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

26: Security

Security

Safety is about system failing without an attacker model

Security is about system failing because of adversarial actions

Security principles: CIA

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

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)

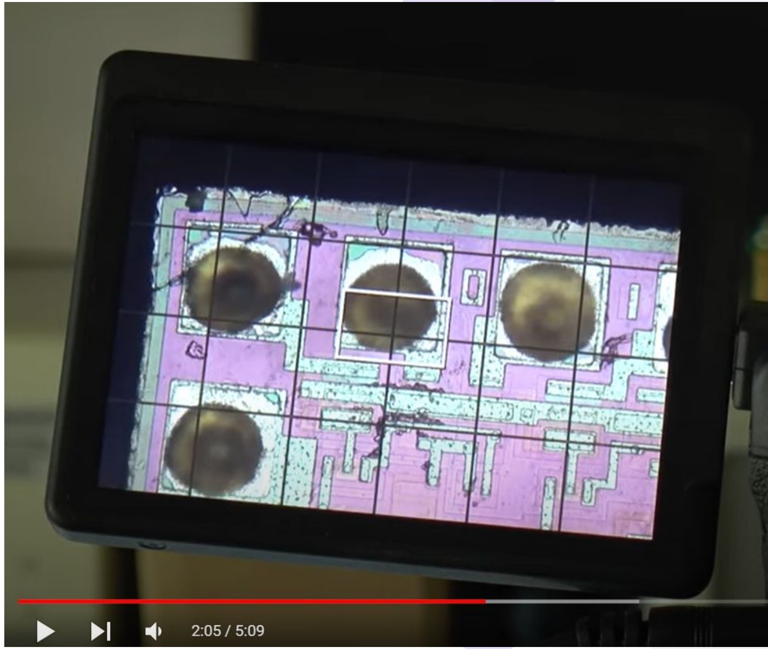
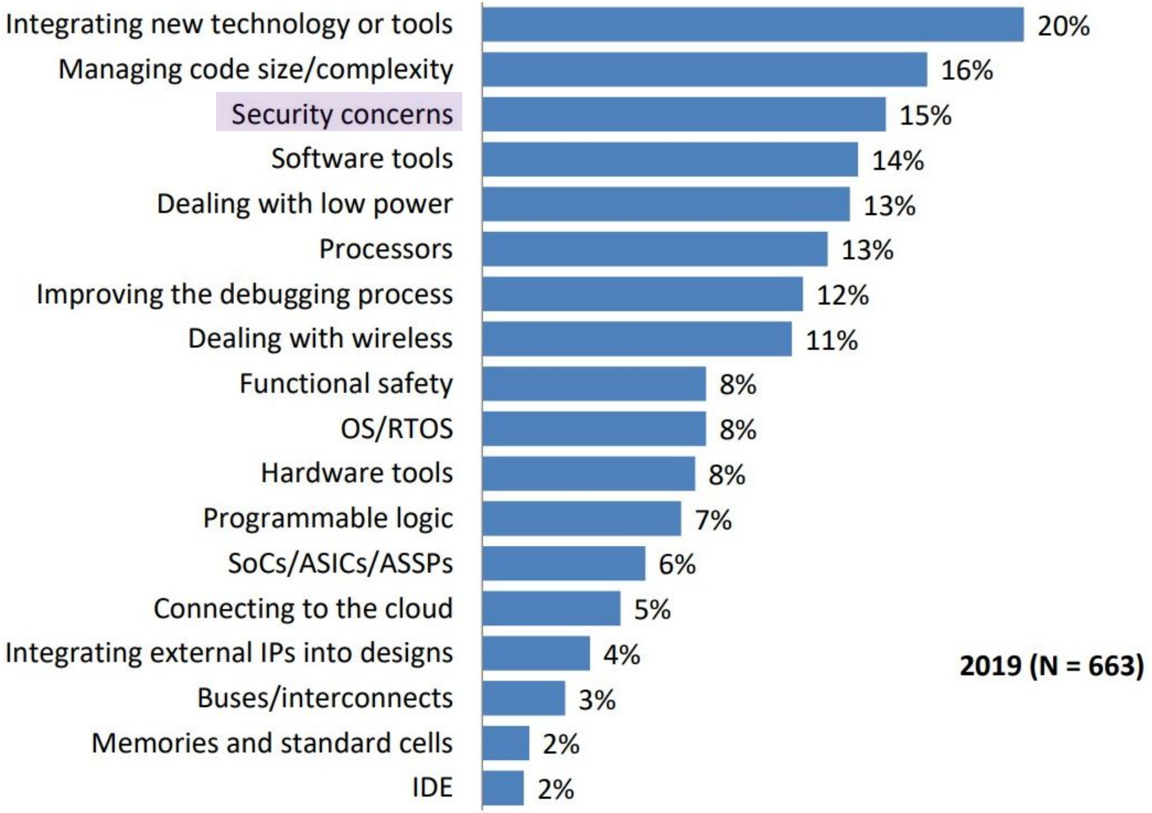
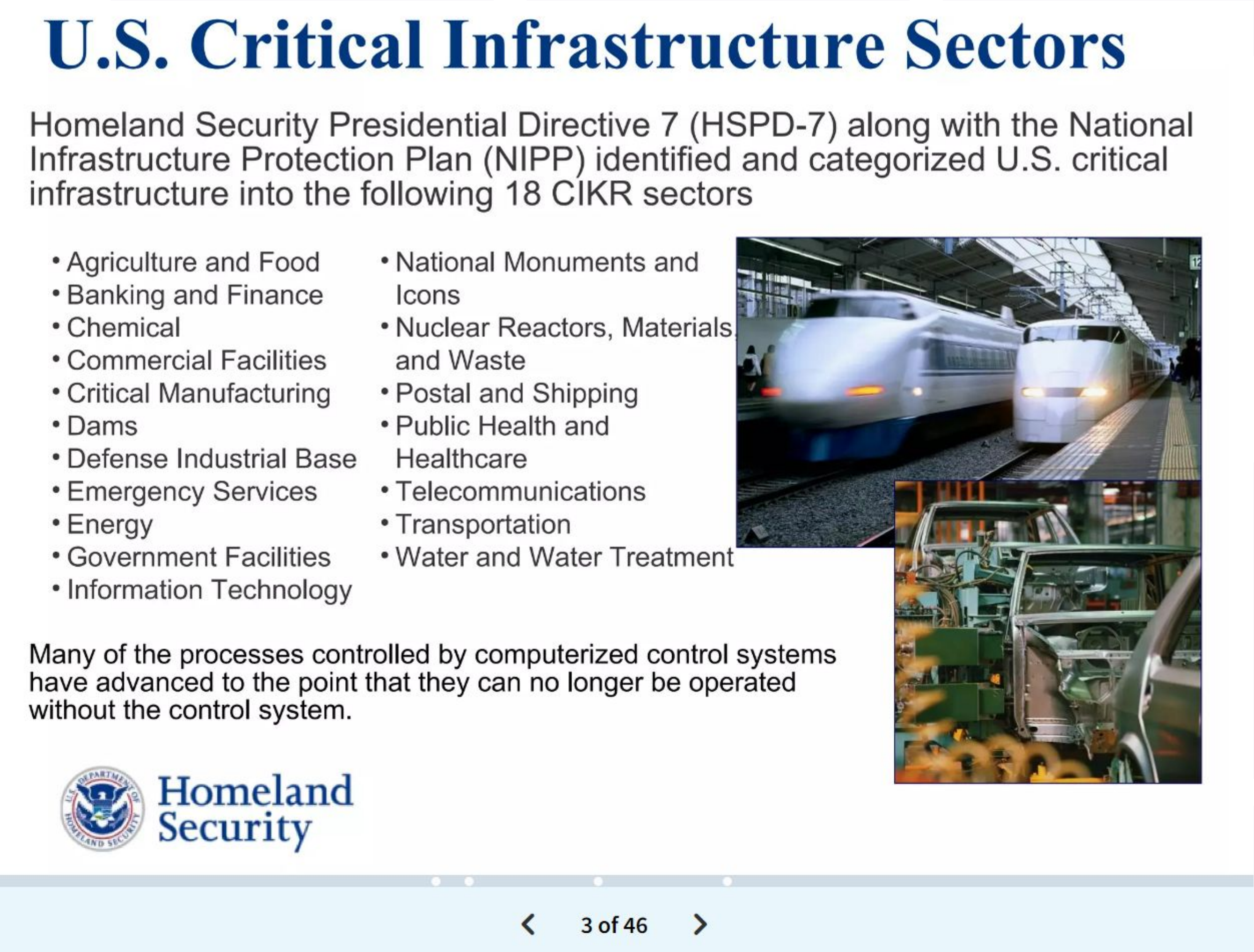


Image source

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



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



U.S. Critical Infrastructure Sectors

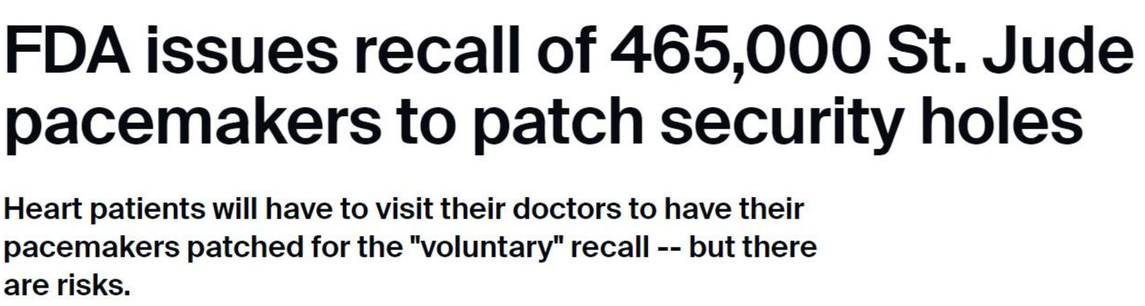
Homeland Security Presidential Directive 7 (HSPD-7) along with the National Infrastructure Protection Plan (NIPP) identified and categorized U.S. critical infrastructure into the following 18 CIKR sectors

- Agriculture and Food
- Banking and Finance
- Chemical
- Commercial Facilities
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Government Facilities
- Information Technology
- National Monuments and Icons
- Nuclear Reactors, Materials, and Waste
- Postal and Shipping
- Public Health and Healthcare
- Telecommunications
- Transportation
- Water and Water Treatment

Many of the processes controlled by computerized control systems have advanced to the point that they can no longer be operated without the control system.

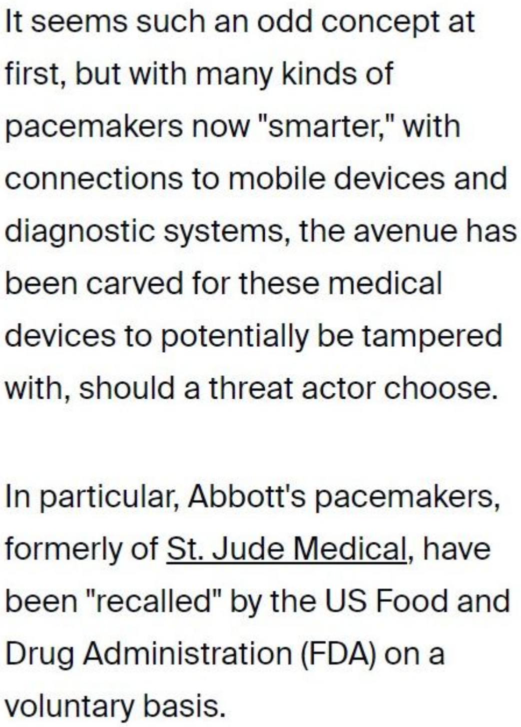
Homeland Security

source



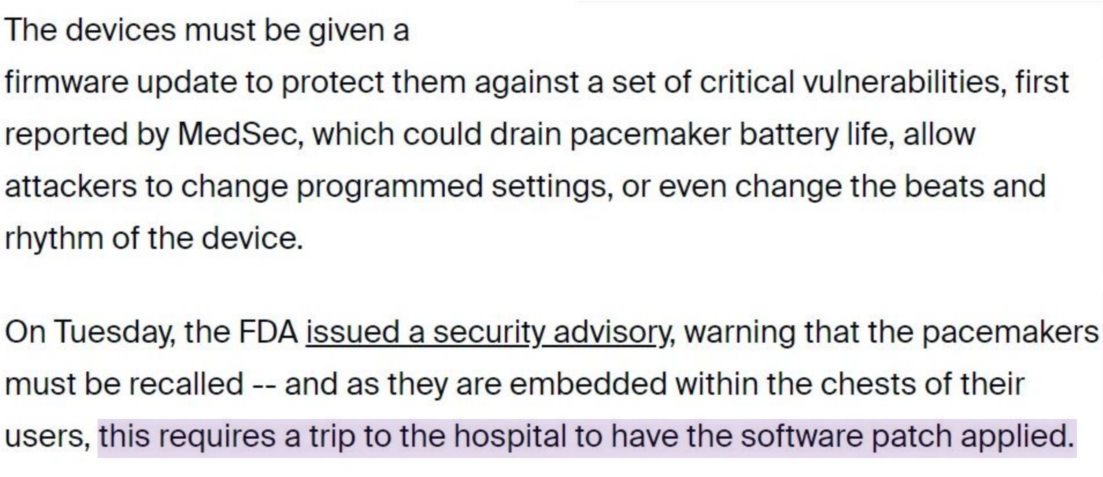
FDA issues recall of 465,000 St. Jude pacemakers to patch security holes

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….

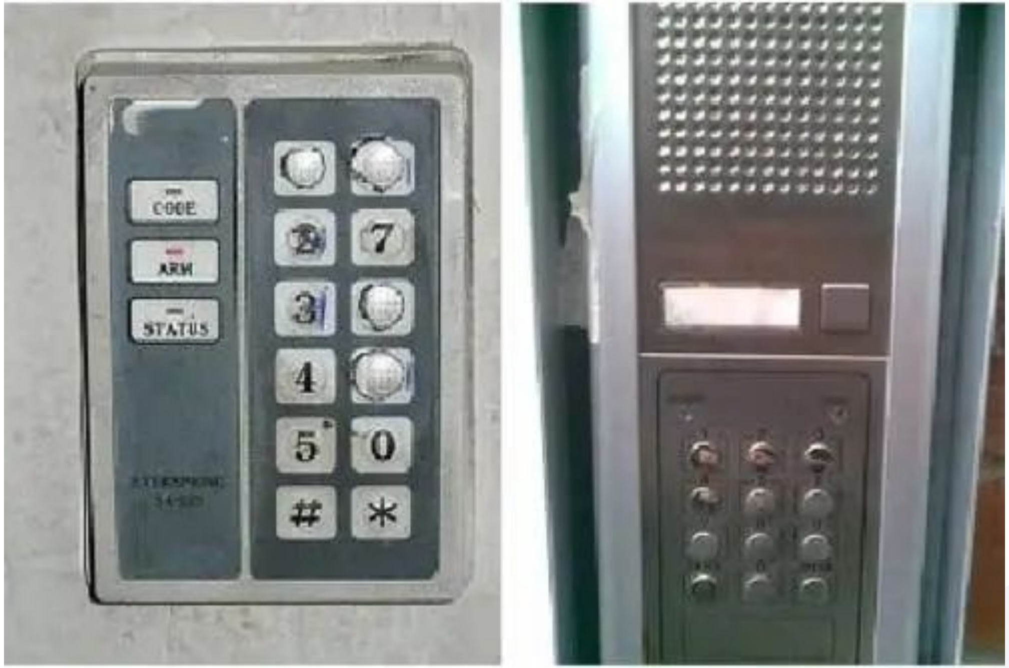
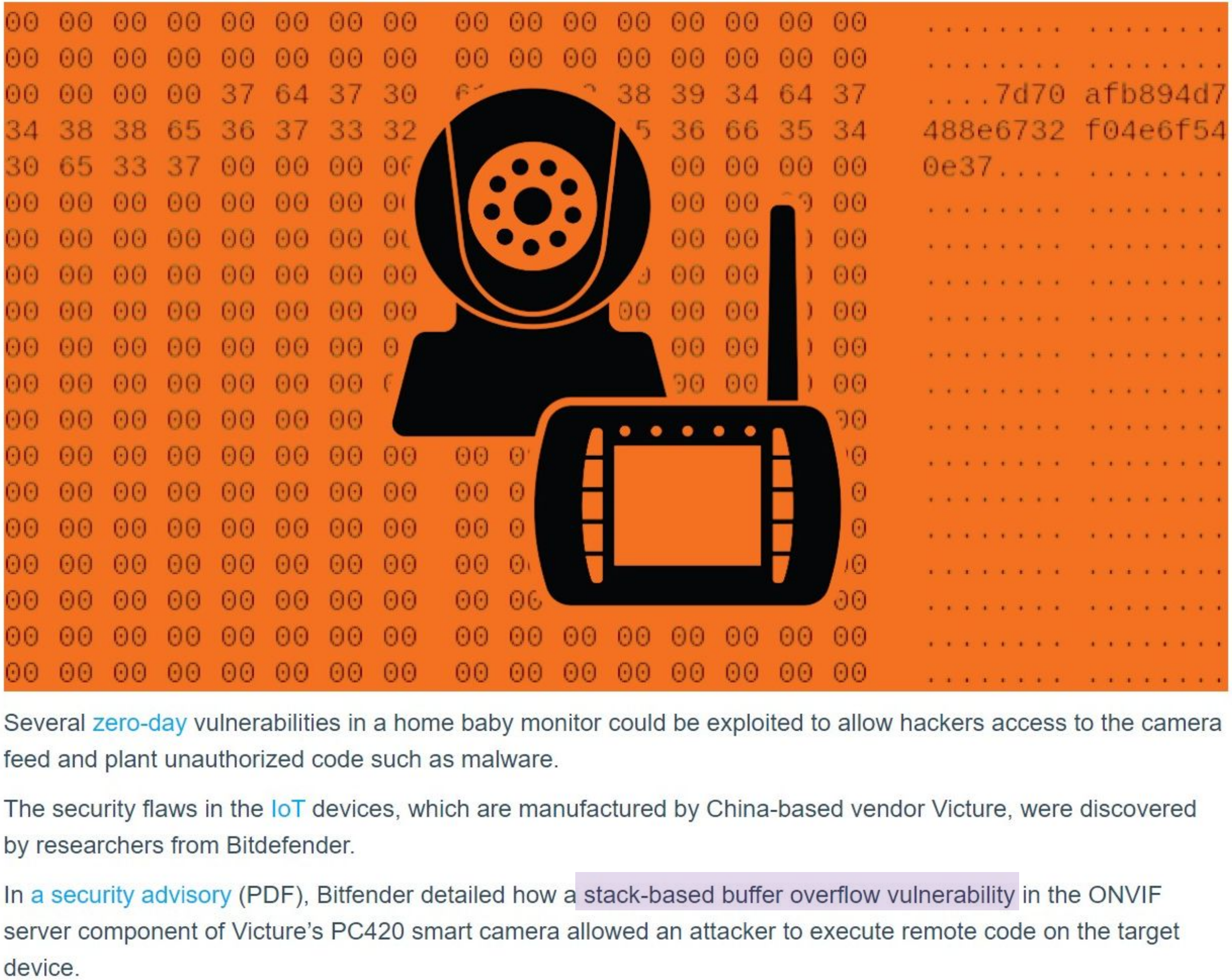


Image source

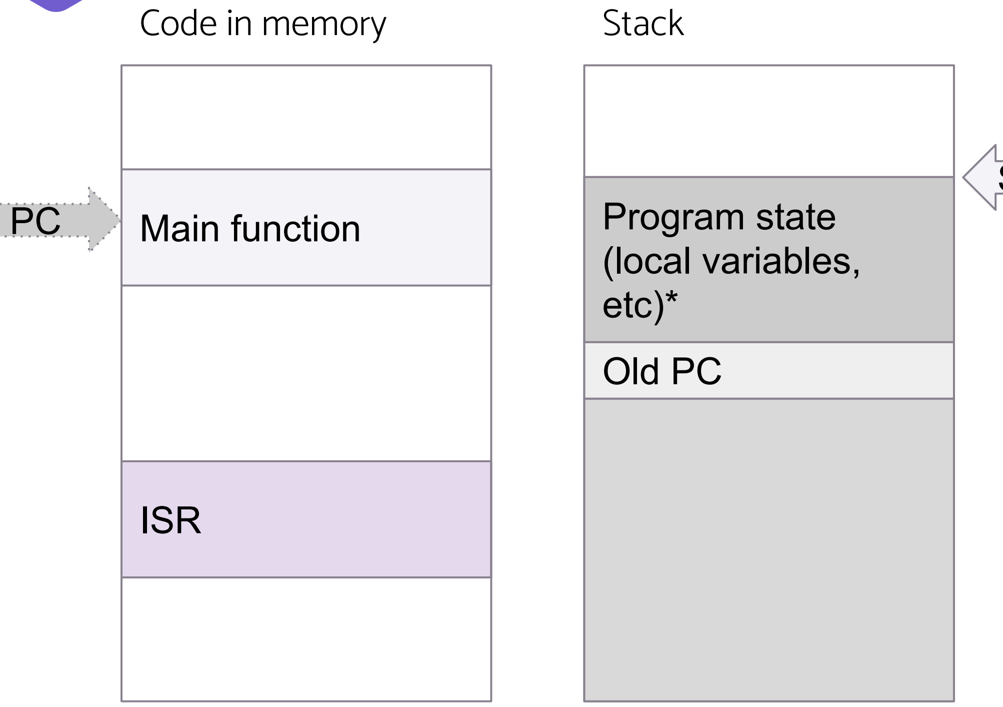


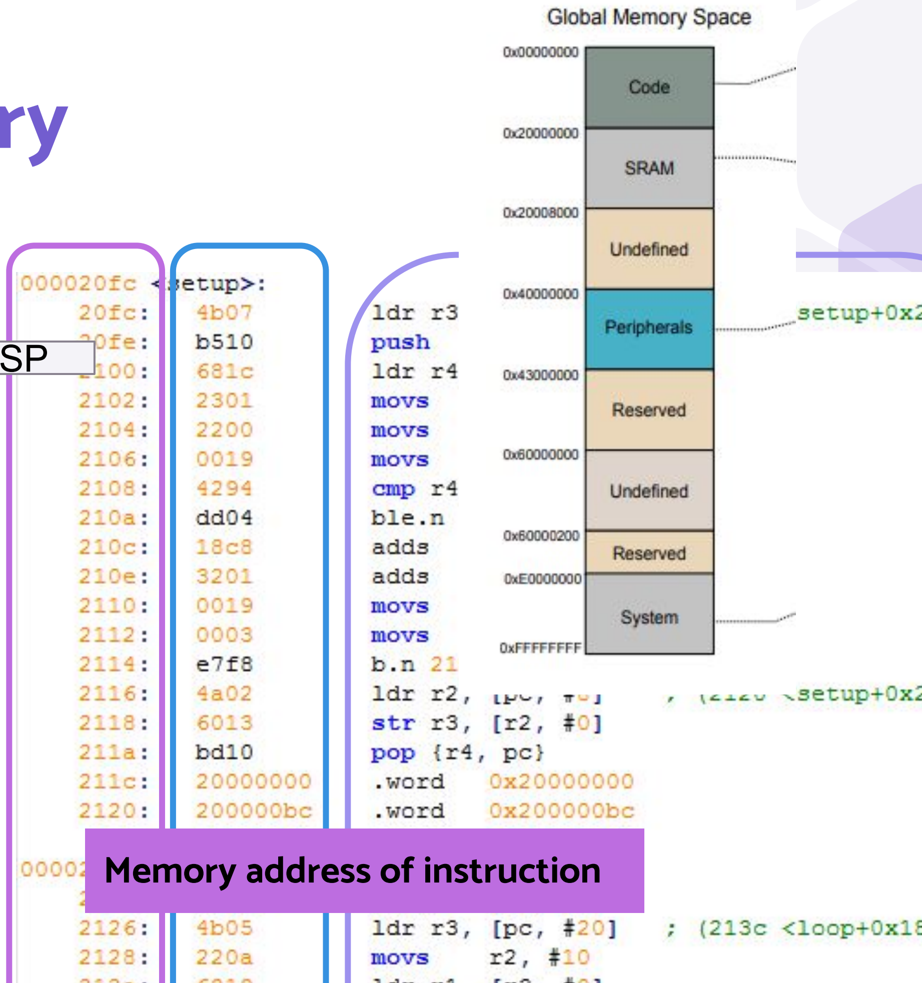
Several zero-day vulnerabilities in a home baby monitor could be exploited to allow hackers access to the camera feed and plant unauthorized code such as malware.

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

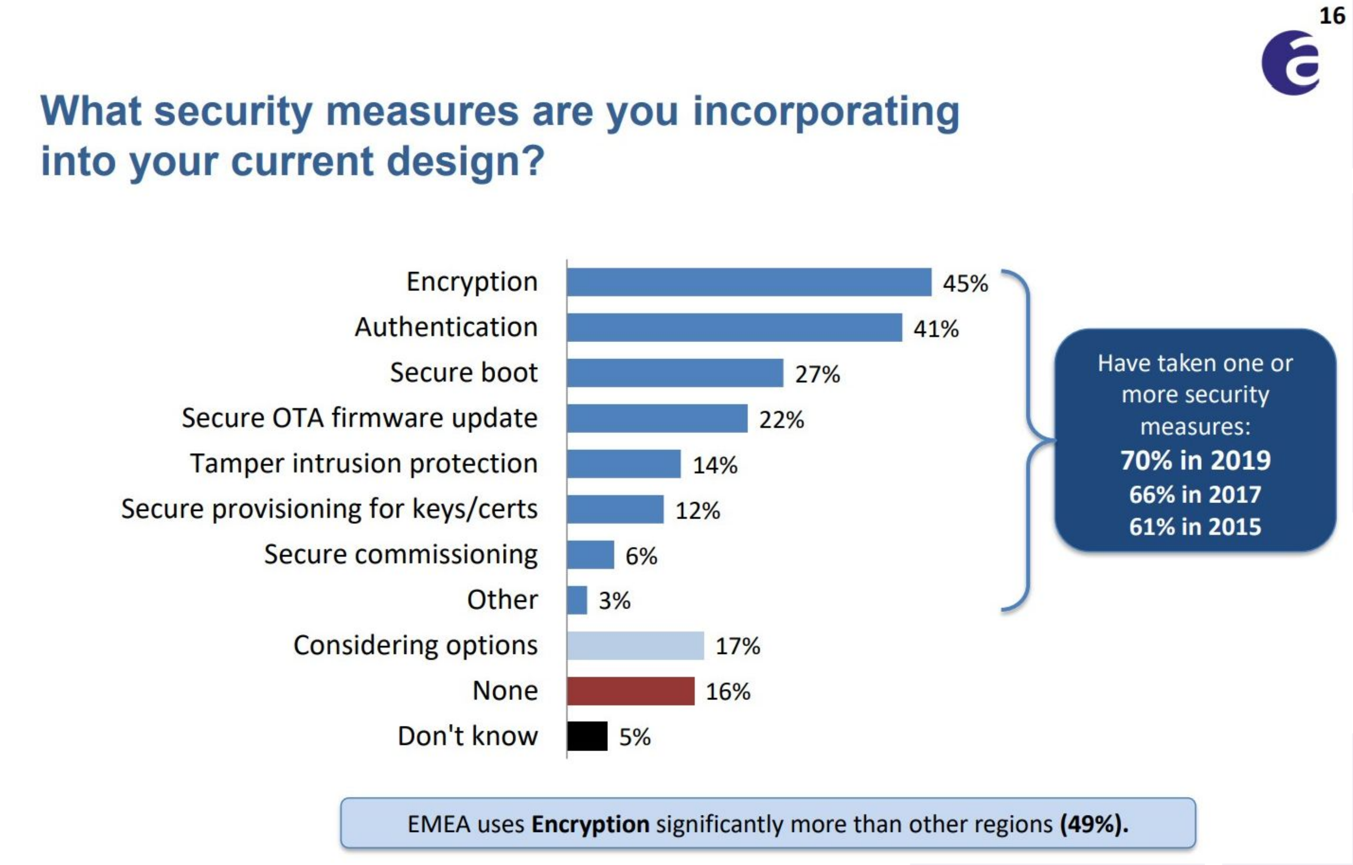




```
000020fc <setup>:
    20fc:   4b07        ldr r3
    20fe:   b510        push
    2100:   681c        ldr r4
    2102:   2301        movs
    2104:   2200        movs
    2106:   0019        movs
    2108:   4294        cmp r4
    210a:   dd04        ble.n
    210c:   18c8        adds
    210e:   3201        adds
    2110:   0019        movs
    2112:   0003        movs
    2114:   e7f8        b.n 21
    2116:   4a02        ldr r2, [pc, #8]        ; (2120 <setup+0x2
    2118:   6013        str r3, [r2, #0]
    211a:   bd10        pop {r4, pc}
    211c:   20000000    .word   0x20000000
    2120:   200000bc    .word   0x200000bc

0002
    2126:   4b05        ldr r3, [pc, #20]       ; (213c <loop+0x18
    2128:   220a        movs    r2, #10
```

Memory address of instruction



16

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%).**

Encryption side-channel attacks

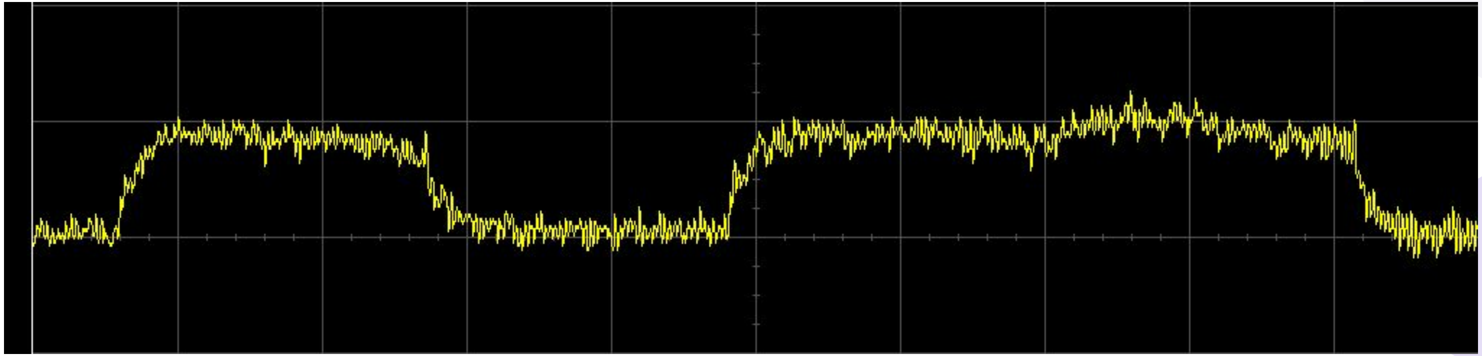
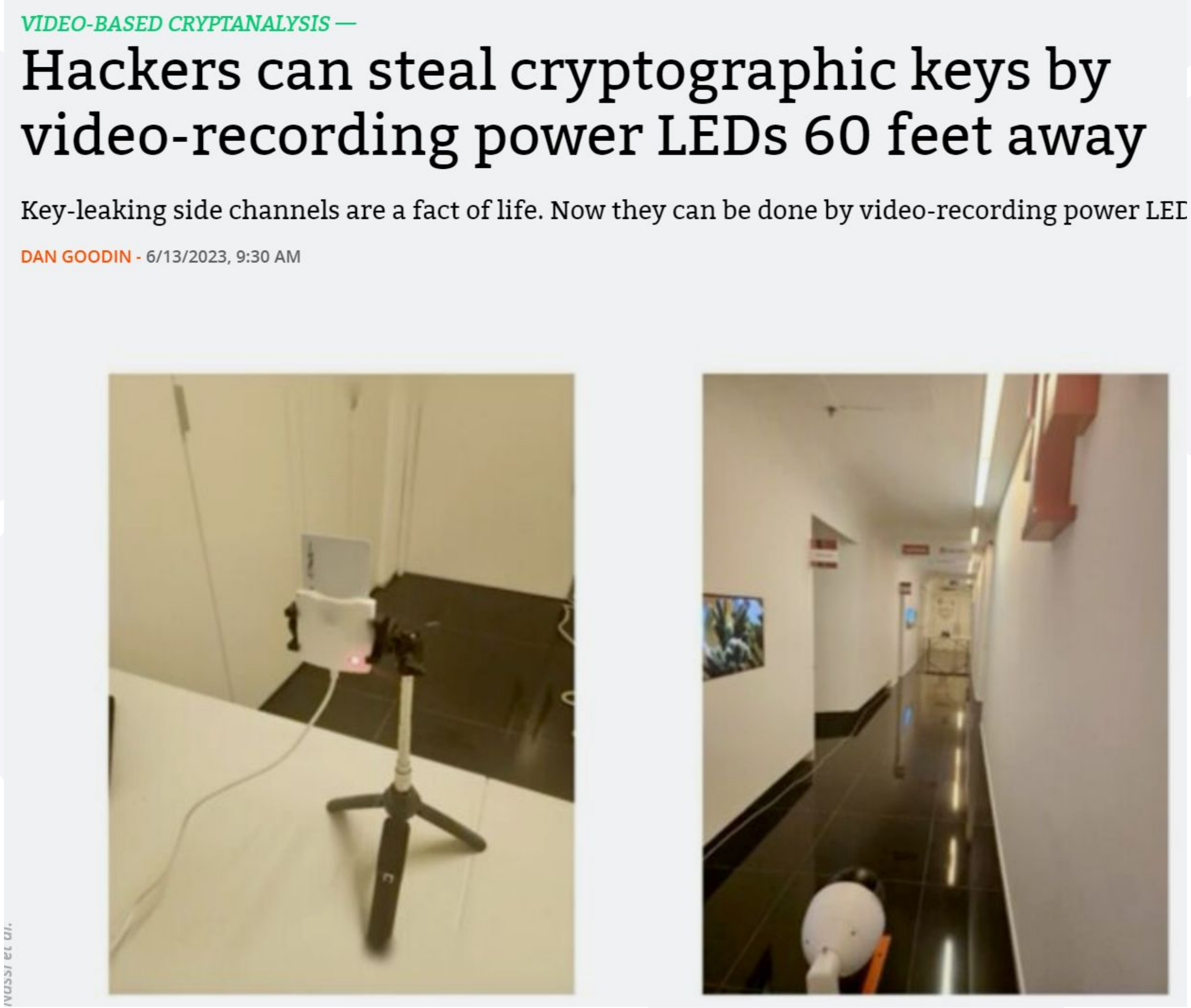


image source



VIDEO-BASED CRYPTANALYSIS —

Hackers can steal cryptographic keys by video-recording power LEDs 60 feet away

Key-leaking side channels are a fact of life. Now they can be done by video-recording power LED

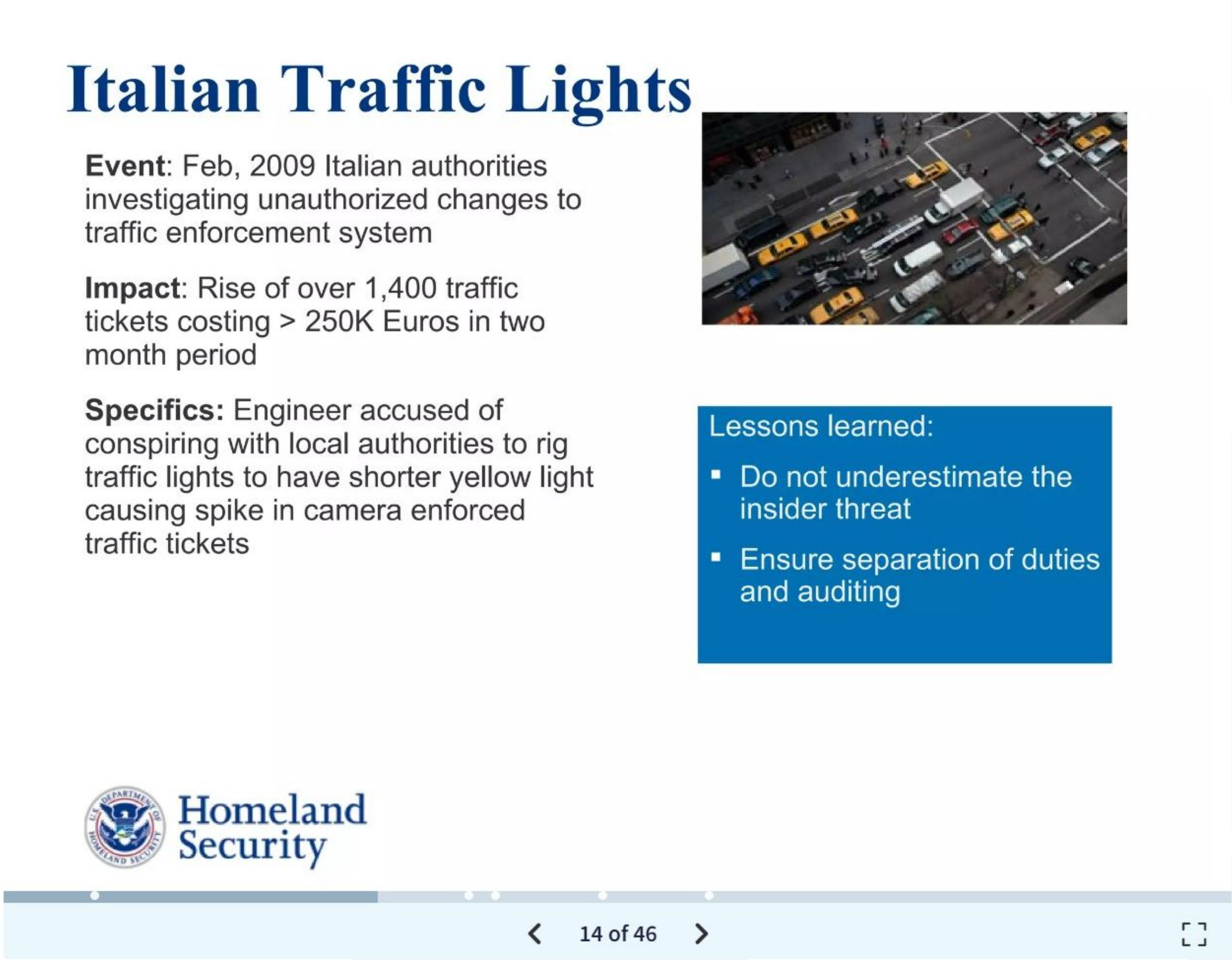
DAN GOODIN - 6/13/2023, 9:30 AM

Nassi et al.

source

Security plans

- Requirements
- Threats
- Vulnerabilities
- Mitigation
- Validation



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

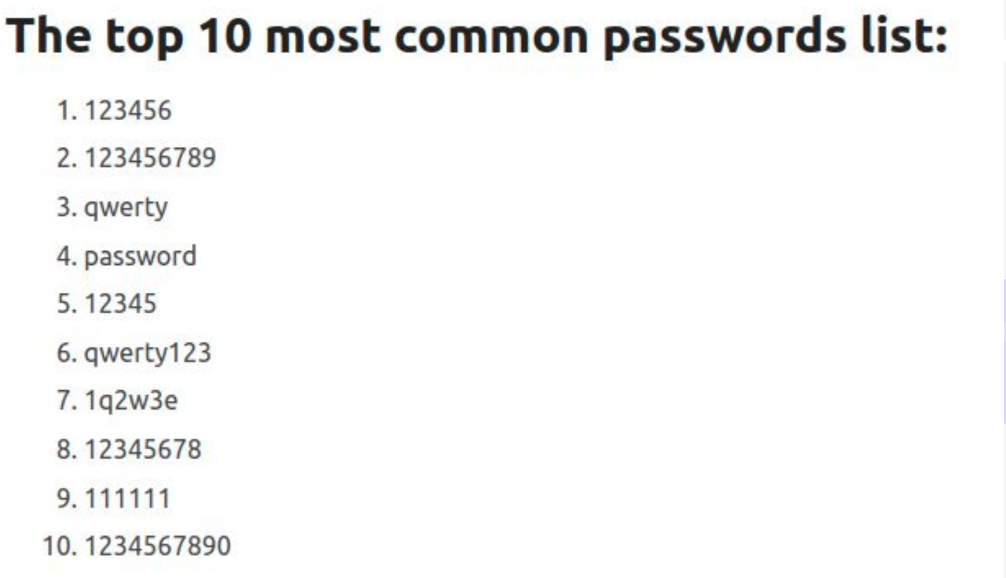
Lessons learned:

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

Homeland Security

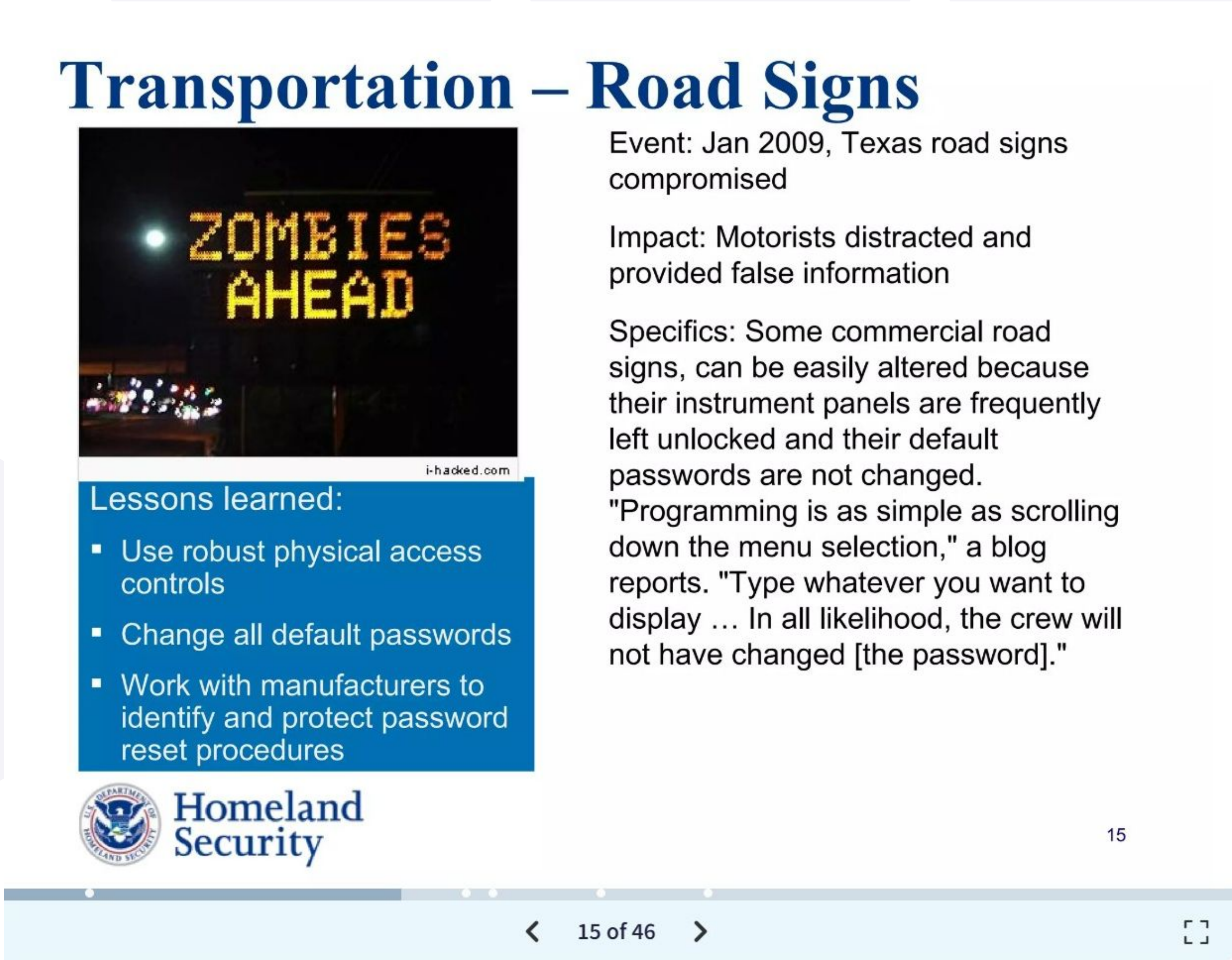
Vulnerabilities

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



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

Event: Jan 2009, Texas road signs compromised

Impact: Motorists distracted and provided false information

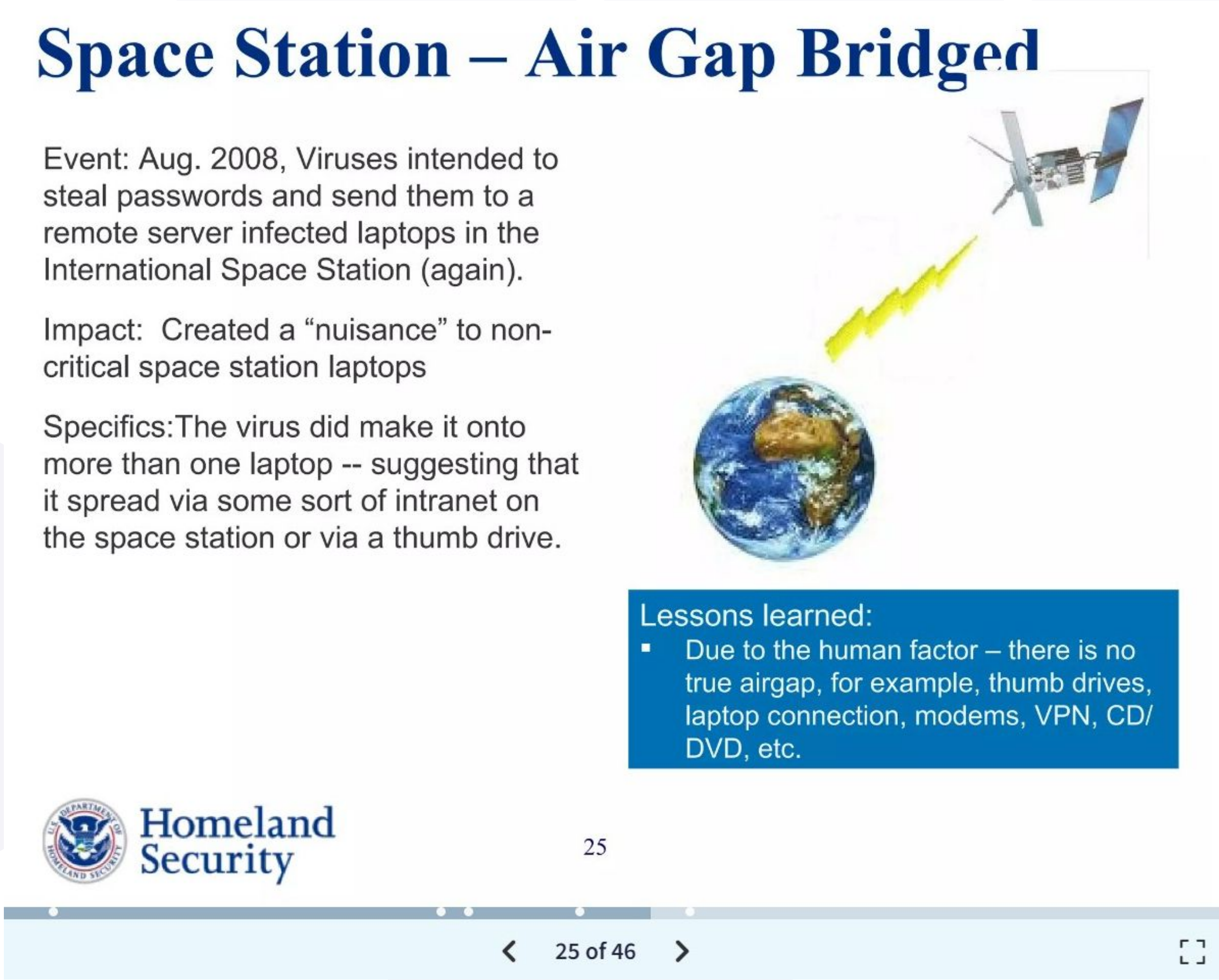
Specifics: Some commercial road signs, can be easily altered because their instrument panels are frequently left unlocked and their default passwords are not changed. "Programming is as simple as scrolling down the menu selection," a blog reports. "Type whatever you want to display … In all likelihood,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

Lessons learned:

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

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.

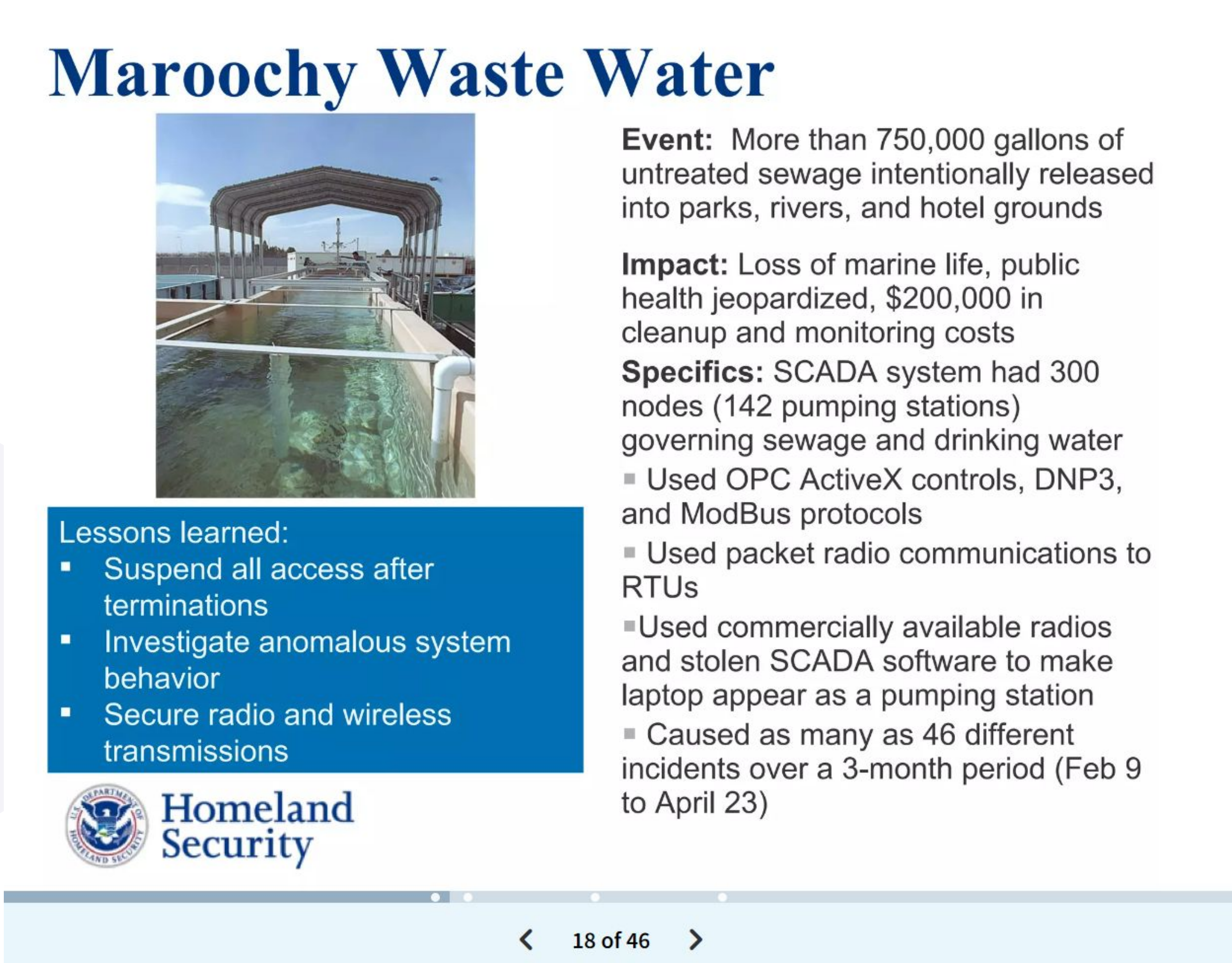
Lessons learned:
- Due to the human factor – there is no true airgap, for example, thumb drives, laptop connection, modems, VPN, CD/ DVD, etc.

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



Maroochy Waste Water

Event: More than 750,000 gallons of untreated sewage intentionally released into parks, rivers, and hotel grounds

Impact: Loss of marine life, public health jeopardized, $200,000 in cleanup and monitoring costs

Specifics: SCADA system had 300 nodes (142 pumping stations) governing sewage and drinking water

- Used OPC ActiveX controls, DNP3, and ModBus protocols
- Used packet radio communications to RTUs
- Used commercially available radios and stolen SCADA software to make laptop appear as a pumping station
- Caused as many as 46 different incidents over a 3-month period (Feb 9 to April 23)

Lessons learned:

- Suspend all access after terminations
- Investigate anomalous system behavior
- Secure radio and wireless transmissions

Homeland Security

18 of 46