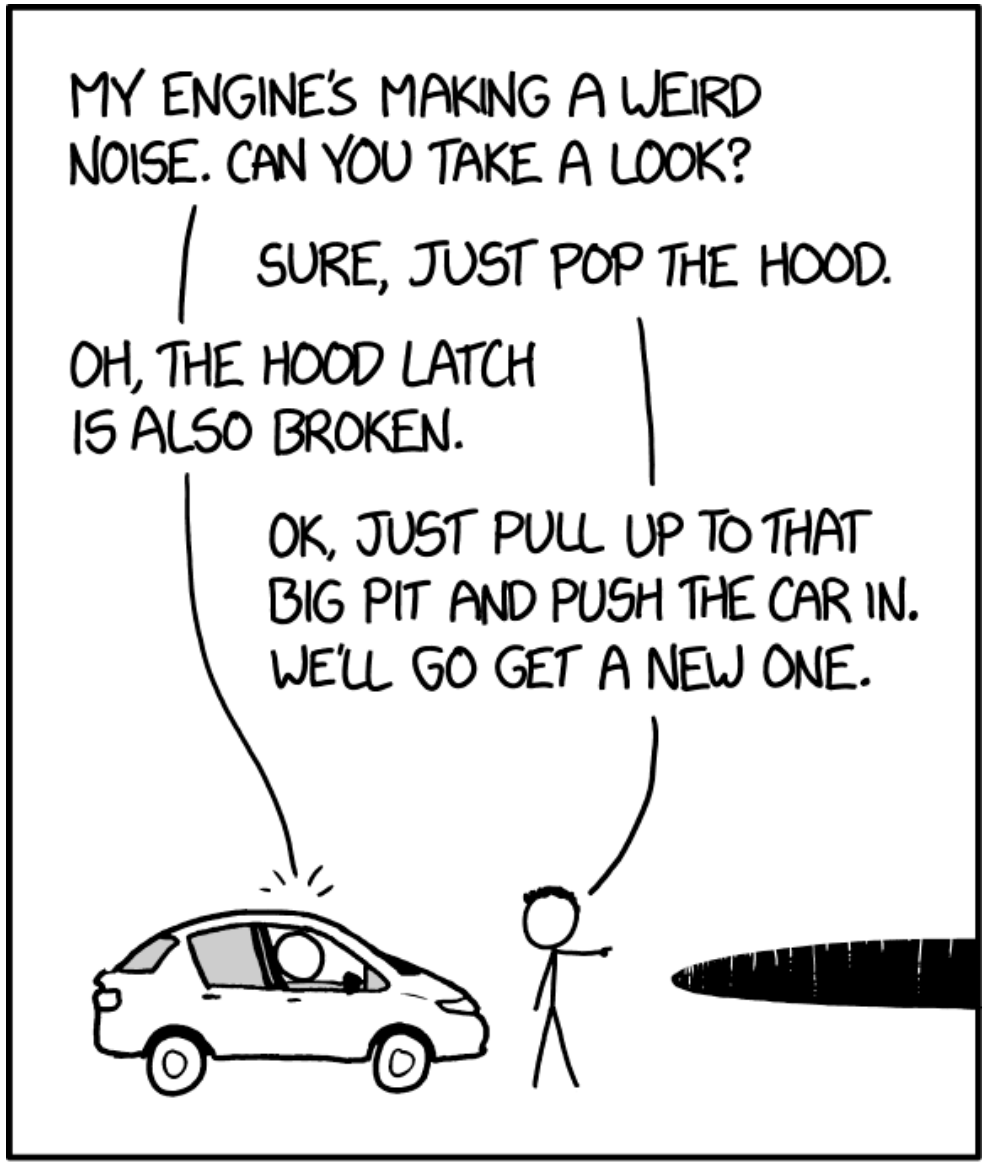
- Phones, laptops: patch them monthly, but make them obsolete quickly so you don’t have to support 100 different models

Sustainability too!

- 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

Sustainability too!

- 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 connect all sorts of durable goods to the Internet, and have to patch them?



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.

Consumer Protection Too!

- 2019/771: EU directive on sales of goods
- Buyers of goods with digital elements are entitled to necessary updates for two years, or for longer if this is a reasonable expectation of the customer
- Trader has burden of proof in first two years
- ‘Reasonable expectation of the customer’ should mean 10+ years for cars, white goods…

The coming tussle with China

- Example: draft ISO 27533
- Biometric authentication on mobile devices: adds modes of operation with templates, matching both on central servers
- This is in parallel to existing Fido Alliance ways of working (bio in secure chip on device)
- Lone academic dissidents can’t push back on this stuff. It will take governments

The coming tussle with China (2)

- Rather than fighting individual suppliers, we need to push technical standards that embed European values of democracy, privacy …
- We also need to embed and defend these values in our own tech policy
- But hang on: the new crypto-war proposal to use upload filters to break end-to-end crypto
- We must abandon this! See “Keys under Doormats”…

More …

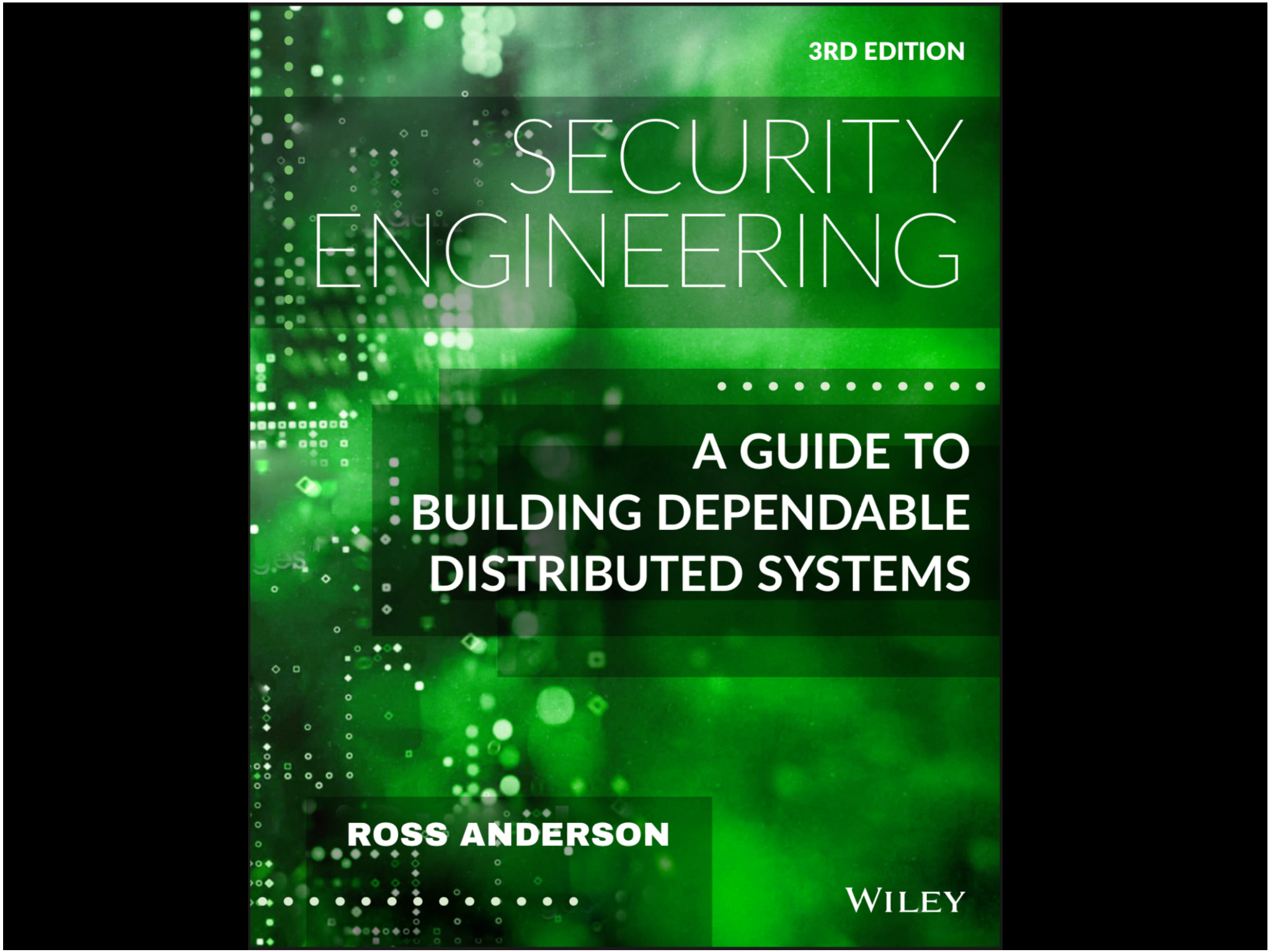
- Our papers 'Standardisation and Certification in the Internet of Things', 'Keys under Doormats' and on sustainability are at

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

- Or see our blog

  https://www.lightbluetouchpaper.org

- Workshop on the Economics of Information Security, CEPS, December 14–15 2020


3RD EDITION
SECURITY ENGINEERING
A GUIDE TO BUILDING DEPENDABLE DISTRIBUTED SYSTEMS
ROSS ANDERSON
WILEY