26: Security

Projects

- Great work on milestone presentations!
  - I will try to read through the reports by the end of next week
- Next steps
  - Keep working towards final demo
  - Keep fleshing out and updating documentation
  - Soon: modeling and verification

Security

Safety is about system failing without an attacker model

Security is about system failing because of adversarial actions

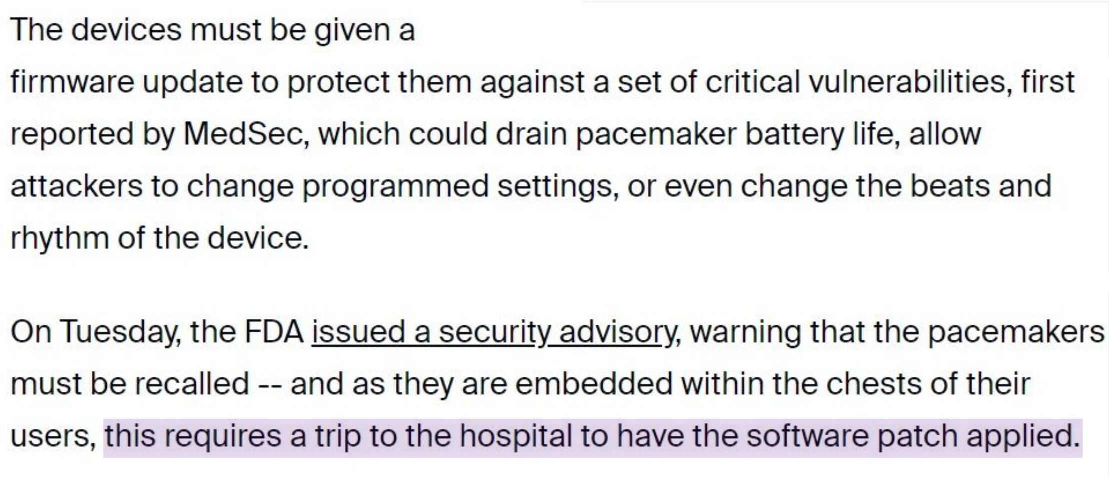
What special considerations do we have to make when thinking about security for embedded systems?

FDA issues recall of 465,000 St. Jude pacemakers to patch security holes

Heart patients will have to visit their doctors to have their pacemakers patched for the "voluntary" recall -- but there are risks.

It seems such an odd concept at first, but with many kinds of pacemakers now "smarter," with connections to mobile devices and diagnostic systems, the avenue has been carved for these medical devices to potentially be tampered with, should a threat actor choose.

In particular, Abbott's pacemakers, formerly of St. Jude Medical, have been "recalled" by the US Food and Drug Administration (FDA) on a voluntary basis.



The devices must be given a firmware update to protect them against a set of critical vulnerabilities, first reported by MedSec, which could drain pacemaker battery life, allow attackers to change programmed settings, or even change the beats and rhythm of the device.

On Tuesday, the FDA issued a security advisory, warning that the pacemakers must be recalled -- and as they are embedded within the chests of their users, this requires a trip to the hospital to have the software patch applied.

source

It’s not just software….

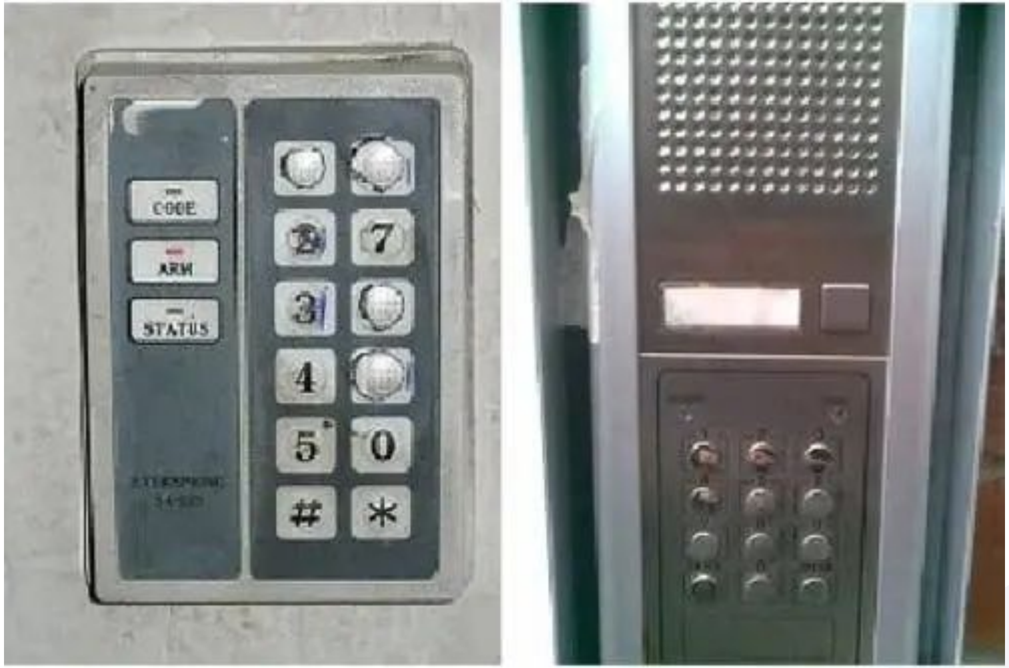
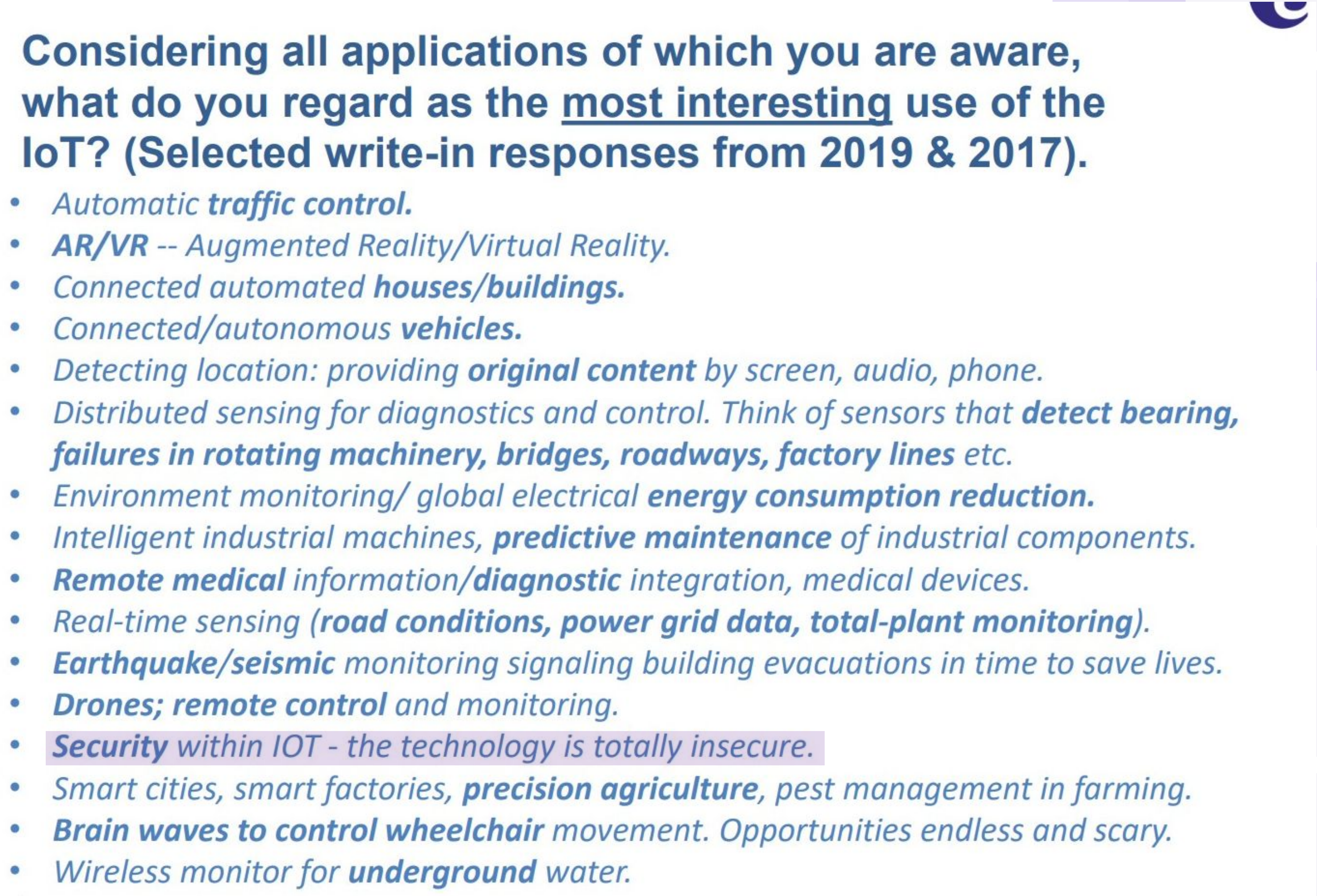


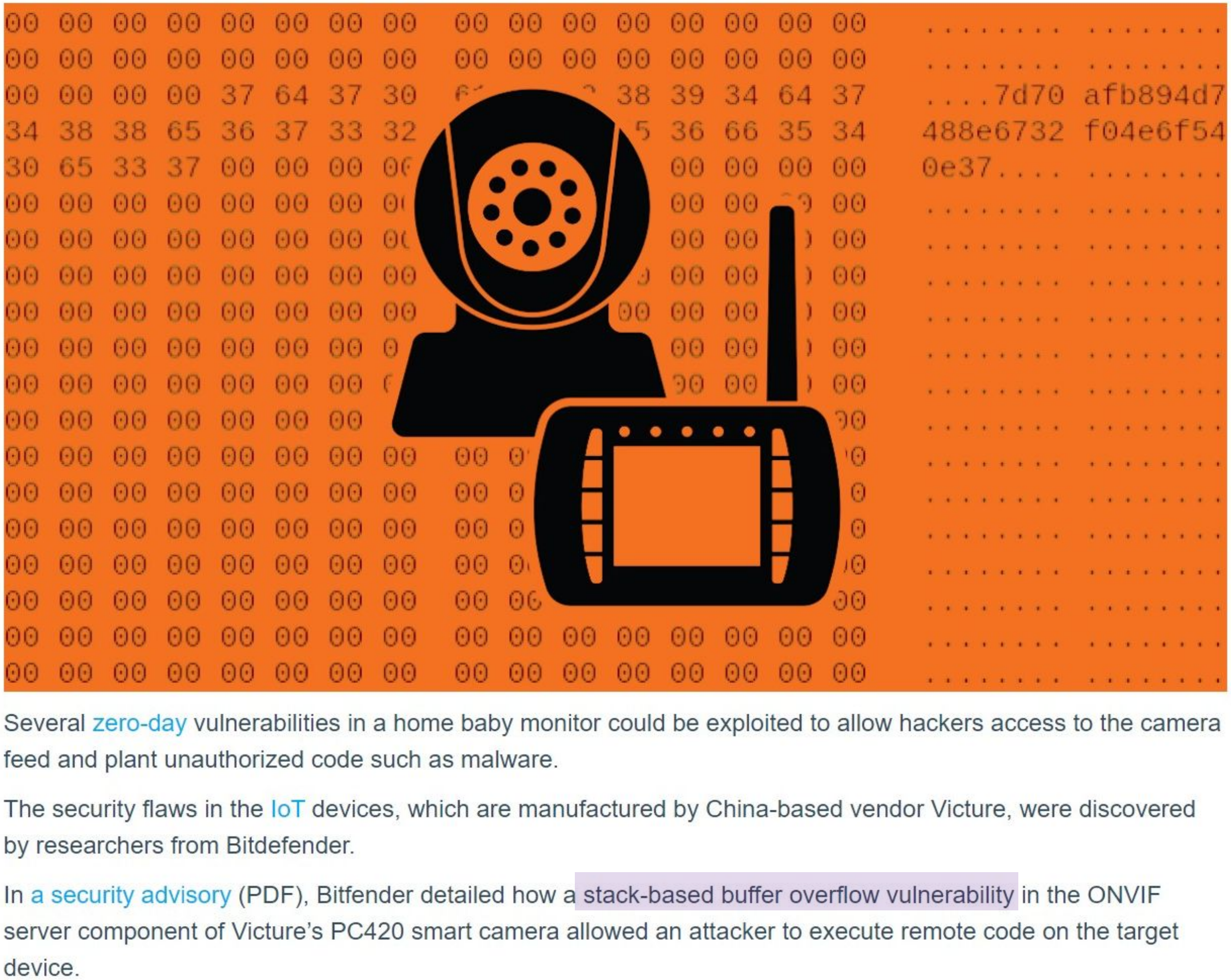
Image source



Considering all applications of which you are aware, what do you regard as the most interesting use of the IoT? (Selected write-in responses from 2019 & 2017).

- *Automatic **traffic control.***
- ***AR/VR** -- Augmented Reality/Virtual Reality.*
- *Connected automated **houses/buildings.***
- *Connected/autonomous **vehicles.***
- *Detecting location: providing **original content** by screen, audio, phone.*
- *Distributed sensing for diagnostics and control. Think of sensors that **detect bearing, failures in rotating machinery, bridges, roadways, factory lines** etc.*
- *Environment monitoring/ global electrical **energy consumption reduction.***
- *Intelligent industrial machines, **predictive maintenance** of industrial components.*
- ***Remote medical** information/**diagnostic** integration, medical devices.*
- *Real-time sensing (**road conditions, power grid data, total-plant monitoring**).*
- ***Earthquake/seismic** monitoring signaling building evacuations in time to save lives.*
- ***Drones; remote control** and monitoring.*
- ***Security** within IOT - the technology is totally insecure.*
- *Smart cities, smart factories, **precision agriculture**, pest management in farming.*
- ***Brain waves to control wheelchair** movement. Opportunities endless and scary.*
- *Wireless monitor for **underground** water.*

source

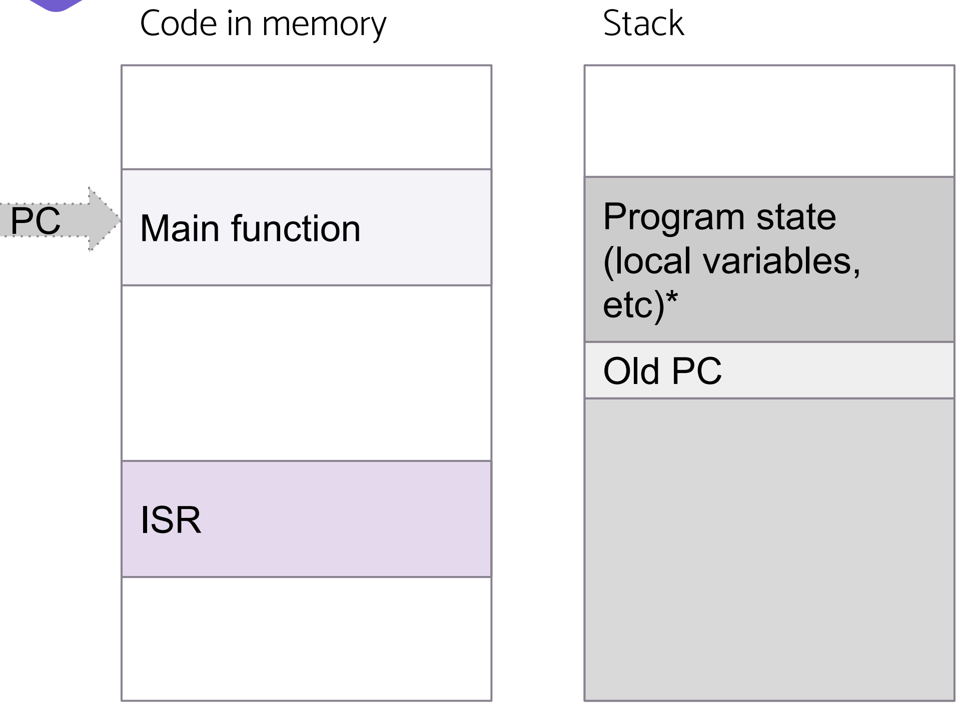


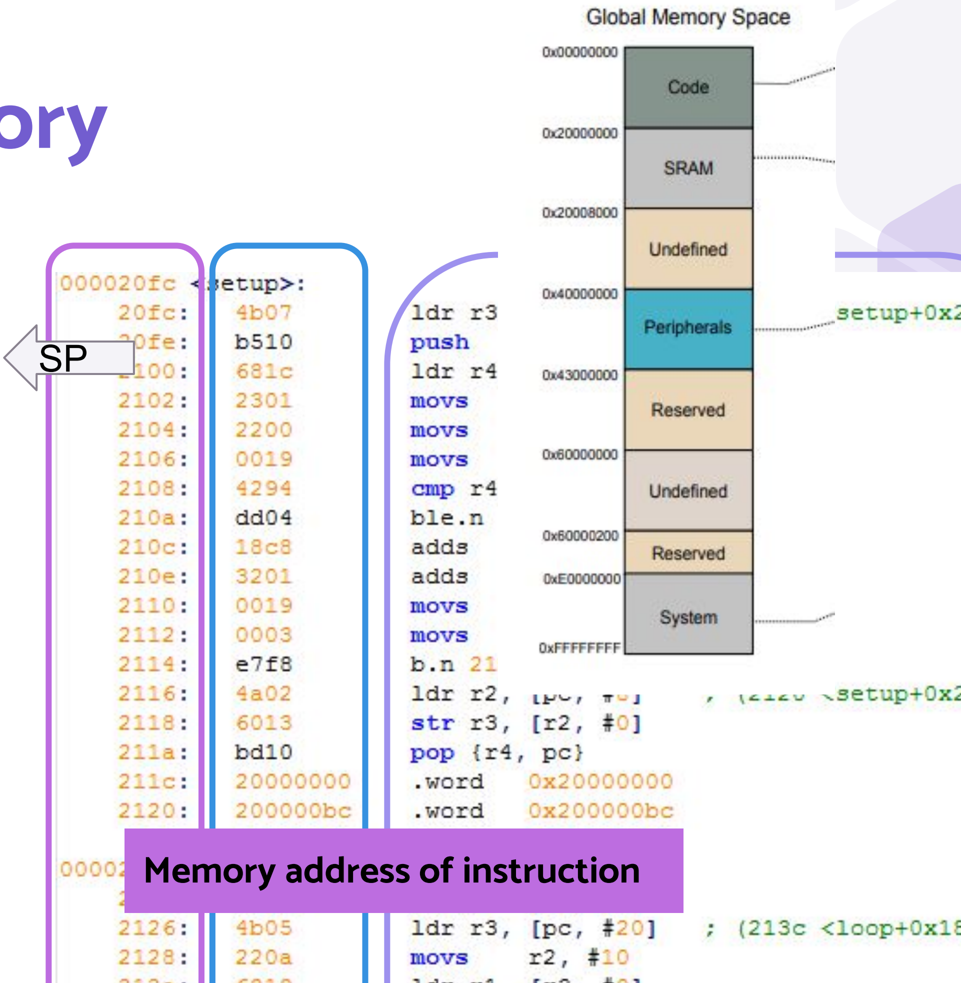
Several zero-day vulnerabilities in a home baby monitor could be exploited to allow hackers access to the camera feed and plant unauthorized code such as malware.

The security flaws in the IoT devices, which are manufactured by China-based vendor Victure, were discovered by researchers from Bitdefender.

In a security advisory (PDF), Bitfender detailed how a stack-based buffer overflow vulnerability in the ONVIF server component of Victure's PC420 smart camera allowed an attacker to execute remote code on the target device.

Review: code in memory

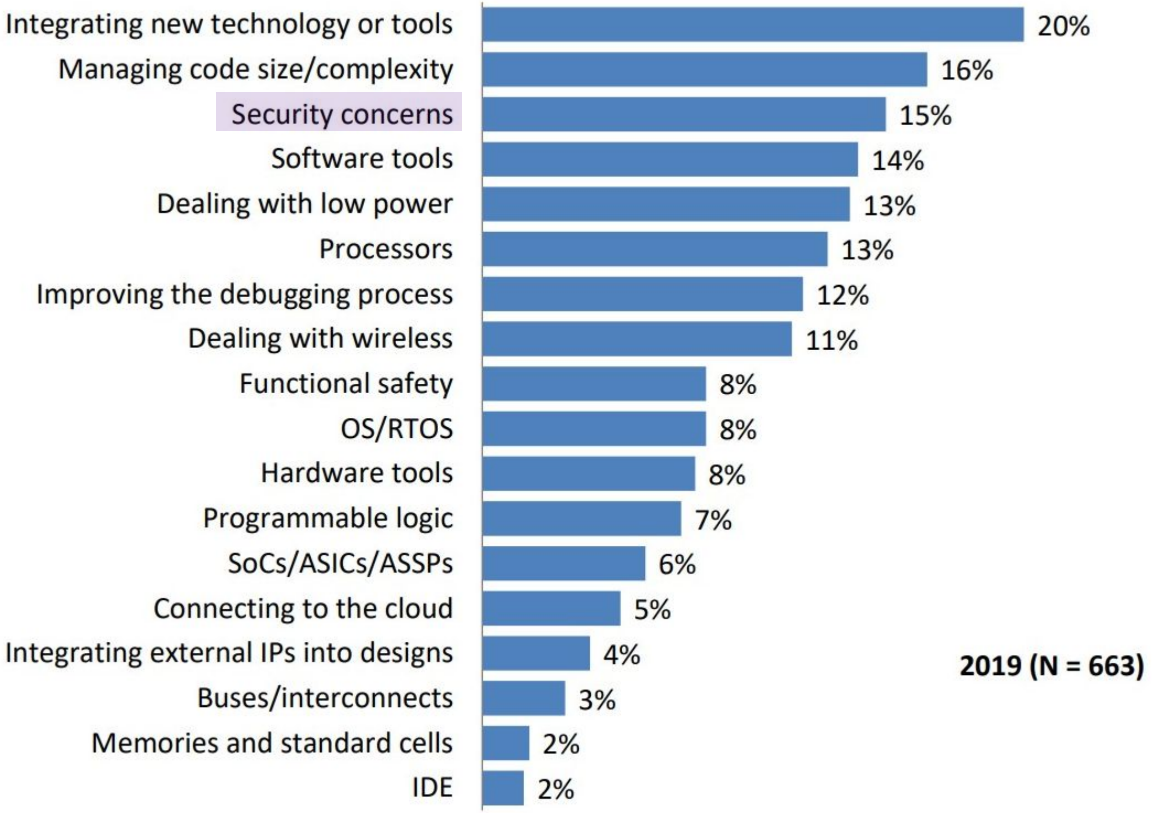


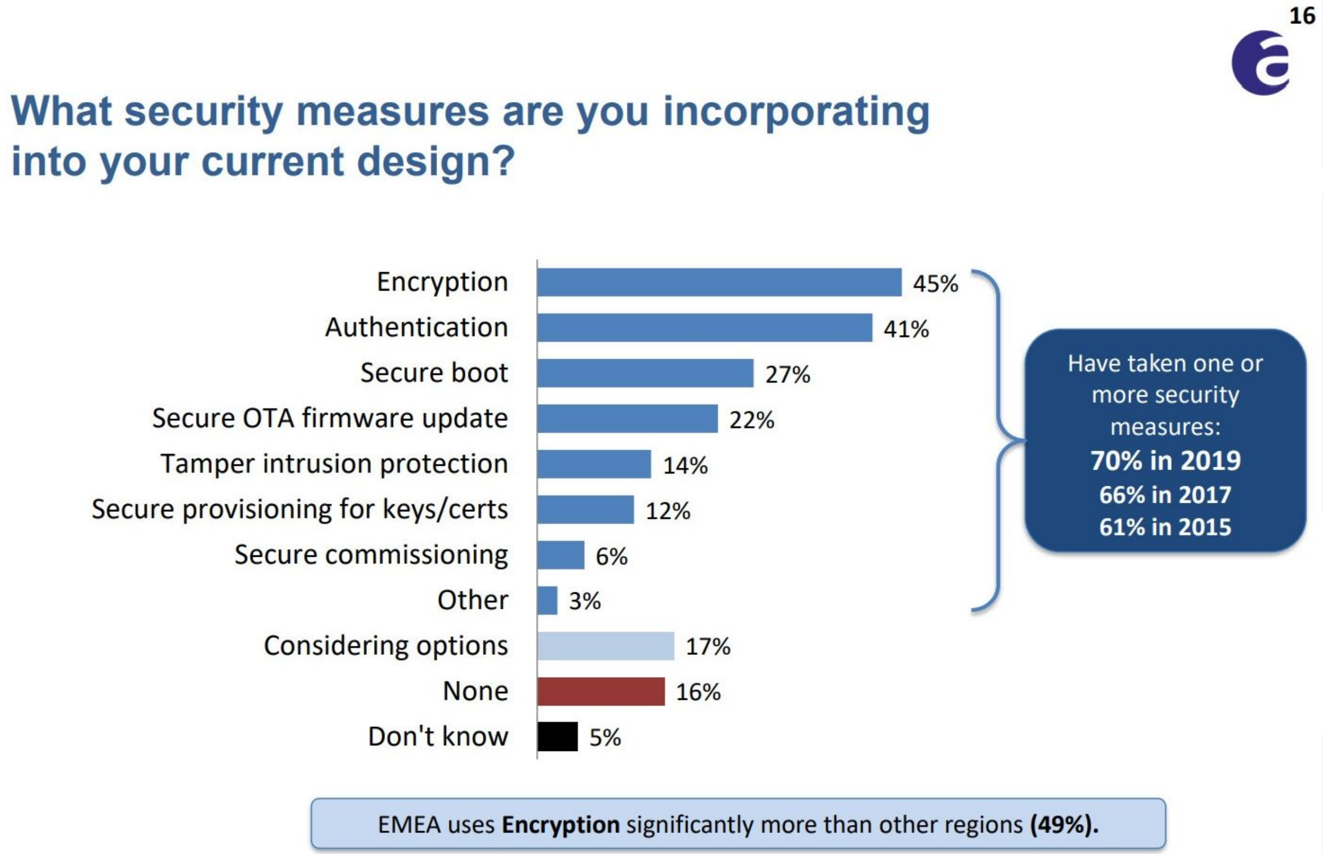


```
000020fc <setup>:
    20fc:   4b07        ldr r3
    20fe:   b510        push
    2100:   681c        ldr r4
    2102:   2301        movs
    2104:   2200        movs
    2106:   0019        movs
    2108:   4294        cmp r4
    210a:   dd04        ble.n
    210c:   18c8        adds
    210e:   3201        adds
    2110:   0019        movs
    2112:   0003        movs
    2114:   e7f8        b.n 21
    2116:   4a02        ldr r2,                    setup+0x2
    2118:   6013        str r3, [r2, #0]
    211a:   bd10        pop {r4, pc}
    211c:   20000000    .word   0x20000000
    2120:   200000bc    .word   0x200000bc

0000
    2126:   4b05        ldr r3, [pc, #20]    ; (213c <loop+0x1
    2128:   220a        movs     r2, #10
```

Thinking about the next year, what areas will be your greatest technology challenges?





What security measures are you incorporating into your current design?

Have taken one or more security measures:
70% in 2019
66% in 2017
61% in 2015

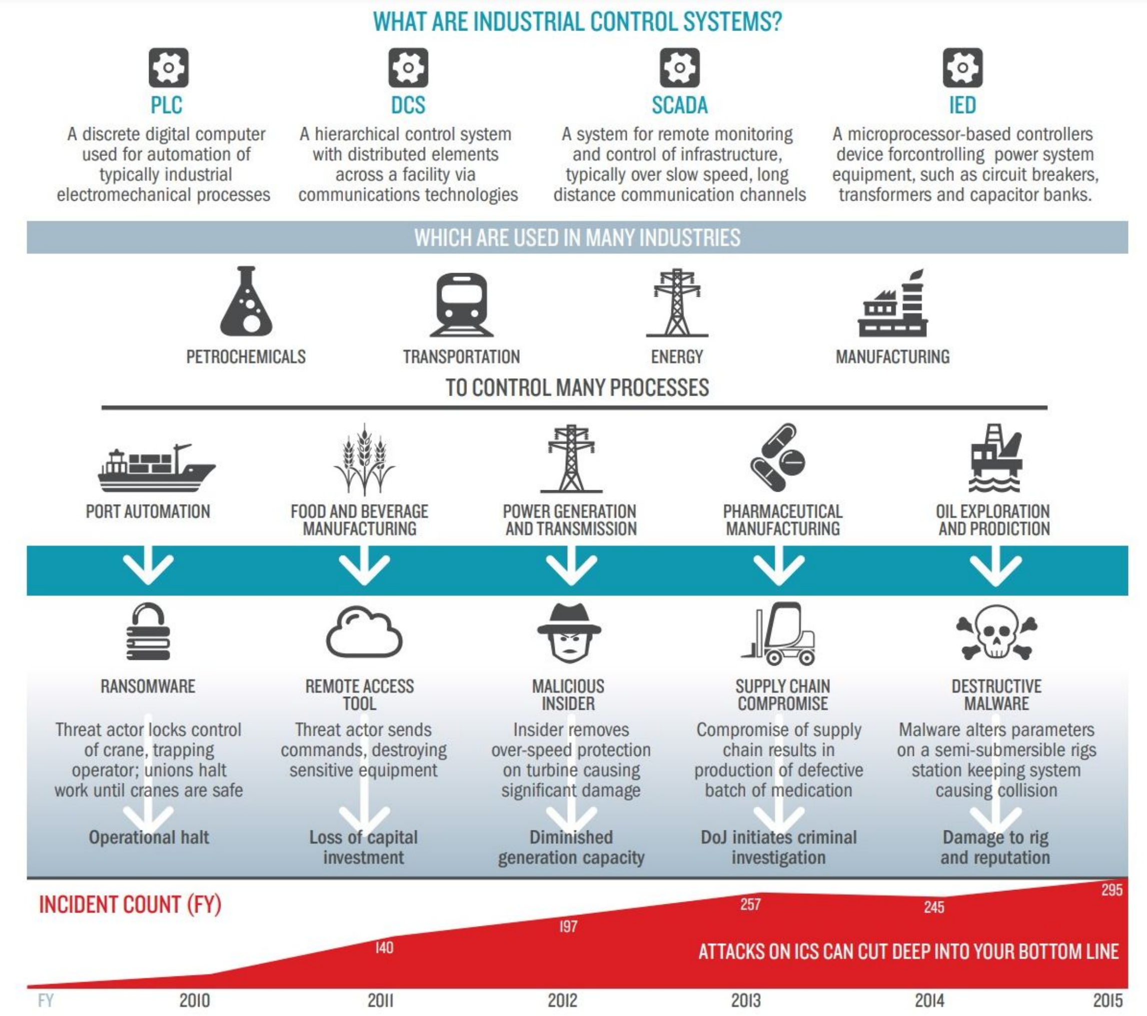
EMEA uses **Encryption** significantly more than other regions **(49%).**

Safety plans

- Requirements
- Threats
- Vulnerabilities
- Mitigation
- Validation

Security requirements: CIA

- Confidentiality: is data released?
- Integrity: is data tampered with?
- Availability: is the system down?



WHAT ARE INDUSTRIAL CONTROL SYSTEMS?

PLC
A discrete digital computer used for automation of typically industrial electromechanical processes

DCS
A hierarchical control system with distributed elements across a facility via communications technologies

SCADA
A system for remote monitoring and control of infrastructure, typically over slow speed, long distance communication channels

IED
A microprocessor-based controllers device forcontrolling power system equipment, such as circuit breakers, transformers and capacitor banks.

WHICH ARE USED IN MANY INDUSTRIES

PETROCHEMICALS
TRANSPORTATION
ENERGY
MANUFACTURING

TO CONTROL MANY PROCESSES

PORT AUTOMATION	FOOD AND BEVERAGE MANUFACTURING	POWER GENERATION AND TRANSMISSION	PHARMACEUTICAL MANUFACTURING	OIL EXPLORATION AND PRODICTION
RANSOMWARE	REMOTE ACCESS TOOL	MALICIOUS INSIDER	SUPPLY CHAIN COMPROMISE	DESTRUCTIVE MALWARE
Threat actor locks control of crane, trapping operator; unions halt work until cranes are safe	Threat actor sends commands, destroying sensitive equipment	Insider removes over-speed protection on turbine causing significant damage	Compromise of supply chain results in production of defective batch of medication	Malware alters parameters on a semi-submersible rigs station keeping system causing collision
Operational halt	Loss of capital investment	Diminished generation capacity	DoJ initiates criminal investigation	Damage to rig and reputation

INCIDENT COUNT (FY)

source

Threats

Securing a system is challenging:

- Have to actively prevent all attacks, while attacker only has to find one way in
- Attackers can be highly motivated and have many resources (ex. nation-states)

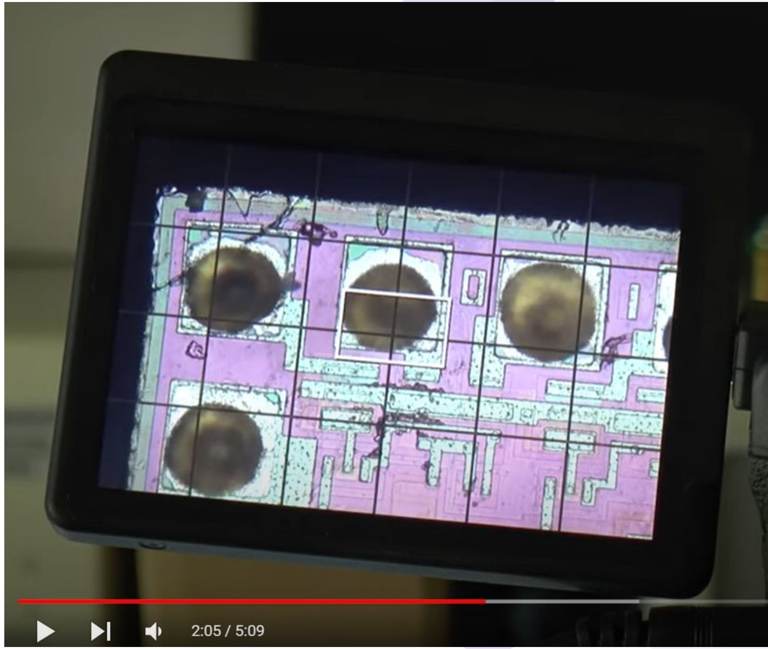
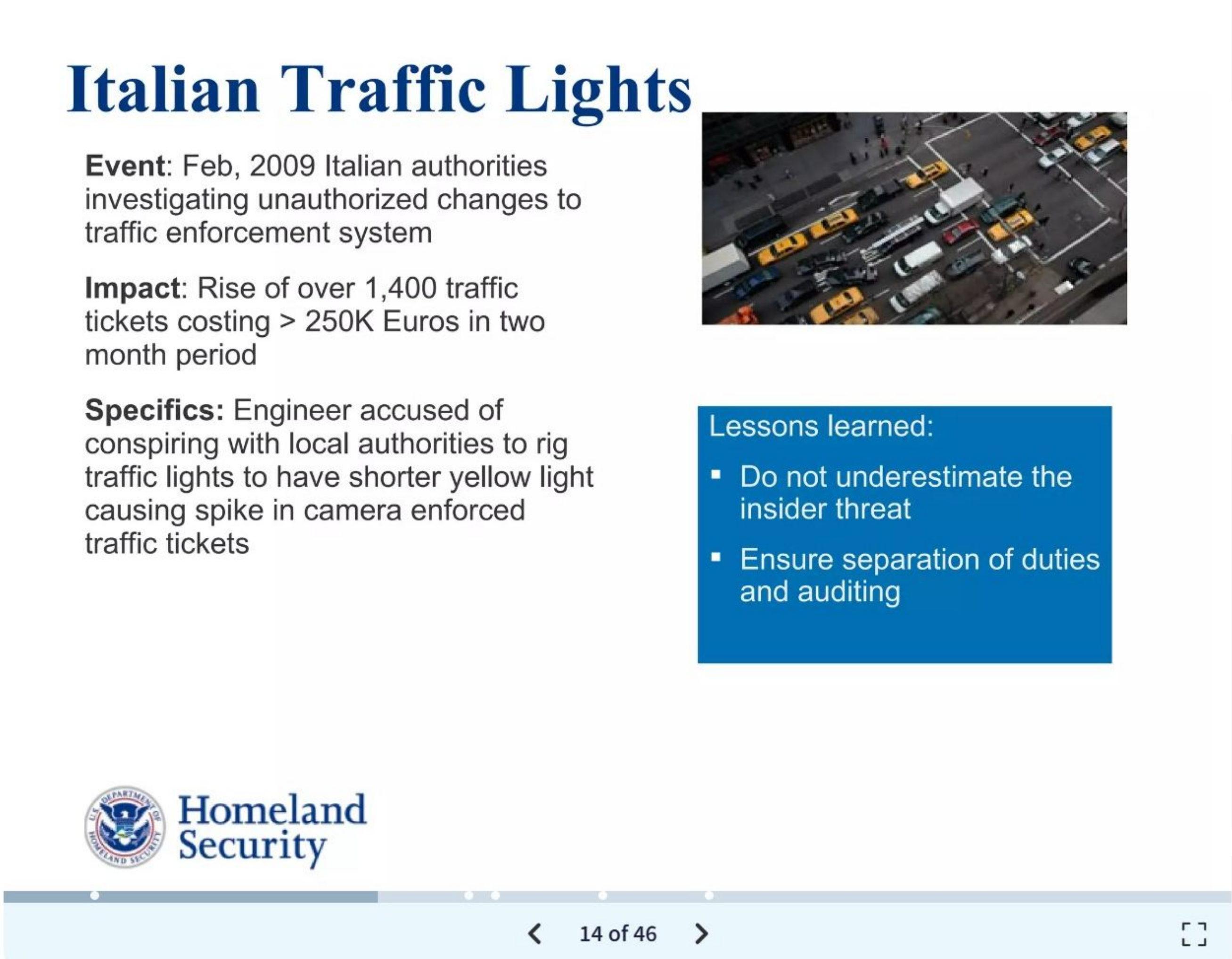


Image source



Italian Traffic Lights

Event: Feb, 2009 Italian authorities investigating unauthorized changes to traffic enforcement system

Impact: Rise of over 1,400 traffic tickets costing > 250K Euros in two month period

Specifics: Engineer accused of conspiring with local authorities to rig traffic lights to have shorter yellow light causing spike in camera enforced traffic tickets

Lessons learned:

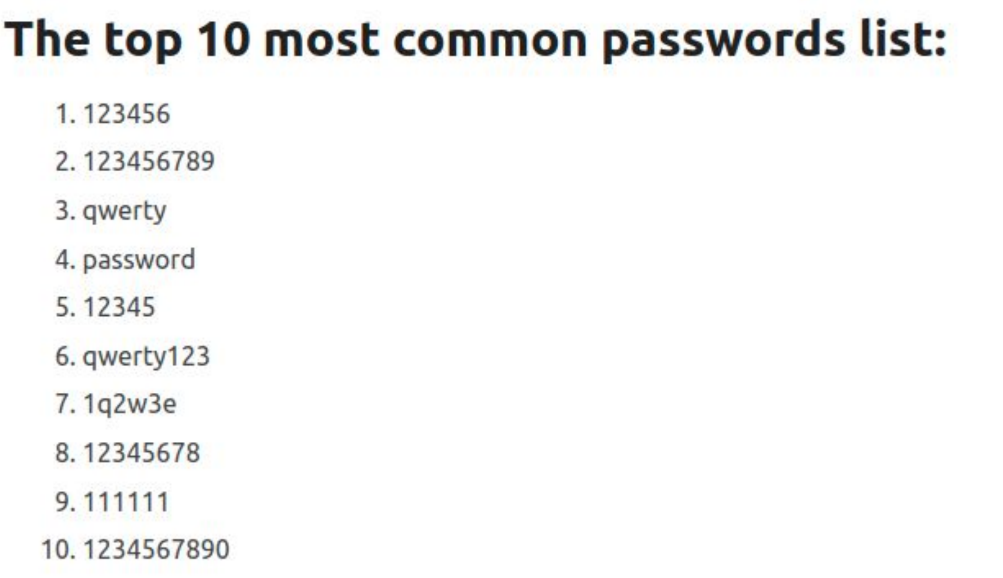
- Do not underestimate the insider threat
- Ensure separation of duties and auditing

Homeland Security

source

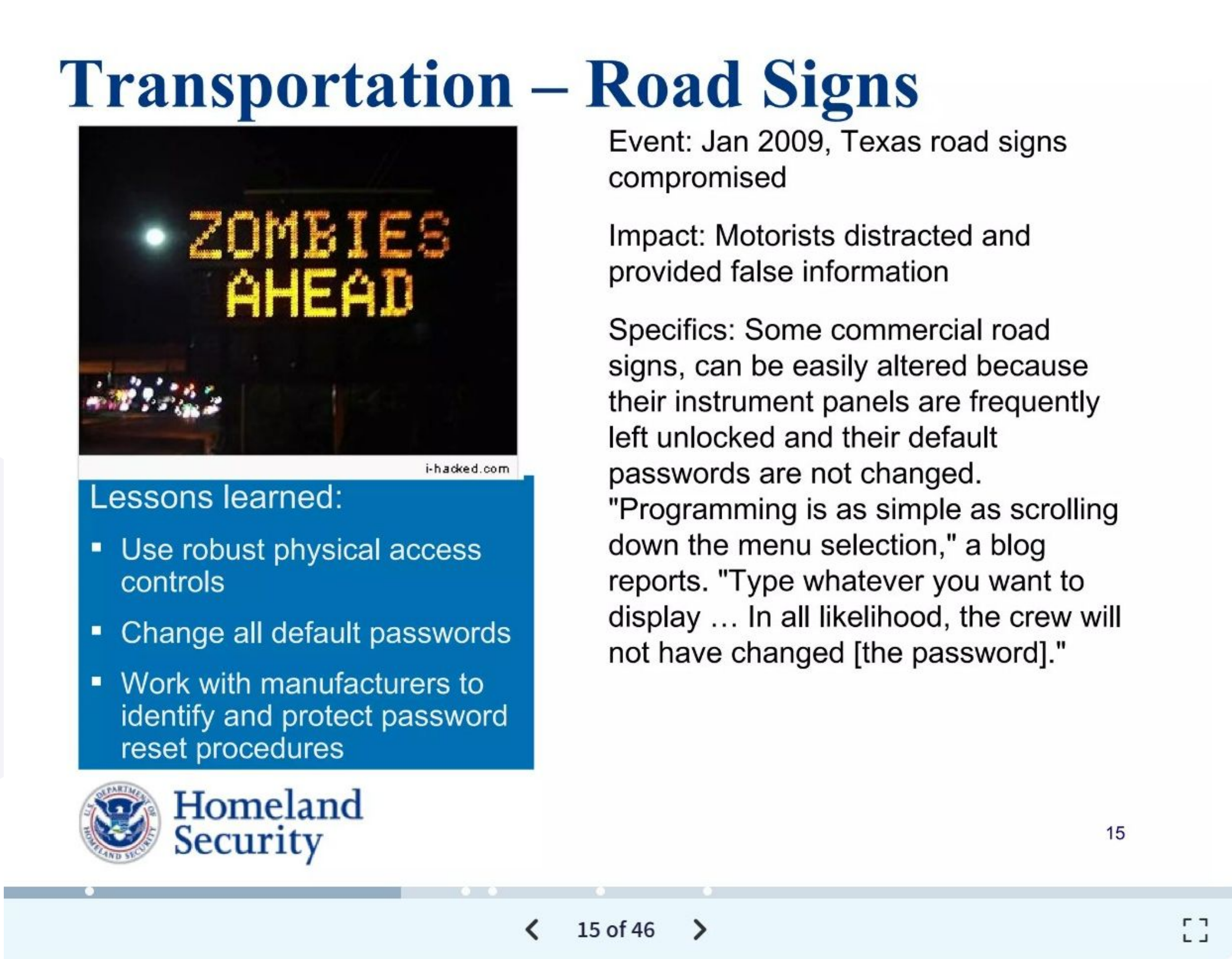
Vulnerabilities

- Connection to internet
- Homebrew crypto
- Physical access
- “Security by obscurity”
- Weak or master passwords
- Constrained resources on MCU



The top 10 most common passwords list:

1. 123456
2. 123456789
3. qwerty
4. password
5. 12345
6. qwerty123
7. 1q2w3e
8. 12345678
9. 111111
10. 1234567890



Transportation – Road Signs

Lessons learned:

- Use robust physical access controls
- Change all default passwords
- Work with manufacturers to identify and protect password reset procedures

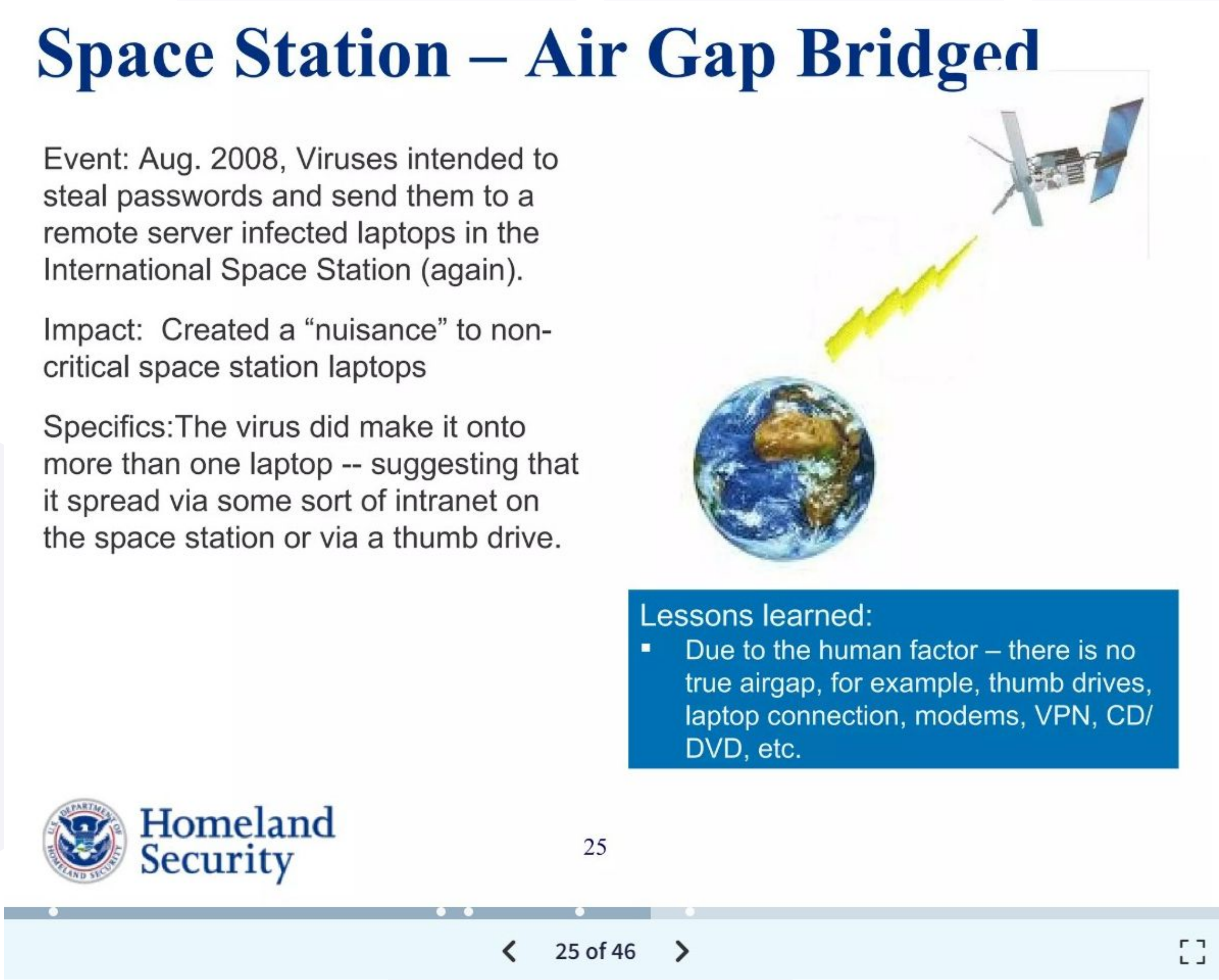
Event: Jan 2009, Texas road signs compromised

Impact: Motorists distracted and provided false information

Specifics: Some commercial road signs, can be easily altered because their instrument panels are frequently left unlocked and their default passwords are not changed. "Programming is as simple as scrolling down the menu selection," a blog reports. "Type whatever you want to display … In all likelihood, the crew will not have changed [the password]."

Homeland Security

15



Space Station – Air Gap Bridged

Event: Aug. 2008, Viruses intended to steal passwords and send them to a remote server infected laptops in the International Space Station (again).

Impact: Created a “nuisance” to non-critical space station laptops

Specifics:The virus did make it onto more than one laptop -- suggesting that it spread via some sort of intranet on the space station or via a thumb drive.

Lessons learned:

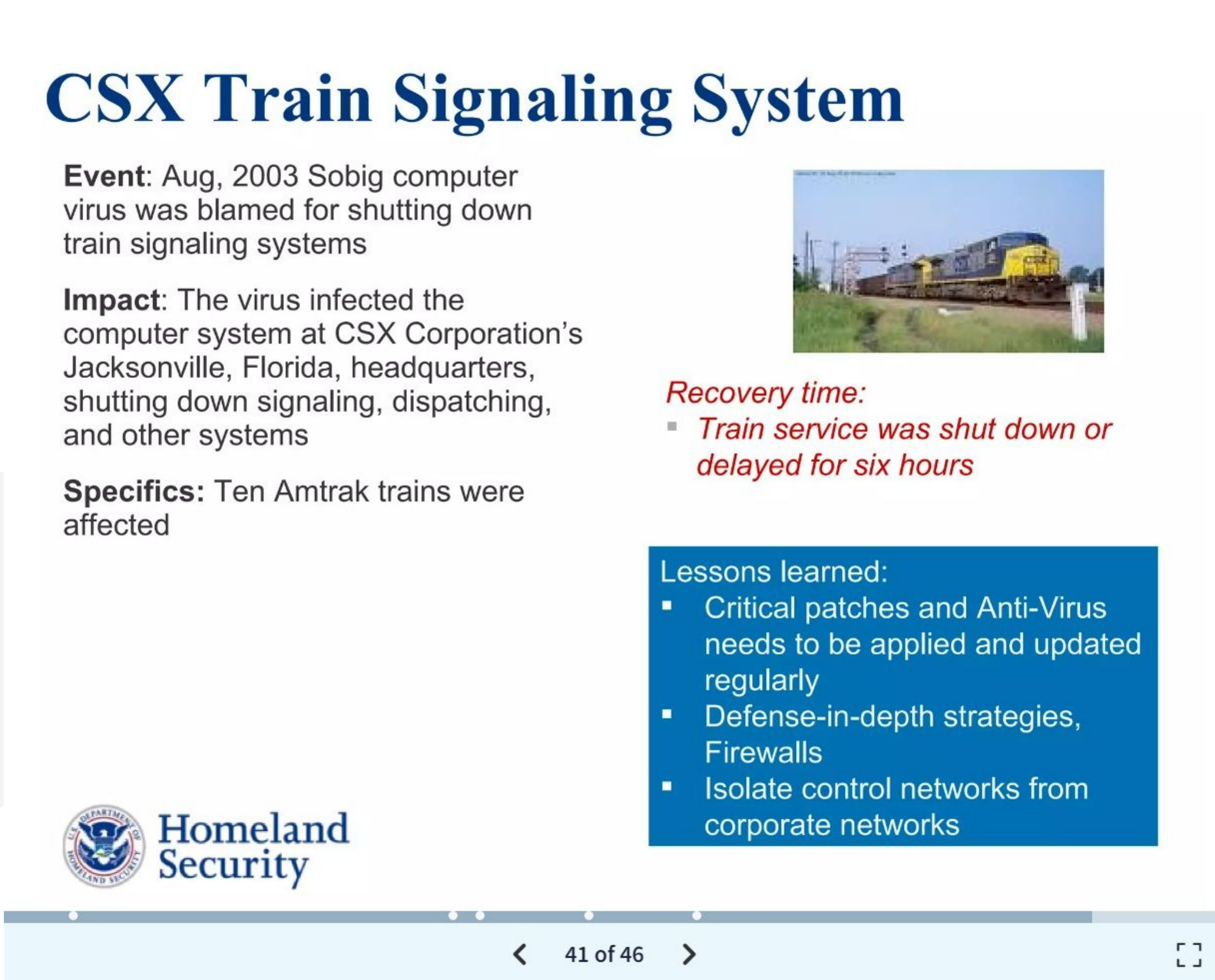
- Due to the human factor – there is no true airgap, for example, thumb drives, laptop connection, modems, VPN, CD/ DVD, etc.

Homeland Security

25

Mitigation/Validation

- Testing is not enough!
- Consult experts, use vetted algorithms
- Principle of least privilege
  - Only give device as much access as it needs (internet connection, access to data, etc)
  - Mitigates effects if device is compromised



CSX Train Signaling System

Event: Aug, 2003 Sobig computer virus was blamed for shutting down train signaling systems

Impact: The virus infected the computer system at CSX Corporation's Jacksonville, Florida, headquarters, shutting down signaling, dispatching, and other systems

Specifics: Ten Amtrak trains were affected

Recovery time:

- *Train service was shut down or delayed for six hours*

Lessons learned:

- Critical patches and Anti-Virus needs to be applied and updated regularly
- Defense-in-depth strategies, Firewalls
- Isolate control networks from corporate networks

Homeland Security