How Security and Safety will Converge in the IoT World

Eireann Leverett

Concinnity Risks

How does IoT change safety?

- The EU regulates safety of all sorts of devices
- They asked Ross Anderson, Richard Clayton and I to examine what IoT means for this
- 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

IoT: Is it a product or a service?

Product Liability

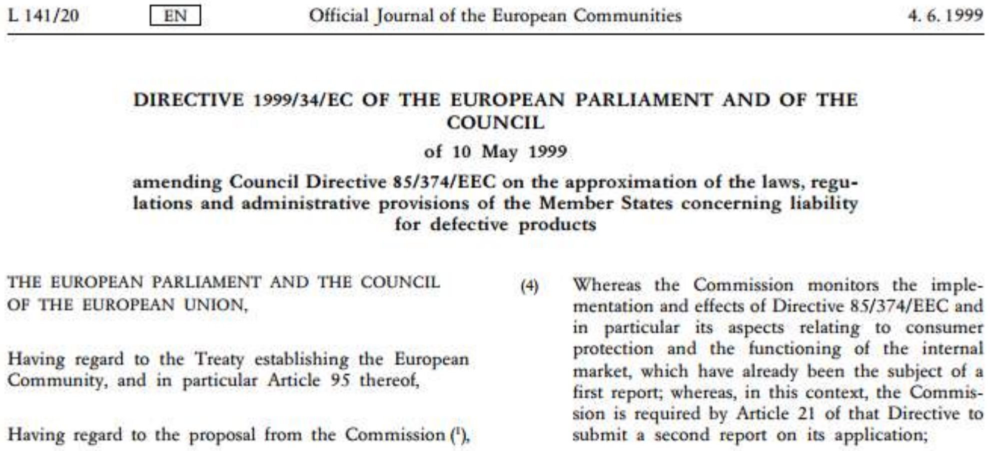
- If a dishwasher floods a kitchen
- If a washing machine overheats
- If a phone catches fire
- If toys are choke hazards
- Recognises differences between defects:
  - Design
  - Manufacturer
  - Informed misuse
- Shared/proportional liability

Firmware/Service Non-Liability

- EULA
- Assumed non-liable
  - For defects
  - For vulnerabilities
  - For exploits

EU Product Liability Directive

- Article 12
- The liability of the producer arising from this Directive may not, in relation to the injured person, be limited or excluded by a provision limiting his liability or exempting him from liability.



L 141/20 EN Official Journal of the European Communities 4. 6. 1999

DIRECTIVE 1999/34/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 10 May 1999

amending Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

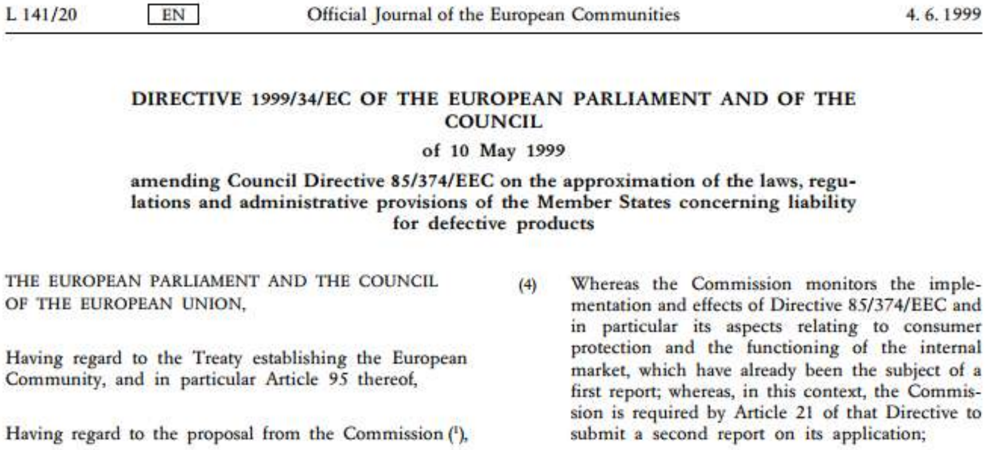
Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission ([1]),

(4) Whereas the Commission monitors the implementation and effects of Directive 85/374/EEC and in particular its aspects relating to consumer protection and the functioning of the internal market, which have already been the subject of a first report; whereas, in this context, the Commission is required by Article 21 of that Directive to submit a second report on its application;

EU Product Liability Directive

- Article 8
- 1. Without prejudice to the provisions of national law concerning the right of contribution or recourse, the liability of the producer shall not be reduced when the damage is caused both by a defect in product and by the act or omission of a third party.
- 2. The liability of the producer may be reduced or disallowed when, having regard to all the circumstances, the damage is caused both by a defect in the product and by the fault of the injured person or any person for whom the injured person is responsible.



L 141/20 EN Official Journal of the European Communities 4. 6. 1999

DIRECTIVE 1999/34/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 10 May 1999

amending Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 95 thereof,

Having regard to the proposal from the Commission [1],

(4) Whereas the Commission monitors the implementation and effects of Directive 85/374/EEC and in particular its aspects relating to consumer protection and the functioning of the internal market, which have already been the subject of a first report; whereas, in this context, the Commission is required by Article 21 of that Directive to submit a second report on its application;

Can exploitation be foreseen?

IoT Manufacturer

- All vulnerabilities are unforeseeable.
- Who would do that?
- How do we know how much to spend on security?
- It’s further up the supply chain, we inherited that code from others.
- Use a firewall.

Ethical Hacker

- No vulnerabilities are unforeseeable.
- The incentives will arise, worry about the vulnerability before you see the motive.
- Test your supply chain too.
- Firewalls have vulnerabilities too.

Foreseeability for Regulators

Some vulnerabilities are completely foreseeable:
-default passwords

Some vulnerabilities are mindblowing surprising:
-Rowhammer

What is in between?
String format bugs, buffer overflows, SQL injection

So how does a regulator or judge who is not a computer scientist decide which is which?

TOOLS.

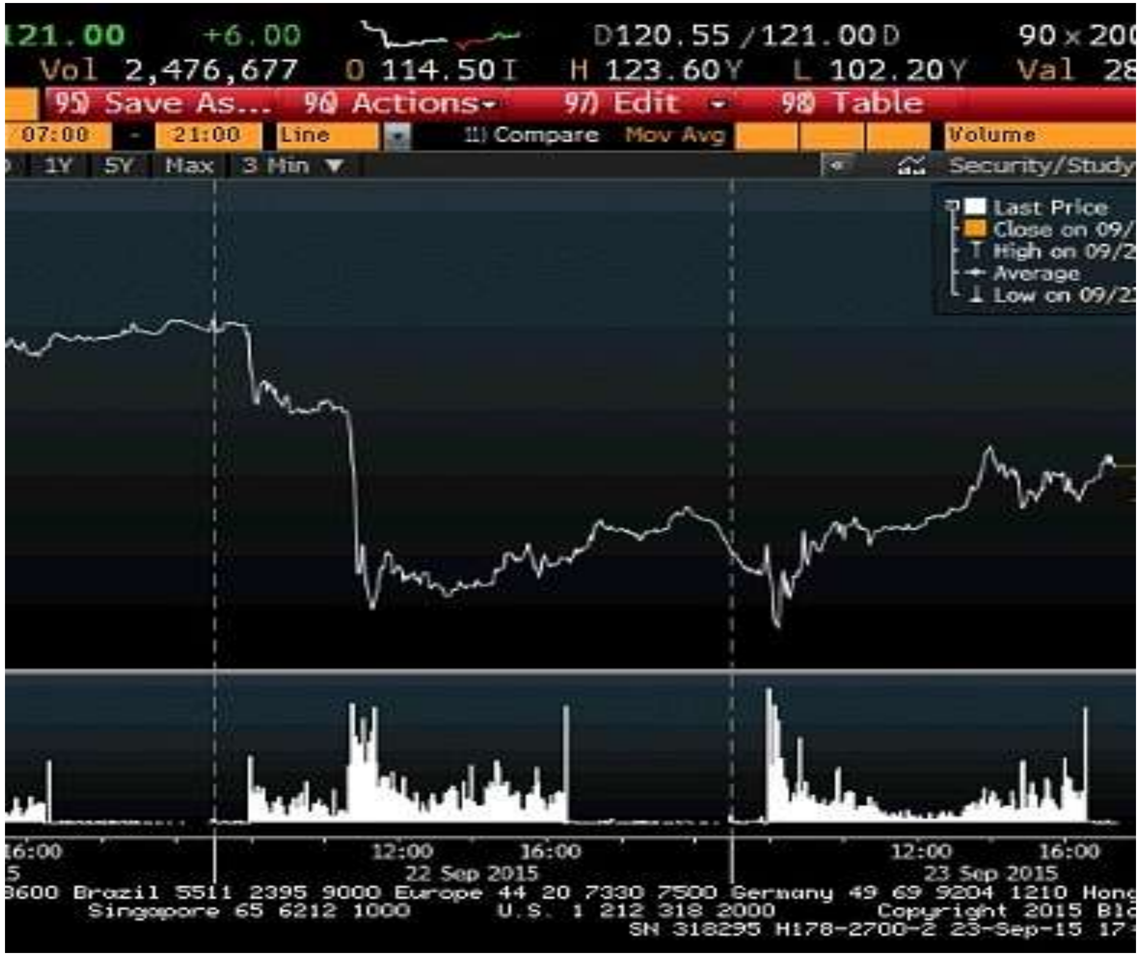
If a tool exists to demonstrate the vulnerability at the time of manufacture…

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)


121.00 +6.00
D120.55 / 121.00 D
90 x 200
Vol 2,476,677 O 114.50 I H 123.60 Y L 102.20 Y Val 28
95) Save As... 96) Actions 97) Edit 98) Table
07:00 - 21:00 Line
11) Compare Mov Avg
Volume
1Y 5Y Max 3 Min
Security/Study
Last Price
Close on 09/
High on 09/2
Average
Low on 09/2
16:00
12:00
16:00
22 Sep 2015
12:00
16:00
23 Sep 2015
3600 Brazil 5511 2395 9000 Europe 44 20 7330 7500 Germany 49 69 9204 1210 Hong
Singapore 65 6212 1000 U.S. 1 212 318 2000 Copyright 2015 Blo
SN 318295 H178-2700-2 23-Sep-15 17

Scaling…

- Traditional car makers moving to autonomy in steps (adaptive cruise control, automatic emergency braking, automatic lane keeping…)
- Challengers like Google, Tesla moving faster
- Tesla has already moved to regular upgrades and the others are racing to follow
- One problem: the test rig (the ‘lab car’) is big, expensive, and gets recycled for new models
- So how will we patch a 2017 car in 2037?

Alaris® Pump
SALINE
CareFusion
Alaris® PC
PRIMARY INFUSION
RATE
VTBI
175.0
Press START
CareFusion

Options
*
Total Volume
Primary
Rate
Run
Hold
On Off Charge
Silence
GRASEBY
500

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
125
1000
TOT VOL STATUS
CLEAR TOT VOL
PRI RATE
PRI VTBI
PRI START
TIME
STOP
ON OFF CHARGE
CLR
SEC RATE
SEC VTBI
SEC START
OPTIONS
Baxter
Flo-Gard® 6201
VOLUMETRIC INFUSION PUMP

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

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

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

Background (2)

- The Medical Device Directives (90/385 EEC, 93/42/EEC, 98/79/EU) are now being revised
- Research by Harold Thimbleby: in the UK, hospital safety usability failures kill about 2000 p.a. (about the same as road accidents)
- Priority: get regulators to do post-approval studies and adverse event reporting
- At present devices are typically approved on paperwork alone

Background (3)

- Usability failures that kill are typically blamed on the nurse (if noticed at all)
- 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
- Software upgrades can break certification!
- Proper safety / security lifecycle is needed

Background (4)

- 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: reperimeterise!
- Have one component that connects you to the network and replace it every 5 years (harder for cars which have multiple RF interfaces)

The Big Challenge

- Established non-IT industries usually have a static approach – pre-market testing with standards that change slowly if at all
- The time constant is typically a decade
- When malicious adversaries can scale bugs into attacks, industries need a dynamic approach with patching, as in IT
- The time constant is then typically a month

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 include

- 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
- 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

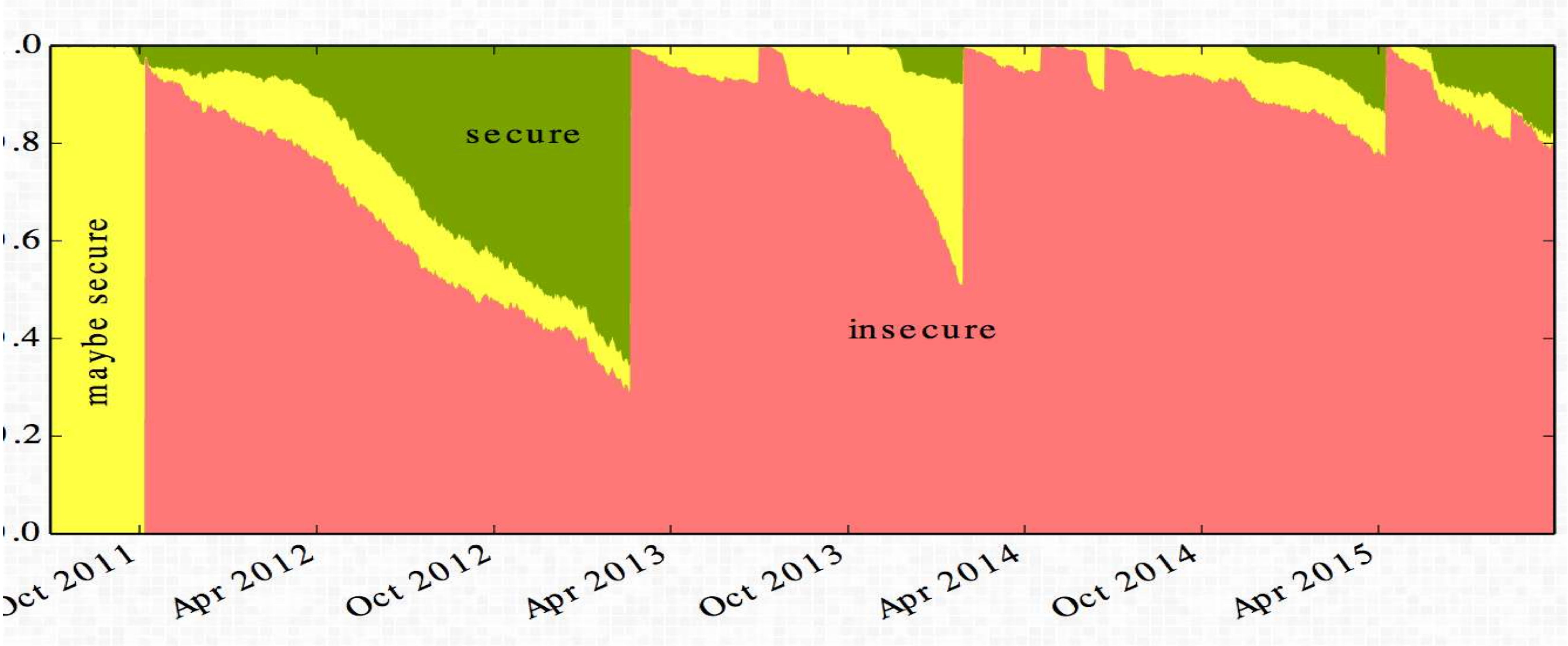
The punch line

- 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?

Security support costs

- Big problem in Android: patching old versions
- The typical OEM’s engineers only work on the current model and the next
- Google started Android OEM incentive program in 2010, with little effect
- So its own brand Nexus phones were next
- But my Nexus 5X – bought last year – will get patches only till 9/2018. I am not happy!

Is Android secure?



Vehicle lifecycle economics

- Vehicle lifetimes in Europe have about doubled in 40 years
- Average age at scrappage in UK now 14.8y
- Vehicle makers might like 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?

Implications for R&D

- 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 this year I’m 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 for programmers to communicate and document intent might help

The grand challenge for research

- If the durable goods we’re designing today are still working in 2037 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?

Conclusions

- Some Vulns are Foreseeable
- The EULA isn't a barrier
- As software eats the world, Traditional Product Liability is being eroded, and not every thing in the real world can be a service.
- Could Liability and a Covigilance approach help?
- If you want to change the world take your 0hdae to the regulator and talk about liability.

More …

- Our paper “Standardisation and Certification in the Internet of Things” is on Ross Anderson's web page

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

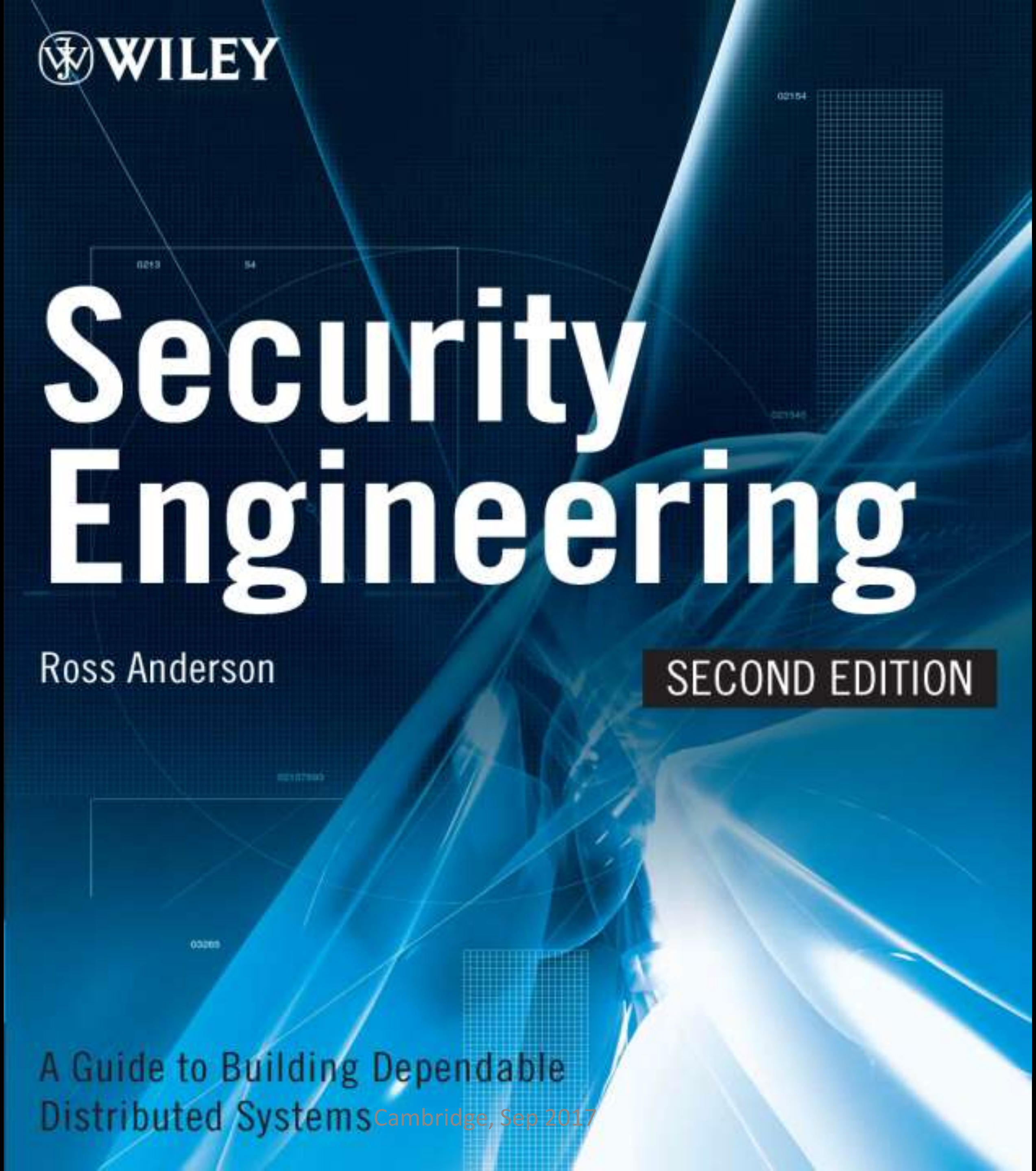
- Or see “When Safety and Security Become One” on our blog

  https://www.lightbluetouchpaper.org

  which also has a couple of videos

Questions?

@blackswanburst



WILEY

Security Engineering

Ross Anderson

SECOND EDITION

A Guide to Building Dependable Distributed Systems