TrustED'16
(Workshop of ACM CCS 2016)

Security of CCTV & Video Surveillance Systems: Threats, Vulnerabilities, Attacks, and Mitigations

Andrei Costin
andrei@firmware.re

Agenda

- Problems and Motivation
- Prior Work
- Threats, Attacks, Mitigations
- Contribution Summary
- Conclusion
- Q&A

Problems and Motivation

- Embedded/IoT devices shown to be **massively insecure**/exploitable [CZFB14] [CZF16] [CEWD16] [FZXC16]

Problems and Motivation

- Embedded/IoT devices shown to be **massively insecure**/exploitable [CZFB14] [CZF16] [CEWD16] [FZXC16]

- CCTV/VSS estimated to 245 mil. devices [IHS15]
  - 20% (i.e., ~50 mil.) are IP-based

Problems and Motivation

- Embedded/IoT devices shown to be **massively insecure**/exploitable [CZFB14] [CZF16] [CEWD16] [FZXC16]
- CCTV/VSS estimated to 245 mil. devices [IHS15]
  - 20% (i.e., ~50 mil.) are IP-based
- At least 38% of CCTV/VSS/cameras shown vulnerable to **default credentials** attacks [CSt10], in comparison:
  - Enterprise Devices ~2%, Home Networking ~7%, Power Management ~7%

Problems and Motivation

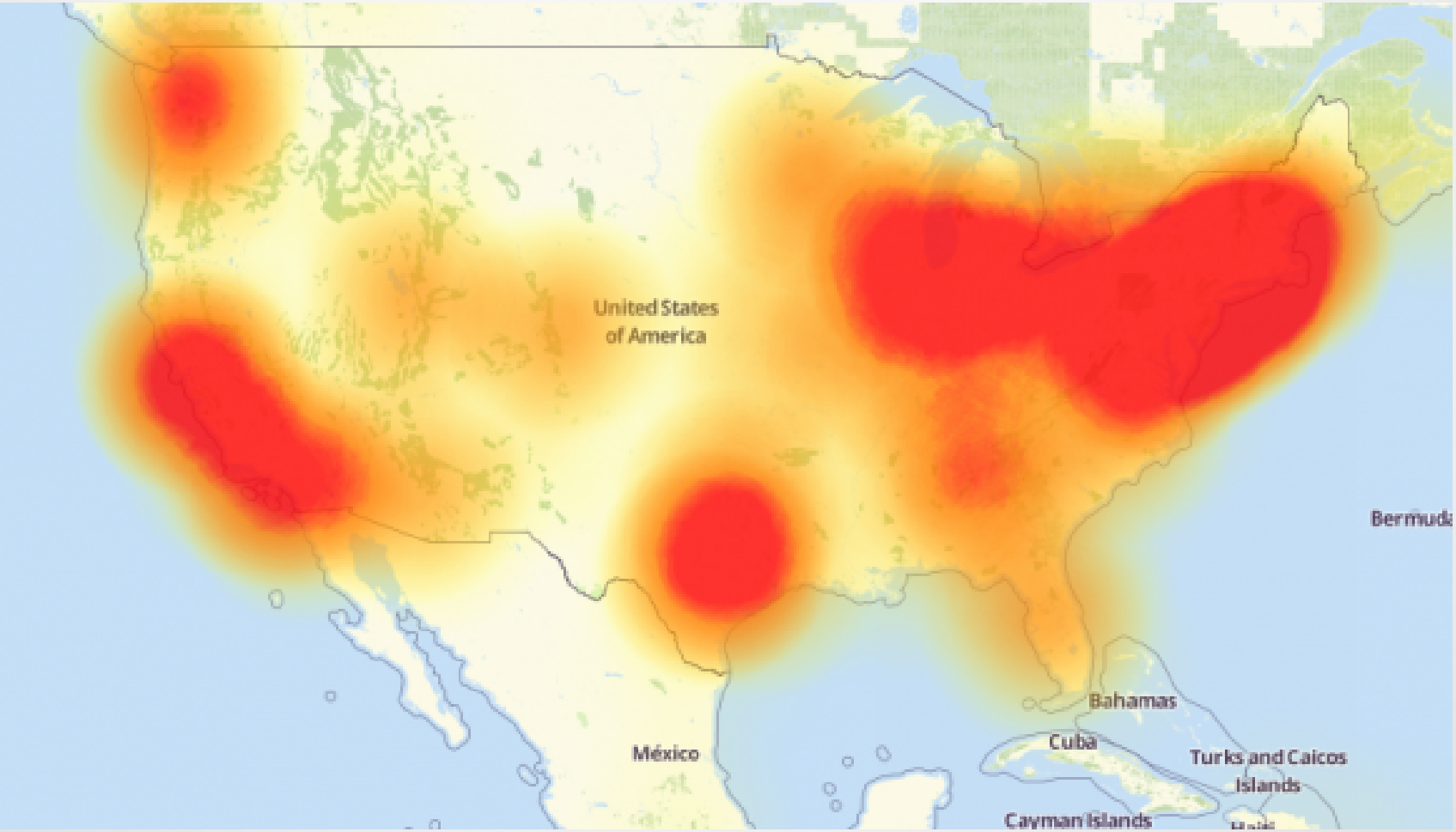
- 21 Sep 2016 and 21 Oct 2016

Problems and Motivation

- **21 Sep 2016** and 21 Oct 2016

Problems and Motivation

- 21 Sep 2016 and **21 Oct 2016**



Source: Downdetector.com

Some Observations

- In 2013, Shodan queries for more than 1 mil. CCTV/VSS online devices [Cos13]
  - https://github.com/zveriu/cctv-ddns-shodan-censys
- http://insecam.org, 2014
  - Streams data from ~100k CCTV/VSS online devices
  - **Privacy invasion** attack via **default credential** vulnerability

Some Observations

- Mirai, 2016: 30k , 100k, 500k, 1500k CCTV/VSS

arstechnica.com/.../inside-the-machine-uprising-how-**cameras-dvrs**-took-down-parts-o...
2 days ago - **Mirai** is hardly the first IoT botnet to make headlines. ... By the time it was over, **more than** 30,000 Internet-connected surveillance **cameras** and ...

Chinese firm admits its hacked DVRs, cameras were behind Friday's ...
www.pcworld.com/.../chinese-firm-admits-its-hacked-products-were-behind-fridays-...
4 days ago - Botnets created from the **Mirai** malware were involved in Friday's cyber ... Security experts have noticed the malware tries a list of **more than** 60 ...

How 1.5 Million Connected Cameras Were Hijacked to Make an ...
motherboard.vice.com/read/15-million-connected-**cameras**-ddos-botnet-brian-krebs
Sep 29, 2016 - How 1.5 Million Connected **Cameras** Were Hijacked to Make an Unprecedented Botnet ... an army made of **more than** one million hacked Internet of Things devices. ... a Chinese manufacturer, with a subsidiary in California, of **cameras** and **DVRs**. ... **Mirai**, the malware allegedly used to build the massive ...

Source Code for DDoS Malware Mirai Released - Bizety
https://www.bizety.com/2016/10/03/source-code-for-ddos-malware-**mirai**-released/
Oct 3, 2016 - Source Code for DDoS Malware **Mirai** released has been confirmed to be the ... **more than** one million web-connected **cameras** and **DVRs**.

The Hacked Camera Botnet: Not New, Just Big | The Security Ledger
https://securityledger.com/2016/09/the-hacked-**camera**-botnet-not-new-just-big/
Sep 30, 2016 - **More than** 100000 infected, Internet connected **cameras** played a part in giant ... made by DAHUA Technology, a U.S. based maker of **cameras** and **DVRs**. ... This time around, the **cameras** are using malware known as **Mirai**, ...

Mirai Bots More Than Double Since Source Code Release - Threatpost
https://threatpost.com/**mirai**-bots-**more-than**-double-since-source-code.../121368/
Oct 19, 2016 - It also estimates that the number of compromised CCTV **cameras**, **DVRs**, home networking equipment overrun by **Mirai** has **more than** doubled ...

Chinese Company Recalls Cameras, DVRs Used In Last Week's ...
https://www.techdirt.com/.../chinese-company-recalls-**cameras-dvrs**-used-last-weeks-m...
3 days ago - At least one **Mirai** [control server] issued an attack command to hit Dyn," ... is little **more than** a small drop in a very deep ocean of dysfunction.

More than 500,000 IoT devices potentially recruitable in the Mirai ...
securityaffairs.co/wordpress/52015/hacking/**mirai**-botnet.html
Oct 8, 2016 - Security experts have discovered **more than** 500000 vulnerable Internet ... number of compromised IoT devices, including **DVRs** and **cameras**.

Some Observations

- More than 80% of devices in Mirai attack were CCTV/VSS

Username/Password	Manufacturer	Link to supporting evidence
admin/123456	ACTi IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/anko	ANKO Products DVR	http://www.cctvforum.com/viewtopic.php?f=3&t=44250
root/pass	Axis IP Camera, et. al	http://www.cleancss.com/router-default/Axis/0543-001
root/vizxv	Dahua Camera	http://www.cam-it.org/index.php?topic=5192.0
root/888888	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/666666	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/7ujMko0vizxv	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
root/7ujMko0admin	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
666666/666666	Dahua IP Camera	http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW4300C
root/dreambox	Dreambox TV receiver	https://www.satellites.co.uk/forums/threads/reset-root-password-plugin.101146/
root/zlxx	EV ZLX Two-way Speaker?	?
root/juantech	Guangzhou Juan Optical	https://news.ycombinator.com/item?id=11114012
root/xc3511	H.264 - Chinese DVR	http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15
root/hi3518	HiSilicon IP Camera	https://acassis.wordpress.com/2014/08/10/i-got-a-new-hi3518-ip-camera-modules/
root/klv123	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/klv1234	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/jvbzd	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/admin	IPX-DDK Network Camera	http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/
root/system	IQinVision Cameras, et. al	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/meinsm	Mobotix Network Camera	http://www.forum.use-ip.co.uk/threads/mobotix-default-password.76/
root/54321	Packet8 VOIP Phone, et. al	http://webcache.googleusercontent.com/search?q=cache:W1phozQZURUJ:community.freepbx.org/t/packet8-atas-phones/411
root/00000000	Panasonic Printer	https://www.experts-exchange.com/questions/26194395/Default-User-Password-for-Panasonic-DP-C405-Web-Interface.html
root/realtek	RealTek Routers	
admin/1111111	Samsung IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/xmhdipc	Shenzhen Anran Security Camera	https://www.amazon.com/MegaPixel-Wireless-Network-Surveillance-Camera/product-reviews/B00EB6FNDI
admin/smcadmin	SMC Routers	http://www.cleancss.com/router-default/SMC/ROUTER
root/ikwb	Toshiba Network Camera	http://faq.surveillixdvrsupport.com/index.php?action=artikel&cat=4&id=8&artlang=en
ubnt/ubnt	Ubiquiti AirOS Router	http://setuprouter.com/router/ubiquiti/airos-airgrid-m5hp/login.htm
supervisor/supervisor	VideoIQ	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/<none>	Vivotek IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/1111	Xerox printers, et. al	https://atyourservice.blogs.xerox.com/2012/08/28/logging-in-as-system-administrator-on-your-xerox-printer/
root/Zte521	ZTE Router	http://www.ironbugs.com/2016/02/hack-and-patch-your-zte-f660-routers.html

Source: KrebsOnSecurity.com

Prior Work

- "Security Requirements for Network CCTV" (Lee and Wan, WAS 2010)
- "User authentication protocol for blocking malicious user in Network CCTV environment" (Park and Sun, ICCIT 2011)
- "Security model for video surveillance system" (Kim and Han, ICTC 2012)

- “Embedded systems security: Threats, vulnerabilities, and attack taxonomy” (Papp et al., PST 2015)

Contribution Summary

- We present a comprehensive survey of generic and specific attacks and mitigations for VSS & CCTV systems

Contribution Summary

- We present a comprehensive survey of generic and specific attacks and mitigations for VSS & CCTV systems

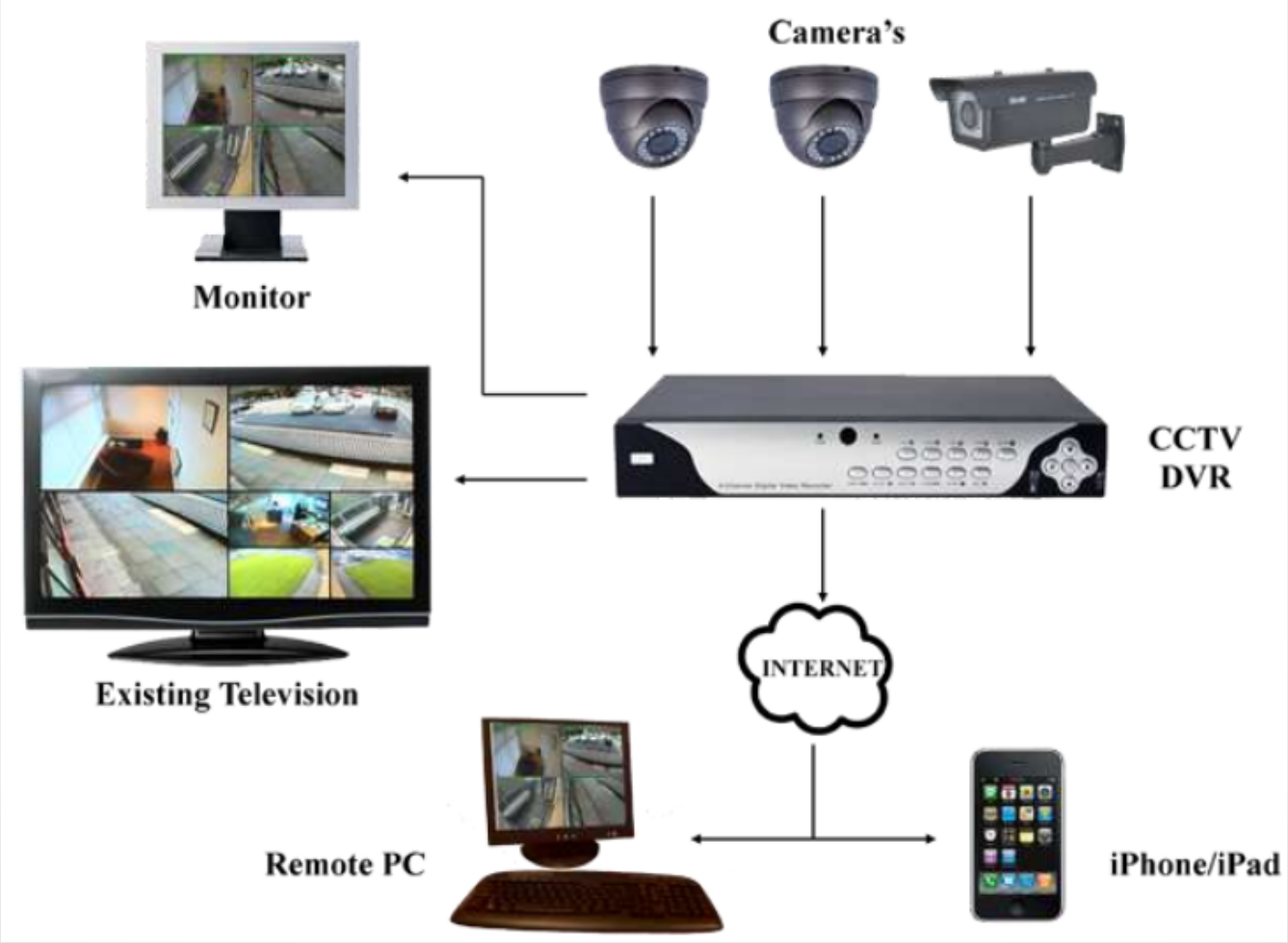
- We discuss in-depth novel and specific attacks on VSS and CCTV systems

Contribution Summary

- We present a comprehensive survey of generic and specific attacks and mitigations for VSS & CCTV systems
- We discuss in-depth novel and specific attacks on VSS and CCTV systems
- We propose one novel covert channel specific to CCTV cameras (namely mechanical movement and position), and propose extensions of several existing covert channels over VSS and CCTV systems

CCTV/VSS Systems

- Simplified schematic of most CCTV/VSS systems



Attack Categories

- Software
- Hardware/Software
- Hardware
- RF/Wireless
- Optical

Attack category: Software

- Attack surfaces
  - Web Interface
  - Other Interfaces (e.g., telnet)
  - Firmware Update Interface

Attack category: Software

- Attack types
  - Weak/broken authentication/authorization
  - Insufficient transport layer protection
  - DoS
  - Command injection
  - XSS
  - CSRF
  - Information leakage/file disclosure
  - Buffer overflow
  - Reverse engineering upgrade
  - Unverified upgrade

Attack category: Hardware/Software

- Attack surfaces
  - USB ports
  - Debug ports
  - Pan-Tilt-Zoom (PTZ)

Attack category: Hardware/Software

- Attack types
  - TOCTTOU
  - Unverified upgrade
  - Bootloader attacks
  - Debug protocols attacks
  - Data exfiltration

Attack category: RF/Wireless

- Attack surfaces
  - “Raw”/modulated RF (GHz range)
  - WiFi 802.11

Attack category: RF/Wireless

- Attack types
  - Eavesdropping
  - Interference/Jamming/DoS

Attack category: Optical

- Attack surfaces
  - PHY Laser
  - PHY Infrared
  - PHY LED
  - Visual Layer (Imagery Semantics)

Attack category: Optical

- Attack types
  - Camera blinding/Dazzling/DoS
  - Data exfiltration
  - Command and control

Generic attacks: Example 1

- Weak/broken authentication or default credentials

Remember that the DVR is, in all likelihood, going to be left on 24 hours a day, 7 days a week. Keep this in mind when choosing a location for installation.

DEFAULT PASSWORD INFORMATION

To ensure your privacy, this DVR supports password protection.

There is no "default" password - until you set a password and enable password protection, the DVR will not ask you for one.

Specific attacks: Example 1

- Data exfiltration via **VisiSploit**

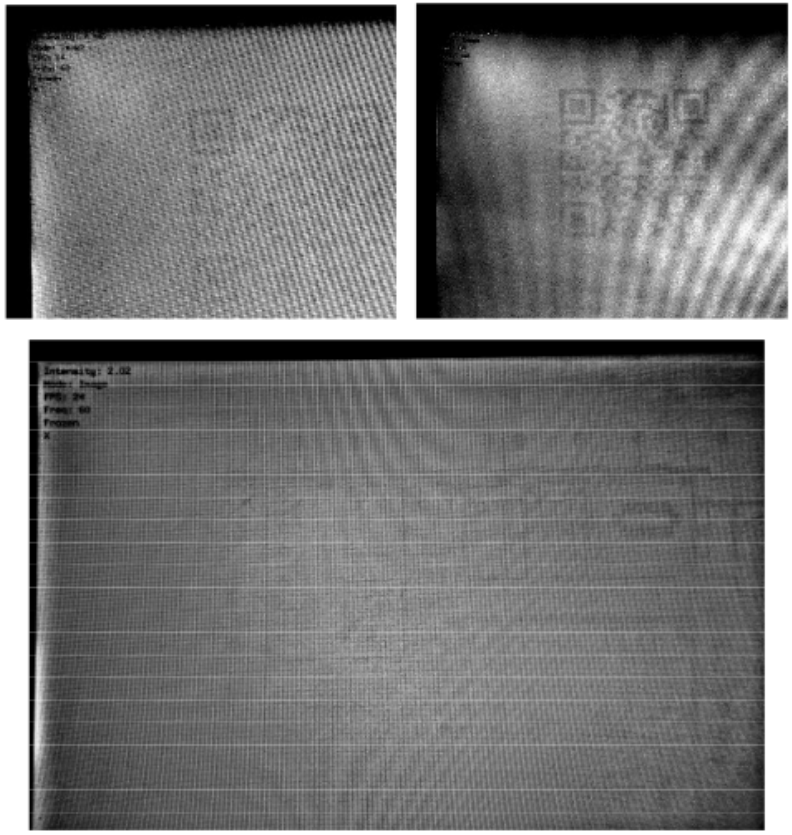


Figure 6. Sample of photos taken during testing, following basic image processing.

Source: Guri et al., arXiv 1607.03946

Specific attacks: Example 1

- Data exfiltration via **VisiSploit extension**

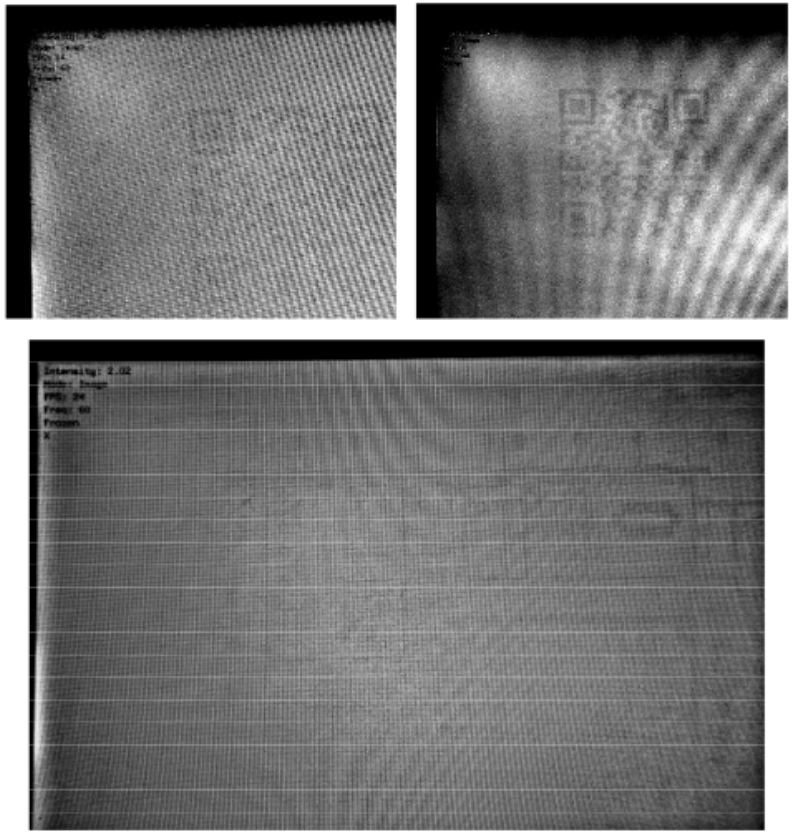


Figure 6. Sample of photos taken during testing, following basic image processing.

Source: Guri et al., arXiv 1607.03946

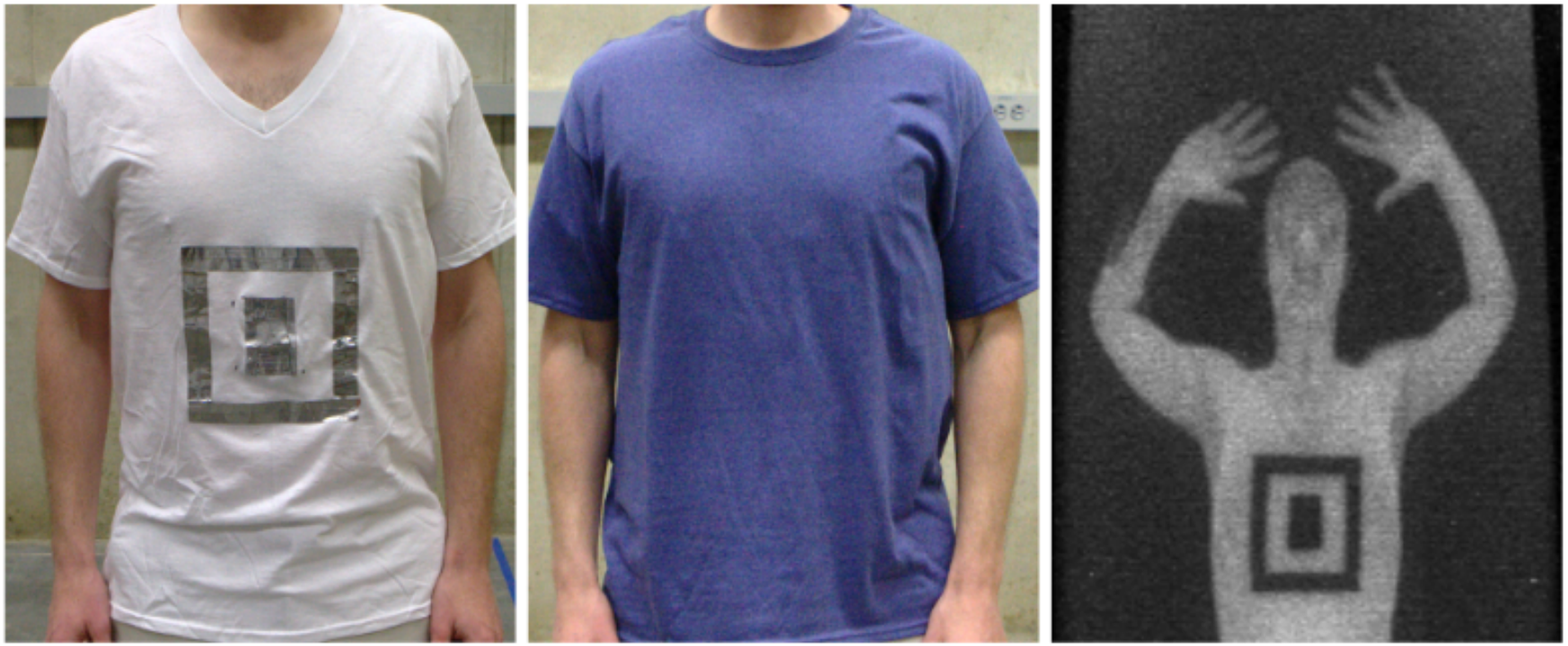
Specific attacks: Example 2

- Command and control via **malicious optical input**

Source: [Cos13]

Specific attacks: Example 2

- Command and control via **malicious optical input**



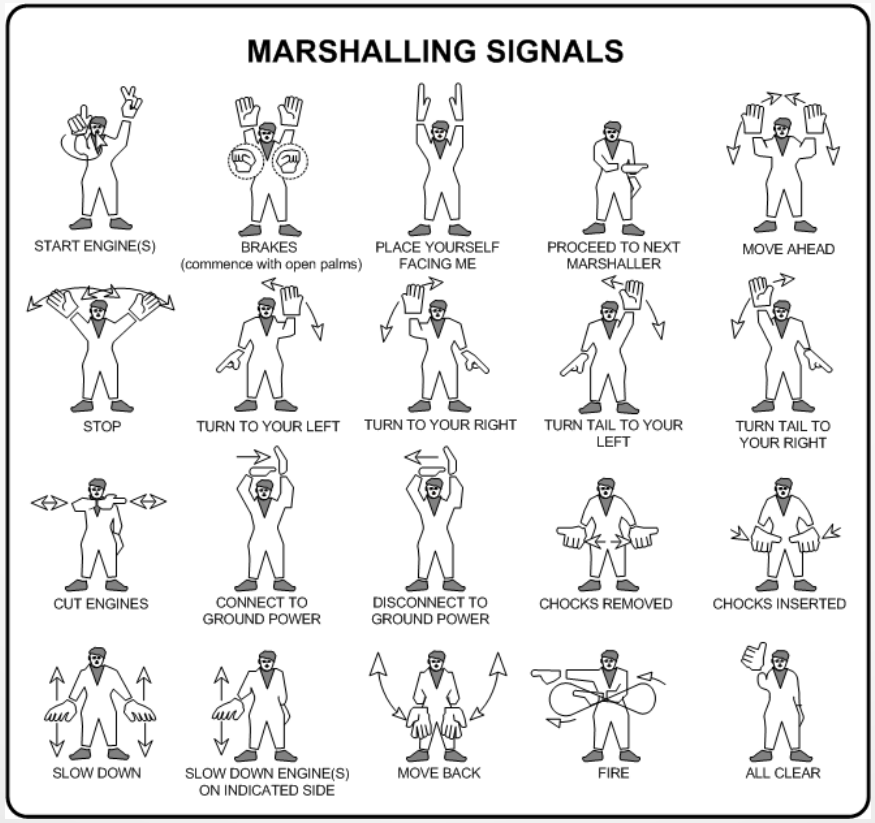
(a) Lead tape pattern (b) Pattern concealed (c) Scan as captured

Figure 7: A Secret Knock — We demonstrate how malware infecting the Secure 1000 user console could be used to defeat the scanner. The malware is triggered when it detects a specific pattern in a scan, as shown here. It then replaces the real image (c) of the attacker, which might reveal hidden contraband, with an innocuous image stored on disk. Pattern recognition occurs in real time.

Source: Mowery et al., USENIX Security 2014

Specific attacks: Example 3

- Data exfiltration via **PTZ mechanics**
  - Similar to *marshalling signals* concept



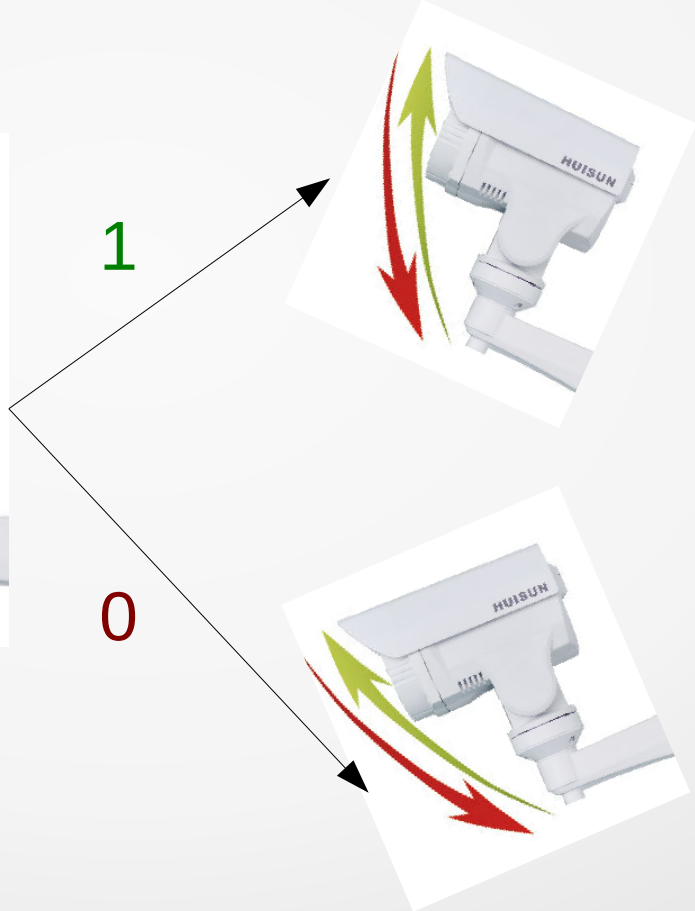
Source: Langley Flying School

Specific attacks: Example 3

- Data exfiltration via **PTZ mechanics**

Camera position in normal operation

Camera position data exfiltration attack



Specific attacks: Example 3

- Data exfiltration via **PTZ mechanics**
  - More cameras = more exfiltration bandwidth

1 0 0 1

Summary: Threats, Attacks, Mitigations

Attack category	Attack surface	Attack type	Attacker type	Directly affected components	Exploitation complexity	Mitigation complexity	Additional comments on mitigation (if applicable)
Software	Web Interface Other Interfaces	Weak access control or weak authentication	Network-Remote Network-Local	- Firmware of DVR, NVR, IP-camera - Software of VMS, CMS, video server	Easy	Easy 91	- Do not use/disable default passwords - Remove hard-coded passwords/accounts - Implement and enforce strong password update policies
Software	Web Interface Other Interfaces	Insufficient Transport Layer Protection 91	Network-Remote Network-Local	- Firmware of DVR, NVR, IP-camera - Software of VMS, CMS, video server	Easy	Easy 91	- Disable clear-text and non-mutually authenticated protocols - Enable and use only HTTPS-like secured protocols - Enable mutually-authenticated protocols
Software	Web Interface Other Interfaces	Denial-of-Service (DoS)	Network-Remote Network-Local	- Firmware of DVR, NVR, IP-camera - Software of VMS, CMS, video server	Easy 71	Complex (it is far easier to build a secure system than to build a correct (and robust) system 90)	- Limit resource allocation - Cache content - Reinforce error handlers - Check buffer overflows - Validate inputs
Software	Web Interface	XSS 91	Network-Remote Network-Local	- Firmware of DVR, NVR, IP-camera - Software of VMS, CMS, video server	Easy 33, 29, 32	Easy to Complex 91	- Properly escape all untrusted data - Positive or "white list" input validation - Use auto-sanitization libraries
Software	Web Interface	CSRF 91	Network-Remote Network-Local	- Firmware of DVR, NVR, IP-camera - Software of VMS, CMS, video server	Easy 33, 29, 32	Easy to Complex 91	- Use unpredictable tokens in each HTTP request - Generate and include the unique token in a hidden field - Reauthenticate and re-CAPTCHA users
Software	Web Interface	Path traversal 90	Network-Remote Network-Local	- Firmware of DVR, NVR, IP-camera - Software of VMS, CMS, video server	Easy 8, 6	Easy 90	- Validate and escape the inputs - Use chrooted jails and code access policies - Normalize the input
Software	Web Interface	Information leakage via file disclosure 89	Network-Remote Network-Local	- Firmware of DVR, NVR, IP-camera - Software of VMS, CMS, video server	Easy 5	Easy 89	- Reinforce error handlers - Validate inputs - Check request authorization - Disable verbose logging
Software	Web Interface	Command injection 88	Network-Remote Network-Local	- Firmware of DVR, NVR, IP-camera - Software of VMS, CMS, video server	Easy 25	Easy to Medium 88	- Validate and normalize inputs - Use APIs instead of raw system calls - Implement a positive or "whitelist" security model
Software	Web Interface	Buffer overflow 87	Network-Remote Network-Local	- Firmware of DVR, NVR, IP-camera - Software of VMS, CMS, video server	Easy 25	Easy to Complex 87	- Validate inputs - Use safe APIs instead of outdated unsafe versions - Use static and dynamic checking tools for discovery - Use compiler-based canary mechanisms
Software	Firmware Update	Reverse engineering	Network-Remote Network-Local Physical-Local	- Bootloader, kernel, firmware of DVR, NVR, IP-camera - Software of VMS, CMS, video server	Easy to Complex	Easy to Complex	- Firmware encryption using crypto standards and PKI
Software	Firmware Update	Unsigned/Unverified upgrade 42	Network-Remote Network-Local Physical-Local	- Bootloader, kernel, firmware of DVR, NVR, IP-camera - Software of VMS, CMS, video server	Easy to Complex	Easy to Complex 42	- Firmware signing and verification using PKI, secure hashing
Software/Hardware	Mechanical Pan-Tilt-Zoom (PTZ)	Data exfiltration	Network-Remote Network-Local Physical-Local	- Cameras with PTZ support - Data "within reach" of camera	Complex	Easy to Medium	
Hardware	Debug Port	- Debug protocols attacks - Bootloader attacks - Unsigned/unverified upgrade 42	Physical-Local	- Bootloader, kernel, firmware of DVR, NVR, IP-camera	Easy to Complex 25	Complex	- Implement "secure scan" techniques 60 - Securely sign and verify bootloaders and firmware images
Hardware	USB Port	- TOCTTOU 81, 111 - Unsigned/unverified upgrade 42	Physical-Local	- Bootloader, kernel, firmware of DVR, NVR, IP-camera - Software of VMS, CMS, video server	Easy	Medium to Complex 108, 98	- Copy the software or firmware files to internal storage and then execute the checks on the copy
Optical	Visual Layer Malicious Images (Imagery Semantics)	- Command and control - Data infiltration	Physical-Local Line of sight	- Cameras - Video sensors - NVR/DVR - Video/Image processing elements	Easy to Complex 39, 80	Easy to Complex 105, 45, 112, 36	
Optical	Visual Layer VisiSploit (Imagery Semantics)	Data exfiltration	Physical-Local Line of sight	- VSS, Cameras, DVR, NVR connected to LCD displays visible to attacker	Complex 53	Complex 53	
Optical	Visual Layer Steganography (Imagery Semantics, Metadata)	Data exfiltration	Network-Remote Network-Local Physical-Local	- VSS, Cameras, DVR, NVR providing image and video feeds	Easy to Medium 97, 79	Easy to Complex 31, 49	
Optical	- PHY LED (output) - PHY Infrared (output)	- Data exfiltration - Command and control	Physical-Local Line of sight	- Cameras with normal and/or IR LEDs - Data "within reach" of camera	Easy to Medium 73, 37, 102, 34	Medium to Complex	
Optical	PHY Infrared	- Command and control - Denial-of-Service (DoS)	Physical-Local Line of sight	- NVR/DVR with IR remote control - Cameras with IR remote control	Easy to Complex 76	Medium to Complex	
Optical	PHY Infrared	Camera blinding (dazzling)	Physical-Local Line of sight	- Cameras - Video sensors	Easy to Medium 18, 44	Easy to Medium 107	- Use infrared filters (in turn, that affects night-vision features)
Optical	PHY Laser	Camera blinding (dazzling)	Physical-Local Line of sight	- Cameras - Video sensors	Medium to Complex 18, 44	Complex 107, 99, 110	- Use wave-length agile filters - Spatial light modulator and wavelength multiplexing
RF/Wireless	Radio Frequency (RF)	Denial-of-Service (DoS) RF Jamming	Physical-Local Line of sight Physical-Remote	- Communication links	Easy	Medium to Complex	- Spread spectrum solutions as - DSSS 84, FHSS 84, UDSSS 95, RD-DSSS 72
RF/Wireless	Radio Frequency (RF)	Eavesdropping	Physical-Local Line of sight Physical-Remote	- Communication links - Private data	Easy 21	Medium to Complex	- Spread spectrum solutions as - DSSS 84, FHSS 84, UDSSS 95, RD-DSSS 72
RF/Wireless	Wi-Fi 802.11	Denial-of-Service (DoS) RF Jamming	Physical-Local Line of sight Physical-Remote	- Communication links	Easy 30	Medium to Complex 30	
RF/Wireless	Wi-Fi 802.11	Eavesdropping	Physical-Local Line of sight Physical-Remote	- Communication links - Private data	Easy	Easy	- Do not use default or simple credentials - Use strong protocols (e.g., WPA2)

Conclusions

- Embedded/IoT devices represent the new powerhorse for large-scale or sophisticated attacks

Conclusions

- Embedded/IoT devices represent the new powerhorse for large-scale or sophisticated attacks
- CCTV and VSS systems are particularly exposed due to their number, ease of installation and intended functionality
  - *Largest Internet DDoS attack to date was run mainly from CCTV and VSS systems*

Conclusions

- Embedded/IoT devices represent the new powerhorse for large-scale or sophisticated attacks
- CCTV and VSS systems are particularly exposed due to their number, ease of installation and intended functionality
  - *Largest Internet DDoS attack to date was run mainly from CCTV and VSS systems*
- CCTV and VSS systems open avenues for *specific attacks*

Conclusions

- Embedded/IoT devices represent the new powerhorse for large-scale or sophisticated attacks
- CCTV and VSS systems are particularly exposed due to their number, ease of installation and intended functionality
  - *Largest Internet DDoS attack to date was run mainly from CCTV and VSS systems*
- CCTV and VSS systems open avenues for *specific attacks*
- A systematic and practical approach should be taken to securing CCTV and VSS systems
  - *Our paper can serve as a starting guideline and checklist*

Acknowledgements

- Prof. Aurélien Francillon
  - For guidance and comments during early versions of this paper

- Enno Rey and ERNW GmbH
  - For generous support that made it possible to present this paper and its results at TrustED’16

References

- [CZFB14] "A Large Scale Analysis of the Security of Embedded Firmwares" (Costin et al., USENIX Security 2014)
- [CZF16] "Automated Dynamic Firmware Analysis at Scale: A Case Study on Embedded Web Interfaces" (Costin et al., ASIACCS 2016)
- [CEWD16] "Towards Automated Dynamic Analysis for Linux-based Embedded Firmware" (Chen et al., NDSS 2016)
- [FZXC16] "Scalable Graph-based Bug Search for Firmware Images" (Feng et al., CCS 2016)
- [CSt10] "A quantitative analysis of the insecurity of embedded network devices: results of a wide-area scan" (Cui and Stolfo, ACSAC 2010)
- [Cos13] "Poor Man's Panopticon: Mass CCTV Surveillance for the masses" (Costin, PowerOfCommunity 2013)
- [IHS15] IHS Video Surveillance Camera Installed Base Report – 2015

Thank you!