What will security standardisation and certification look like ten years from now?

Ross Anderson, Cambridge
(with Éireann Leverett and
Richard Clayton)

How does IoT change safety?

- Eireann Leverett, Richard Clayton and I did a roject for EU Joint Research Centre Milan
- 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
- The lessons are much more widely applicable!

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 have to update safety regulation (and safety regulators) to cope?

Background

- Markets do safety in some industries (aviation) way better than others (cars, medical devices …)
- 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
- Some 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…)
- Challengers like Google, Tesla moving fast
- Tesla has already moved to regular software upgrades (one of which brought autonomy)
- Toyota says it'll fit all new cars with enough sensors; autonomy is then an upgrade away


CareFusion
Alaris® PC
PRIMARY INFUSION
RATE
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
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 (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 Member State regulators to do post-approval studies and adverse event reporting
- At present devices are typically approved on paperwork alone, without adequate testing and with no attention to usability

Background (4)

- Usability failures which kill are typically blamed on the nurse (if noticed at all)
- Attacks are very much harder to ignore!
- In 2015, the FDA ordered hospitals to stop using the Hospira Symbiq infusion pump, after demo of tampering over wifi
- They balked when researchers found 300 more products with similar issues
- Software upgrades can break certification!

Background (5)

- ENISA reports that the energy sector has one of the highest rates of attacks on CNI
- UK experience: after alarms about smart meter security, GCHQ engaged with the CNI threat but not the lower-level ones
- EU: NIS Directive
- But who's responsible for seeing to it that smart meters don't let the power company rip off the customer, or vice versa?

The Big Picture

- Europe has a multistakeholder approach with broad principles of liability, transparency and privacy plus specific industry requirements on testing and certification
- This system is about to get a really big shock!
- EU institutions will need more cybersecurity expertise to support safety, privacy, consumer protection and competition – not just the old-fashioned concerns around critical infrastructure

The Big Challenge

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

Many questions include…

- How will incentive structures evolve?
- How do we add post-market surveillance to pre-market testing?
- Who will investigate incidents, and to whom will they be reported?
- How do we bring safety engineers and security engineers together?
- Will EU regulators all have to hire security engineers, or do we need an expert agency?

Stresses and Strains

- Responsible disclosure failure – Volkswagen v Birmingham and Nijmegen universities
- The IT industry has learned how to cope
  - Security breach disclosure to align incentives
  - Responsible vulnerability disclosure for a learning system
  - Institutional support such as CERTs
- We now have standards (ISO 29147, 30111)
- To whom should academics report bugs in cars?

Research opportunities

- One problem will be long-term maintenance
- If navigation software being written in Cambridge now is installed in a Landrover in 2019, who will supply the patches in 2039?
- It's hard enough for Google to get Samsung to patch Android phones shipped in 2014 …
- Cars have dozens of CPUs in subsystems sold by multiple subcontractors

Institutional Players

- Dozens of European regulators (+ hundreds in Member States)
- Standards bodies (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

Detailed recommendations

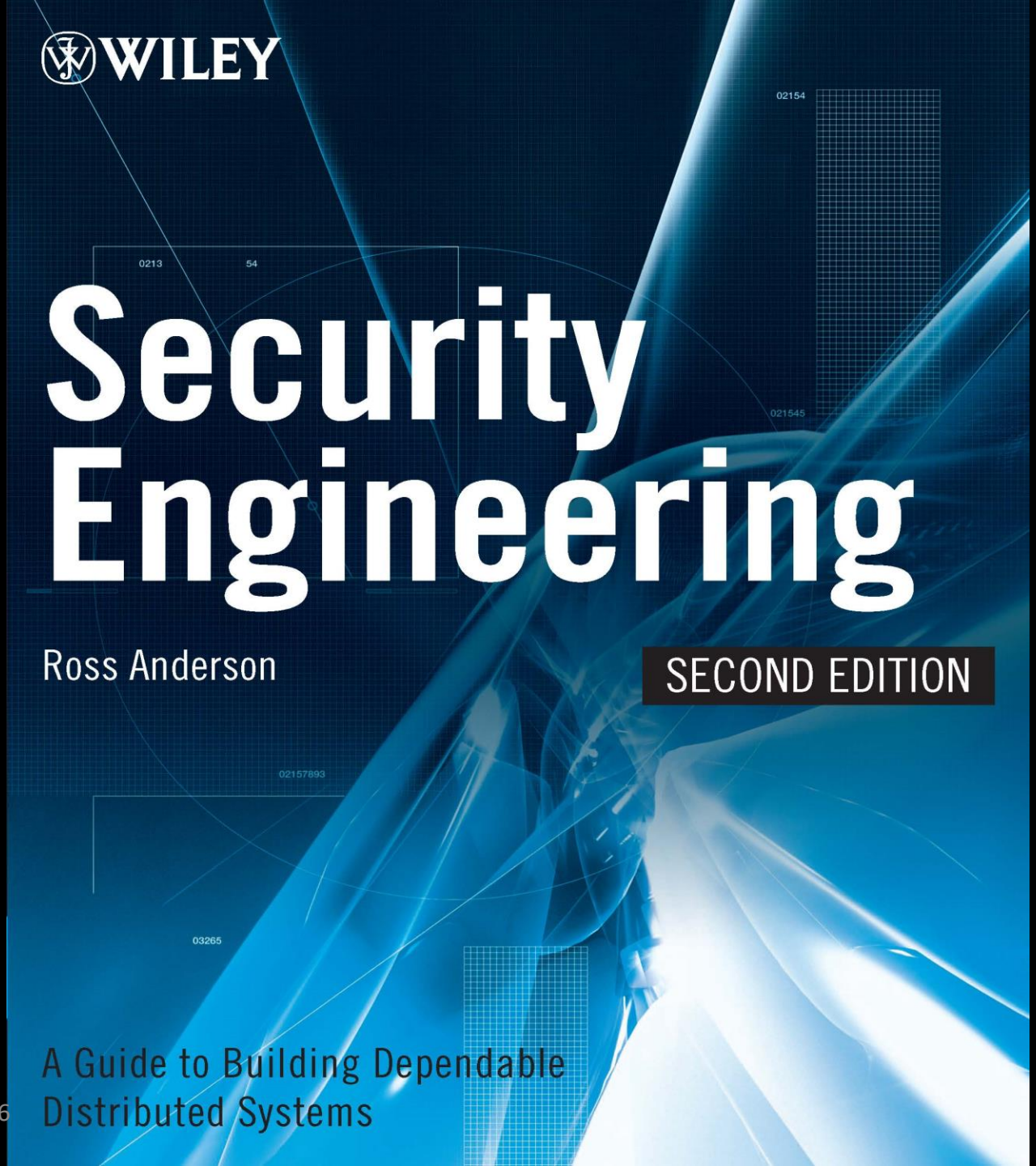
- Update Product Liability Directive to cope with systems that involve multiple products and services
- Require vendors to self-certify, for their CE mark, that products are secure by default, and can be updated if need be
- Update NIS Directive to report breaches and vulnerabilities to safety regulators and users
- Move safety standards bodies towards assessing security and safety together

Detailed recommendations (2)

- Safety regulators should require a secure development lifecycle with documented vulnerability management following ISO 29174 and ISO 30111 at a minimum
- We have to move from certifying products to assurance of whole systems including the patch cycle
- Create a European Security Engineering Agency to support policymakers and regulators

What's the vision?

- US engineers see Europe as the world's privacy regulator – since Washington doesn't care and nobody else is big enough to matter
- In ten years' time, Europe should be the world's safety regulator too
- To do that we need to adapt our structures to cope with safety and security together, and with monthly updates too



London, Dec 6 2016