EMBEDDED SYSTEMS SAFETY & SECURITY

Dangerous Flaws in Safety-Critical Device Design

Michael Barr

ESC Boston 2017

@barrgroup

About Michael Barr

Co-founder and CTO, **Barr Group**

Experienced implementer of embedded systems and software

- B.S. and M.S. degrees in electrical engineering

Testifying expert witness

- Security of encrypted communications
- Patent validity and infringement
- Software copyright and trade secrets
- Product liability

Former adjunct professor, University of Maryland

Former editor-in-chief, *Embedded Systems Programming*

- Author of 3 books and more than 70 articles and papers

@embeddedbarr

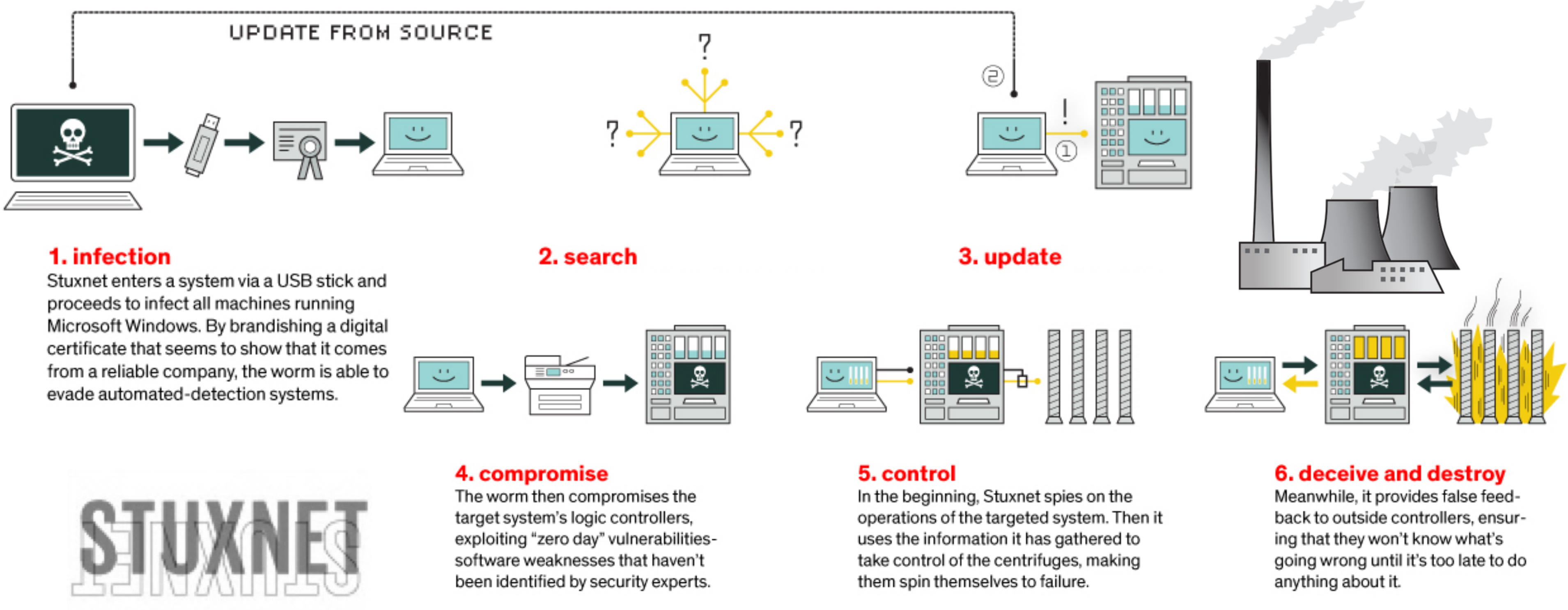
“May You Live in Interesting Times”

Embedded systems are an emerging battlefield

- Anonymous hackers live safely behind locked doors
- Meanwhile able to attack innocents across the globe

Hostile governments are among many potential threats…

Industrial Controls: Hacked!



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search

3. update

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

Critical Infrastructure: Hacked!

Electricity blackout in Eastern Ukraine

- December 23, 2015
- More than 1,000,000 homes and businesses affected

How perpetrated?

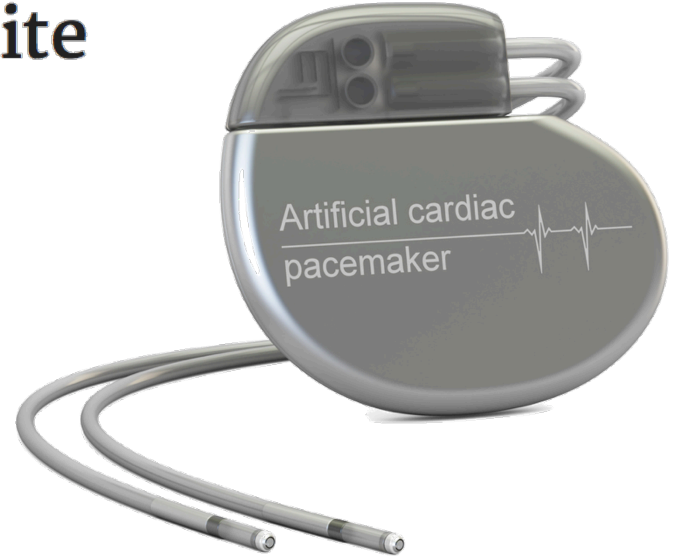
- BlackEnergy virus + remote SSH shutdown + KillDisk
- Believed to be the work of Russia

Implantable Devices: Hacked!

Security holes enable attackers to switch off pacemakers, rewrite firmware from 30 feet away.

The effect of the wireless attacks could not be overstated — in a speech at the BreakPoint security conference in Melbourne today, Jack said such attacks were tantamount to “anonymous assassination”, and in a realistic but worse-case scenario, “mass murder”.

In a video demonstration, which Jack declined to release publicly because it may reveal the name of the manufacturer, he issued a series of 830 volt shocks to the pacemaker using a laptop.



Connected Cars: Hacked!

https://www.wired.com/2016/08/
jeep-hackers-return-high-speed-steering-acceleration-hacks/

Botnets, Viruses and Worms: Oh, My!

Mirai

- Linux worm infecting embedded systems right now
  - Via telnet and default username+password combos
- Together a million-strong "botnet"
  - Primarily routers and security cameras, by numbers

BrickerBot

- Similar entry but targeting BusyBox Linux specifically
- Wipes the file-system: a "*Permanent Denial of Service*"

And many more to come…

The Future as it Could Be

Smart, energy-efficient homes anticipate our every need

Improved longevity and health

- Including via continuous health monitoring and remote medical care

Self-driving cars and trucks zip along smart highways

- Saving lives while reducing congestion

Fully automated production of food, energy, and more

- Potentially eliminating poverty, starvation, homelessness, and war

The Internet of Things ("IoT")

Gartner: "25 billion Internet-connected 'things' by 2020"

- *"physical objects [with] embedded technology to sense or interact"*

✓ Utilities
✓ Manufacturing
✓ Government
✓ Transportation
✓ Medical
✓ Consumer

Huawei: 100 billion by 2025

“Embedded Systems Safety & Security Survey”

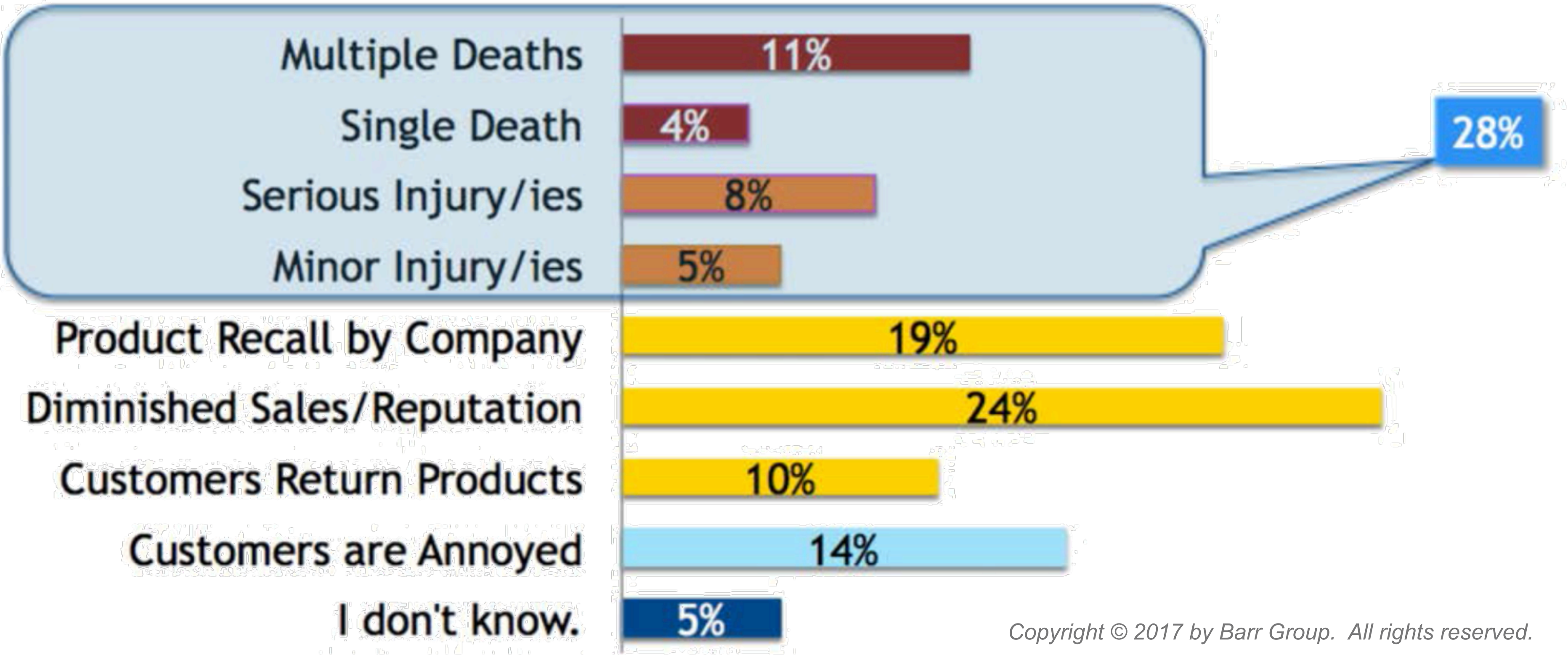
BARR group

2017 - Qualified: 1,726

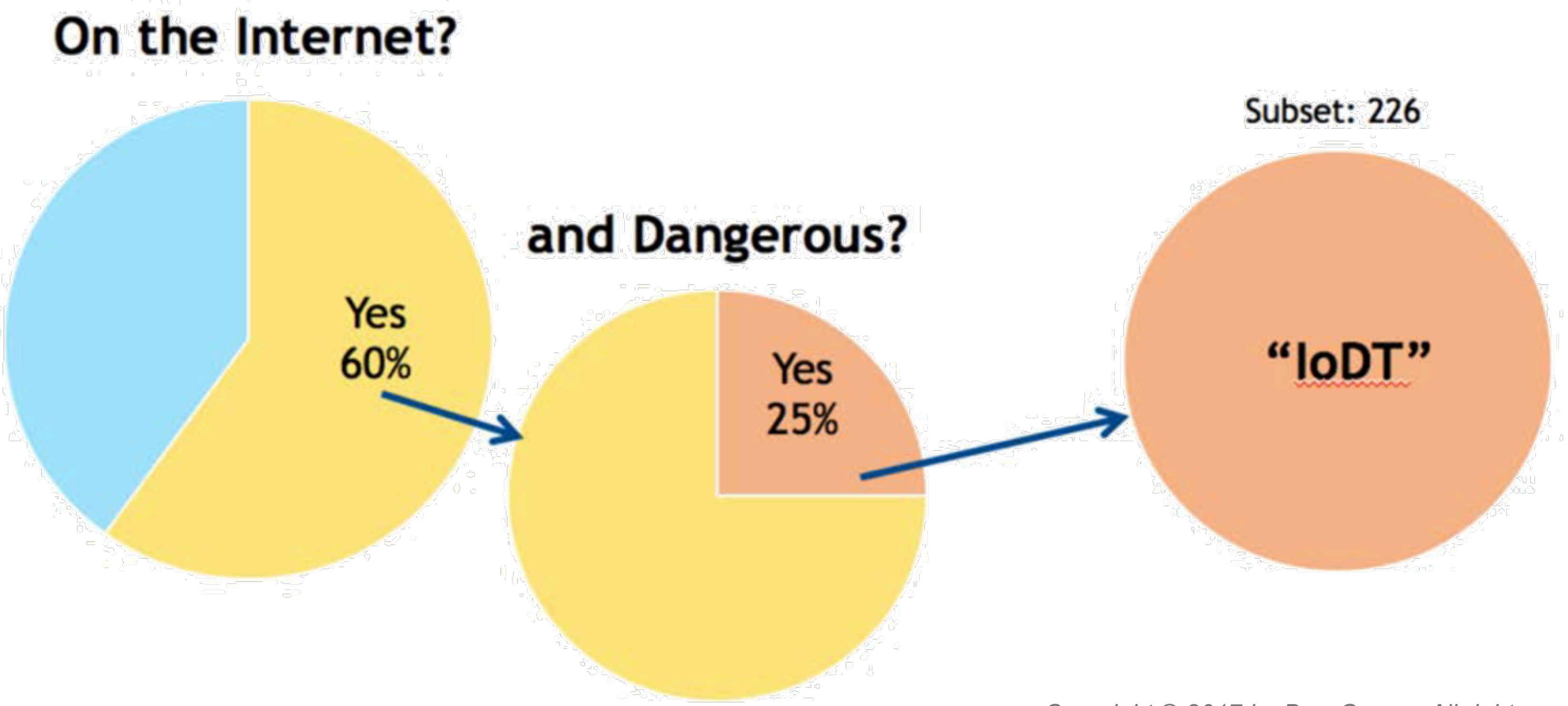
US & Canada	52%
Europe	27%
Asia	12%
Rest of World	9%

https://barrgroup.com/Embedded-Systems/Surveys/2017-embedded-systems-safety-security-survey

Safety-Critical Systems



The Internet of DANGEROUS Things



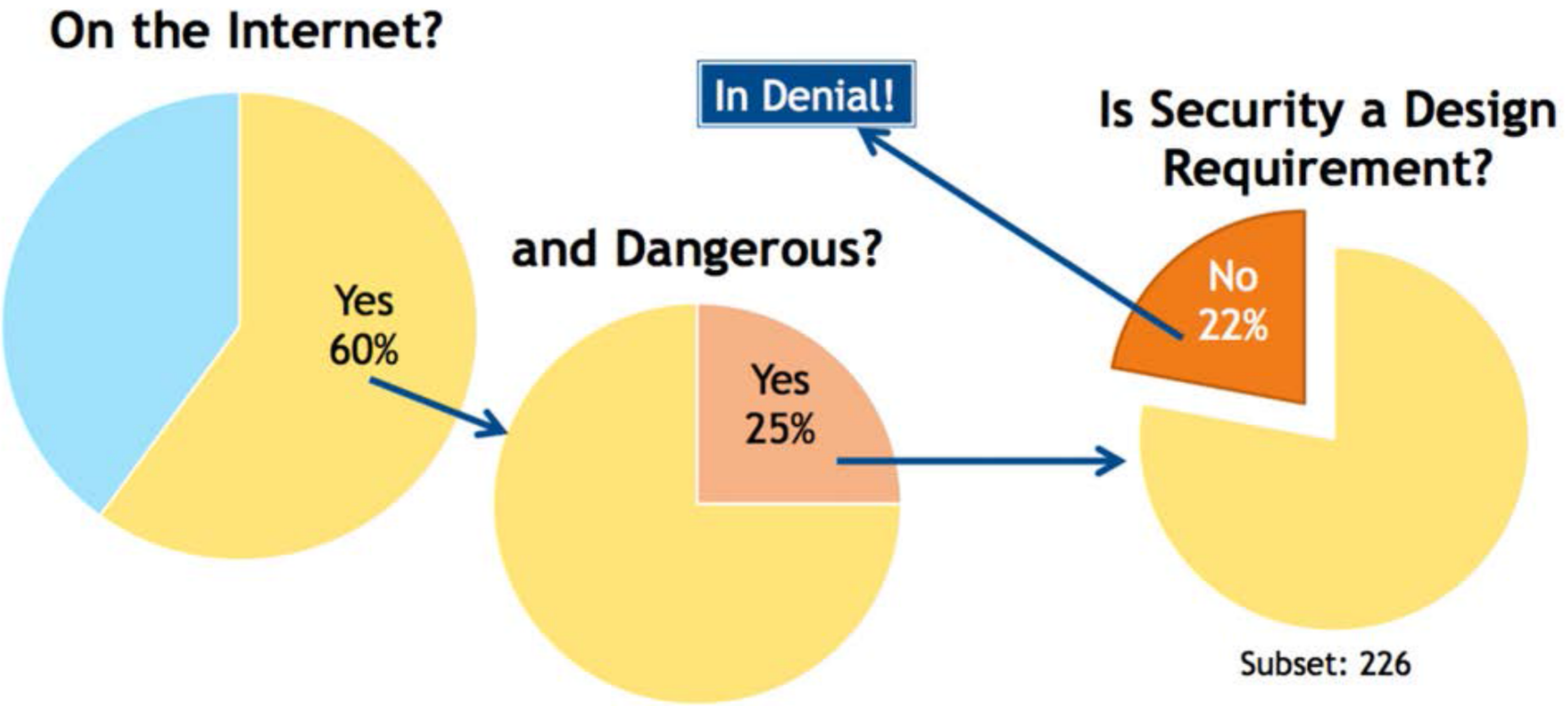
On the Internet?

and Dangerous?

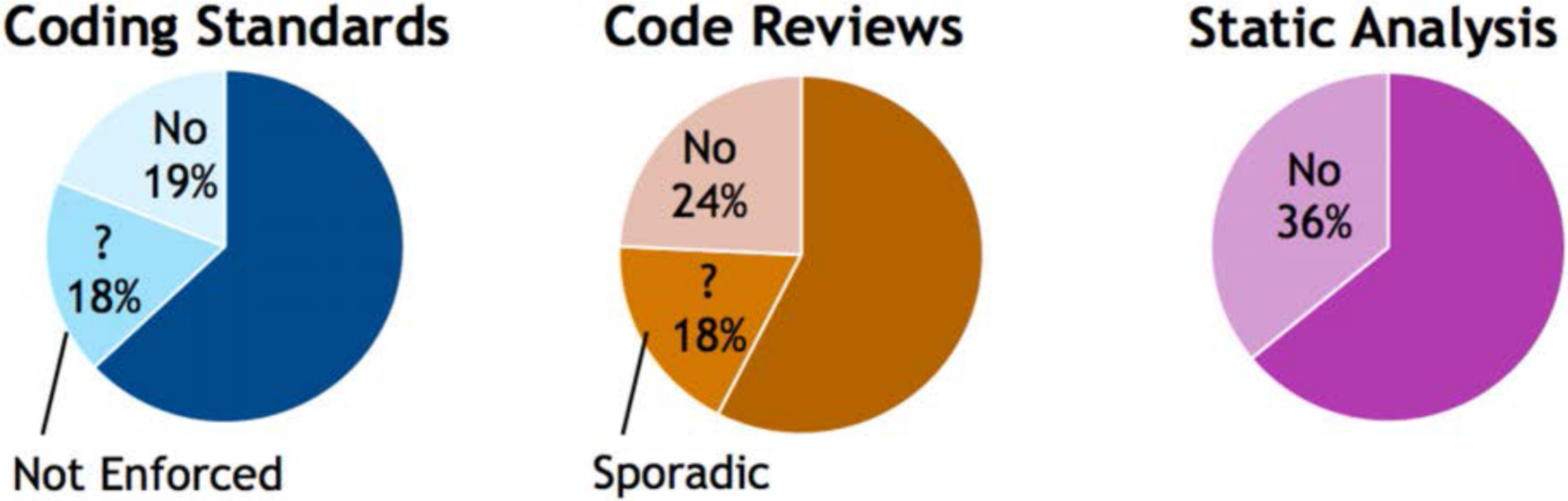
Subset: 226

Should Dangerous Things Include Security Features?

Too Many Heads in the Sand!



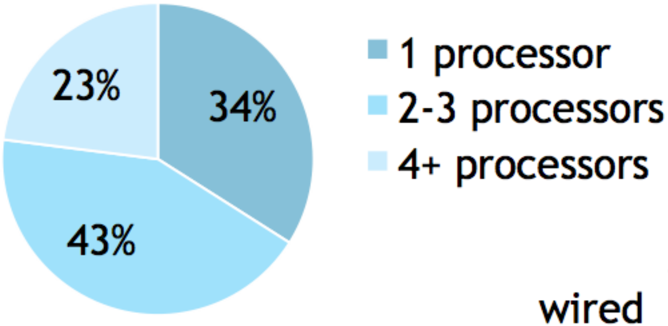
Too Little Use of Best Practices

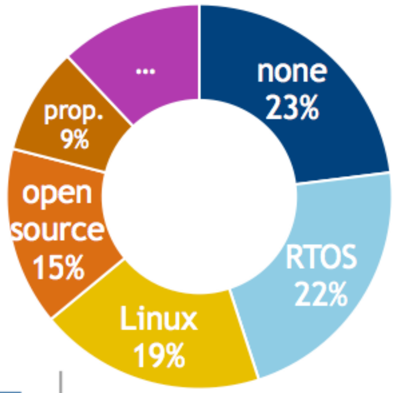


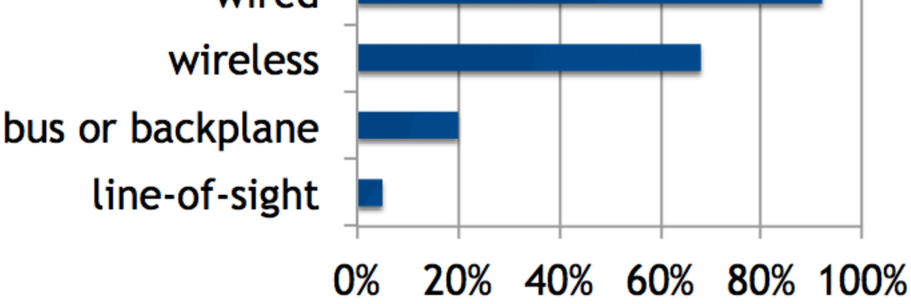
What Would You Say If Security Was Ignored?

No “One-Size Fits” Solutions

Architectural Variations…







Strategic Challenges

Security is always an arms race

- Long-lived products eventually computationally disadvantaged
- No path to upgrade already vast networks of insecure devices

Some systems MUST be super cheap

- Many “smart” devices can only emerge at minimal cost
  - Hence: 8- and16-bit microcontrollers still sell in the billions/year
  - e.g., TPMS tire pressure sensor in every wheel of every vehicle
- Not every embedded system can bear all costs of security

Aside: How to Prevent Stolen Cars?

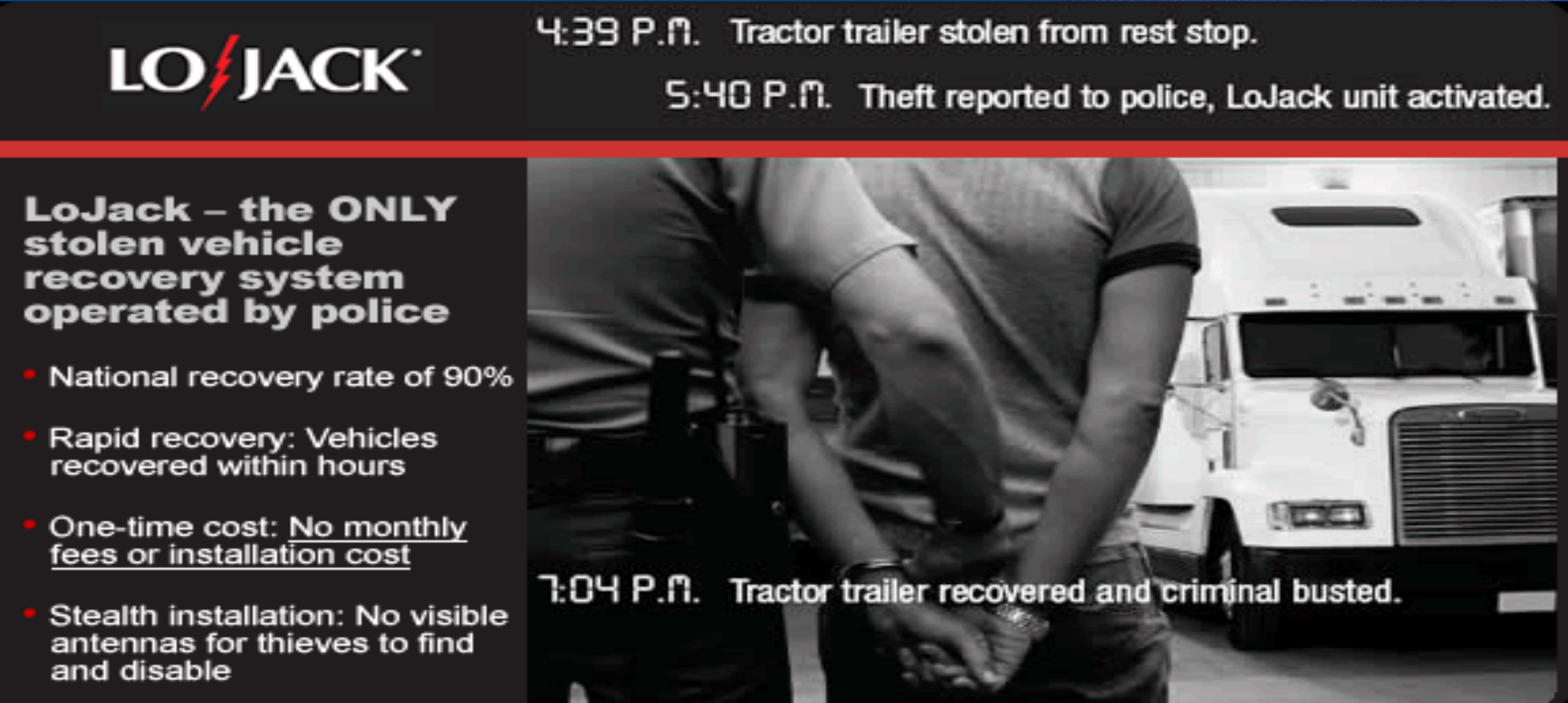
Concept: individually secure each vehicle

- Sensor-based alarm systems
- Locking steering columns
- Add-on devices like The Club →

Cost born by every owner

- But only ever achieves “more secure than the next guy”

Alternative: Detect and Respond



LOJACK

4:39 P.M. Tractor trailer stolen from rest stop.

5:40 P.M. Theft reported to police, LoJack unit activated.

LoJack – the ONLY stolen vehicle recovery system operated by police

- National recovery rate of 90%
- Rapid recovery: Vehicles recovered within hours
- One-time cost: No monthly fees or installation cost
- Stealth installation: No visible antennas for thieves to find and disable

7:04 P.M. Tractor trailer recovered and criminal busted.

Externalizing Embedded Security

Remote hacks require packet exchange…

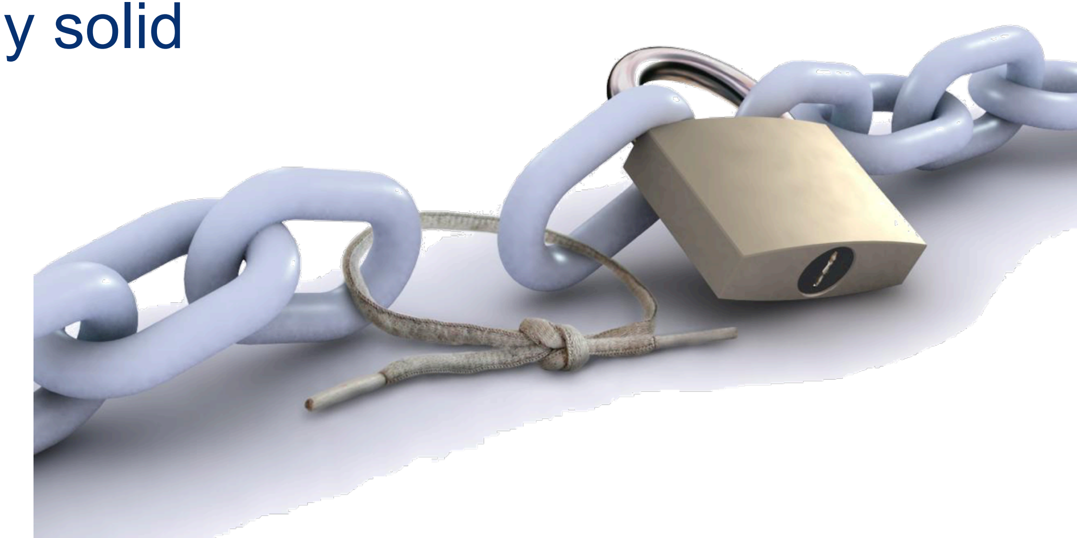
Concept: “LoHack”

- Prevent
  - Opt-in network firewalls (e.g., for cars, hospitals, etc.)
- Detect
  - Honeypots (run by device makers)
  - Cloud-based data traffic analysis and learning algorithms
- React
  - Firewall updates PLUS coordination with law enforcement

Image: https://www.ixiacom.com/solutions/iot

Isn’t Encrypting Data Good Enough?

Crypto (the math) is usually solid



But crypto can be broken

- Bugs in implementation
- Holes in protocols
- Backdoors
- Leaked keys

And crypto will never be the only link in your security…

How Hackers Think

What is the goal?

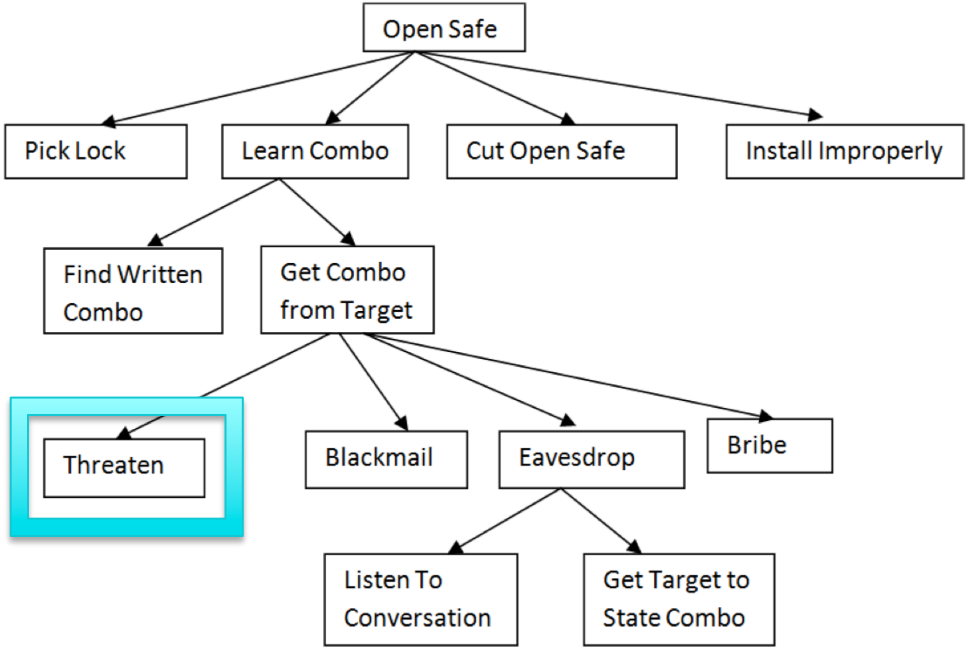
Which path is easiest for me?

My skills, my tools/assets, etc.

How could I get caught?

And what's the worst that happens?

Is it worth the risk (to me)?



Action Plan

1. DON'T ignore security: We have an ethical duty!

   ACM Code of Ethics, Rule 1.2: "Avoid harm to others. …"

   IEEE Code of Ethics, Rule 1: "to accept responsibility in making decisions consistent with the safety, health, and welfare of the public"

2. DO adopt (bug-reducing) software best practices
3. DO use cryptography where appropriate
4. DO practice defense in depth
5. DO get and stay educated about security

About Barr Group

BARR group

Mission: "*Help as many engineers as possible design <u>safer, more reliable, and more secure</u> embedded systems*"

Expertise and services

- Product **safety and security** audits and guidance
- **Process and architecture** reviews and improvements
- Public and private **training courses** in best practices
- **Engineering design assistance** with electronics and software

@barrgroup