Disclosing Vulnerabilities and Breaches in the 'Internet of Things'

Ross Anderson

Cambridge

What will the IoT change?

- Privacy made the early running with the smart TV and the Cayla doll – but your phone already hears everything and is full of adware
- Denial-of-service was next with the Mirai botnet – but we already have botnets
- But safety looks like the real pressure point
- Phones and laptops don't kill many people directly; cars and medical devices do…

How does IoT change safety?

- Eireann Leverett, Richard Clayton and I did a project for the European Commission
- The EU has complex regulatory regimes for the safety of all sorts of devices
- How will these have to change once there's software everywhere?
- We looked specifically at vehicles, medical devices, and electrotechnical equipment
- But the lessons are more widely applicable!

EU problem statement

- We regulate safety in many industries
- The “Internet of Things” puts computers and communications everywhere
- This creates new safety risks around security
- Indeed, the two are the same in the languages spoken by most EU citizens (sicurezza, seguridad, sûreté, Sicherheit, trygghet…)
- How do we update safety regulation (and safety regulators) to cope?

Background

- Markets do safety in some industries (aviation) way better than others
- Cars were dreadful until Nader's 'Unsafe at Any Speed' fired up the public, got insurance industry involvement and led to the NHTSA
- In the EU, we got the Product Liability Directive 85/374/EES, Framework Directive 2007/43/EC on type approval, and much much else
- Broad principles, plus many detailed rules

Background (2)

- Traditional car makers moving to autonomy in steps (adaptive cruise control, automatic emergency braking, automatic lane keeping…)
- Tesla has already moved to regular upgrades and the legacy OEMs are racing to follow
- But managing vulnerabilities is hard, and expensive: Android is patched for 3 years, Windows for 5
- So how will we patch a 2017 car in 2037?


CEPS, Sep 27 2017


CareFusion
Alaris® PC
PRIMARY INFUSION
RATE
2
VTBI
175.0
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


ALARM PUMPING ALERT
BACK LIGHT
SILENCE
CLEAR TOT VOL
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
BACK-UP
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 (3)

- 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
- Even less post-market feedback than in pharma…

Background (4)

- Usability failures that kill are typically blamed on the nurse (if noticed at all)
- But attacks are much harder to ignore – a 2015 wifi tampering demo led the FDA to blacklist the Hospira Symbiq infusion pump
- 2017: recall of 450,000 St Jude pacemakers
- But software upgrades can break certification!
- Proper safety / security lifecycle is needed

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 will 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 …

Institutional Players

- Dozens of European regulators (+ hundreds in Member States)
- Standards bodies (UNECE, ETSI, CEN, CENELEC)
- Safety labs (KEMA, EuroNCAP, …)
- Security labs (CLEFs, Underwriters' Labs, commercial pen testers, ENCS, academics …)
- Other custodians of the many safety and security standards including NIST, IEEE, IEC
- Other principals, e.g. insurance industry

Policy recommendations included

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

Translating this to engineering

- The problem as always will be scale
- Europe has 50,000 fatal accidents a year and ten times that many causing serious injury
- Future cars will generate vast amounts of data
- How do the right data get to traffic cops, insurers, safety regulators and others?
- We can't just report vulnerabilities and breaches to ENISA / SIAs / DP agencies!
- Culture change too (e.g. VW v Birmingham)

Implications for computer science

- Computer science has always been about managing complexity
- Safety-critical durable goods, online, and composed of heterogeneous components from mutually mistrustful suppliers, are the new grand challenge
- Since doing this project I've started teaching safety and security together in the same course to first-year undergraduates

Conclusions

- The EU regulates safety in dozens of industries
- Once safety-critical goods can be attacked online, it's patch or scrap
- For durable goods like cars and medical devices, this will be a really really big deal
- To manage the ecosystem, a vast amount of data on vulnerabilities, breaches and accidents will have to be managed
- Many policy challenges lie ahead!

More …

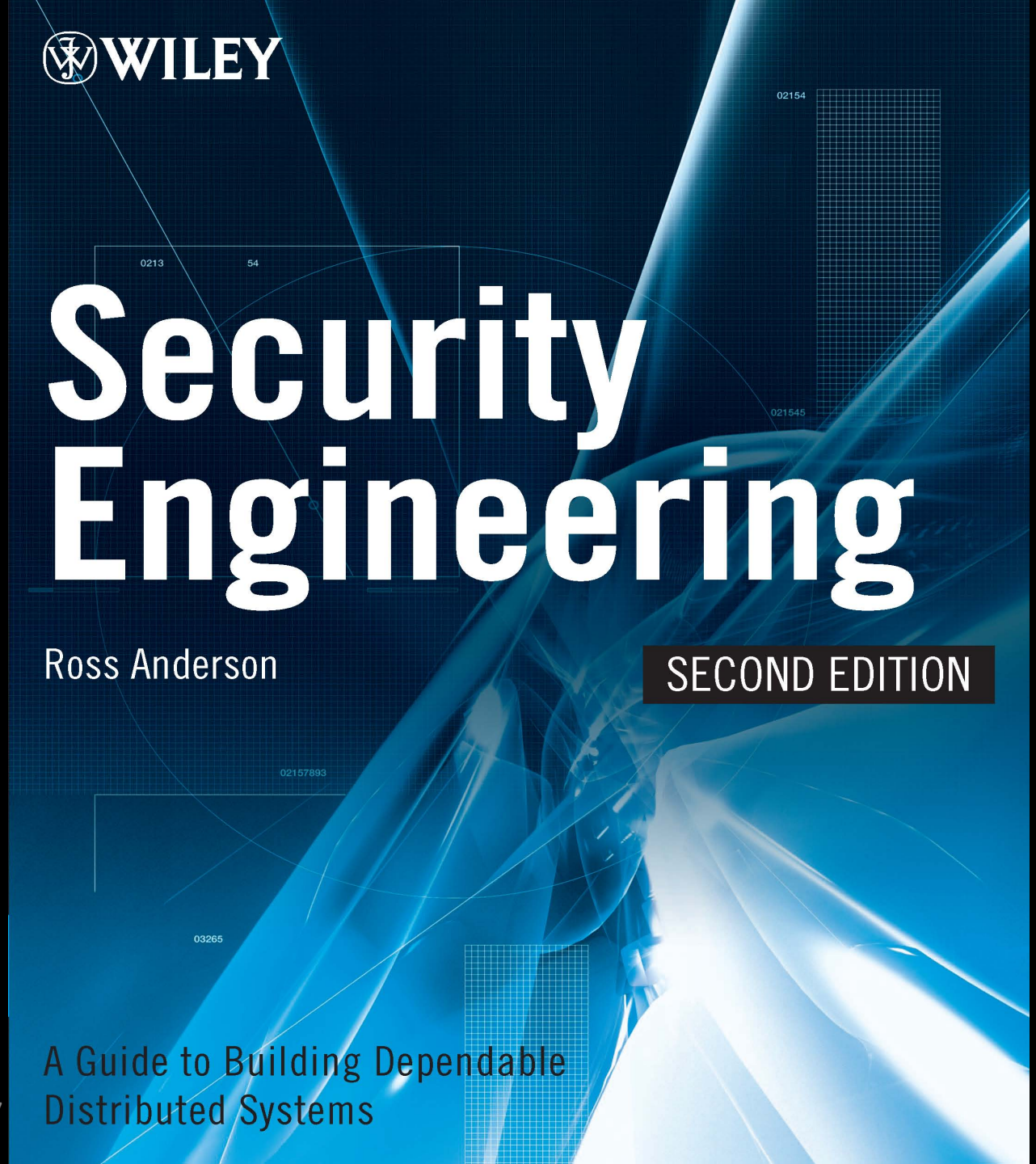
- Our paper "Standardisation and Certification in the Internet of Things" is on my web page

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

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

  https://www.lightbluetouchpaper.org

  which also has a couple of videos



CEPS, Sep 27 2017