Multi-dimensional Security Integrity Analysis of Broad Market Internet-connected Cameras

Mark Stanislav

Dissertation Committee

- Dr. Josh Pauli (Chair)
- Dr. Wayne E. Pauli
- Dr. Deb Tech
- Dr. Andrea Matwyshyn
- Kevin Nassery

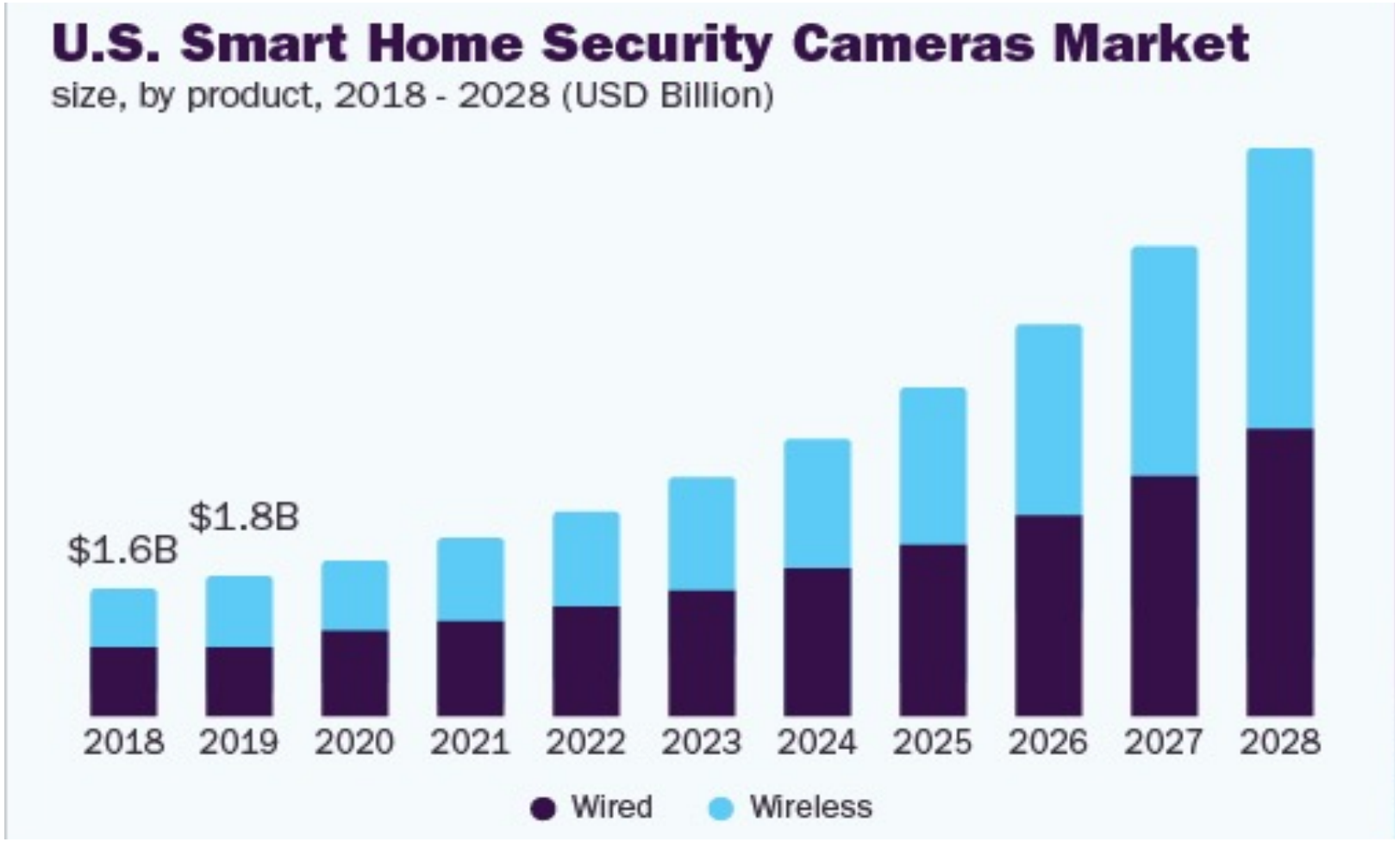
Presentation Outline

- Introduction
- Research Methodology
- Results
- Conclusion
- Audience Questions

Introduction

U.S. IoT Camera Market

(Grand View Research, 2021)



The **global** market is expected to reach $10.4B by 2026 (KBV Research, 2020).

Complex Attack Surface

Interfaces	Software	Networking
UART	Firmware/OS	Bluetooth
JTAG	Web Servers	Ethernet
I2C	Remote Login	Wi-Fi
RS-232	Mobile Applications	Zigbee
SPI	Cloud Services	Z-Wave
USB	Reverse Proxies	Cellular
GPIO	API/SDK	NFC

A Long History of Internet-connected Cameras

AXIS
2100 (2002)

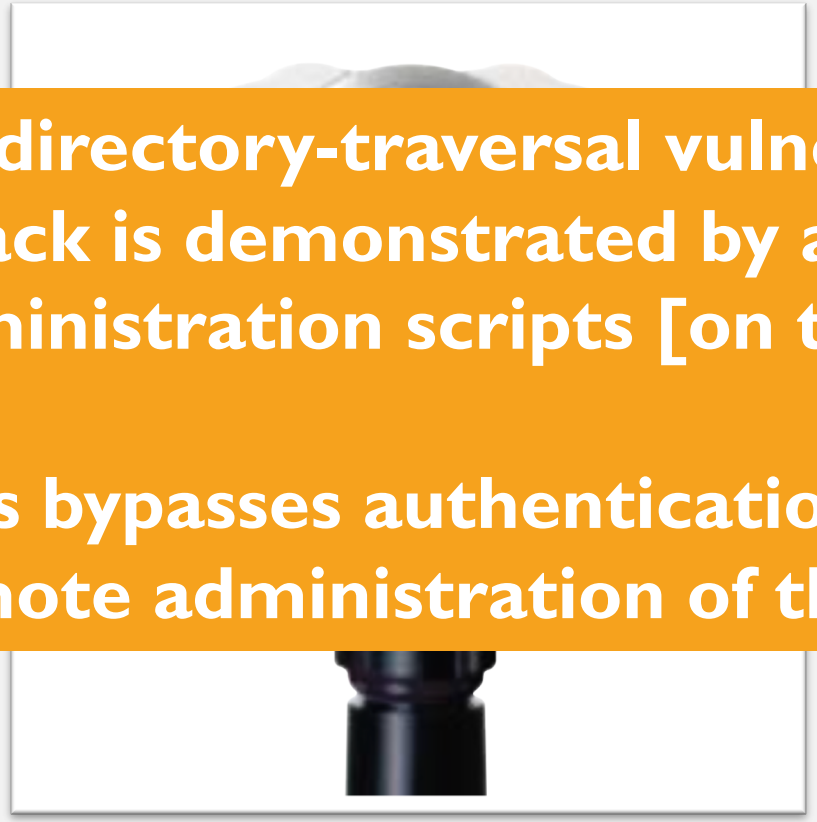
Networking: Ethernet
Firmware: Linux

D-Link
DCS-1000W (2002)

Networking: Ethernet, Wi-Fi
Firmware: Custom

A Long History of Internet-connected Cameras

AXIS
2100 (2002)



Networking: Ethernet
Firmware: Linux

D-Link
DCS-1000W (2002)

Networking: Ethernet, Wi-Fi
Firmware: Custom

"A directory-traversal vulnerability in HTTP POST requests. This attack is demonstrated by an anonymous user calling protected administration scripts [on the AXIS 2100].

This bypasses authentication checks and gives anonymous users remote administration of the devices" (Bashis, 2004).

An Increasingly Pervasive Issue

camhacker.com
40,000+ cameras
(Dvorak, 2006)

Shape Security/Qualys
40,000+ baby monitors
(Hill, 2013)

insecam.com
73,000+ cameras
(Biggs, 2014)

Bitdefender
130,000+ cameras
(Franceschi-Bicchierai, 2017)

That's getting worse...

Aug 13, 2013, 06:35pm EDT

How A Creep Hacked A Baby Monitor To Say Lewd Things To A 2-Year-Old

Kashmir Hill Former Staff

Tech

Welcome to The Not-So Private Parts where technology & privacy collide

Seen At 11: Cyber Spies Could Target Your Child Through A Baby Monitor

April 21, 2015 at 11:28 pm **Filed Under:** App Hacks, Baby monitor, Baby Monitor App, Baby Monitor Hacks, Lance Ulanoff, Mashable, Smartphone, Weijia Jiang

FOLLOW US

OUR | NEWSLETTER

MOST VIEWED

Sources: Victim Of Quee
Invasion Likely Targeted

Family says hackers accessed a Ring camera in their 8-year-old daughter's room

Ring Camera Hacked

By Jessica Holley | December 10, 2019 at 7:02 PM CST - Updated December 12 at 3:42 PM

By **FOX19 Digital Media Staff** | April 25, 2014 at 3:14 AM EDT - Updated July 2 at 7:10 AM

CINCINNATI, OH (FOX19) - Heather Schreck was asleep around midnight in her Hebron home when a voice startled her.

"All of a sudden, I heard what sounded like a man's voice but I was asleep so I wasn't sure," Heather said.

Disoriented and confused, Heather picked up her cell phone to check the camera in her 10-month-old daughter Emma's room. The camera was moving, but she wasn't moving it.

Baby monitor camera hacked while child rocked to sleep

The Canadian Press
Published Thursday, July 23, 2015 6:10AM EDT
Last Updated Thursday, July 23, 2015 6:25PM EDT

CTV London: Hacker hijacks baby monitor

NOW PLAYING

OPP are warning parents to take precautions after a scary experi for a family northwest of London Bicknell explains.

FBI Warn Hackers are Using Hijacked Home Security Devices for ‘Swatting’

Author:
Becky Bracken

December 30, 2020
/ 4:42 pm

Stolen email credentials are being used to hijack home surveillance devices, such as Ring, to call police with a fake emergency, then watch the chaos unfold.

Stolen email passwords are being used to hijack smart home security systems to “swat” unsuspecting users, the Federal Bureau of Investigation warned this week. The

..and worse.

IoT Bot Nets

- **Mirai** – 100,000+ devices led to a 1.2Tbps DDoS (Trend Micro, 2016)
  - Eventually grew to 600,000+ devices, with 100s-of-thousands of cameras
- **BASHLITE** – 1,000+ devices led to a 400Gbps DDoS (Ashford, 2016)
- **Satori** – 800,000+ devices led to a 1Tbps DDoS (Vaas, 2019)
- **Tsunami/Fbot** – 35,000+ devices led to 100Gbps DDoS (Vaas, 2019)

IoT Security Frameworks, Standards, & Certifications

Year	Version	Organization	Title	Controls
2014	N/A	NCC Group	*Security of Things: An Implementers' Guide to Cyber-Security for Internet of Things Devices and Beyond*	82
2017	2.5	Online Trust Alliance	*IoT Trust Framework*	40
2018	N/A	UK DCMS	*Code of Practice for Consumer IoT Security*	13
2019	N/A	UL	*IoT Security Rating*	43
2020	2.1	IoT Security Foundation	*IoT Security Compliance Framework*	240
2020	1.1	ioXt	*IoT Security Certificate, Base Profile*	22
2021	Pre-1.0	OWASP	*IoT Security Verification Standard*	125
2021	2.0	Cloud Security Alliance	*IoT Security Controls Framework*	155
2021	N/A	CTIA	*Cybersecurity Certification Program for IoT Devices*	45

Additional roll-up guidance published by ENISA (2017; 83 controls) & CSDE (2019; 13 controls)

Previous IoT Camera Research

Hacking IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities
(Stanislav & Beardsley, 2015)

Broad Market? ⛔

- Baby monitors were only being assessed
- Only a total of nine cameras were evaluated
- Highly variable camera prices and release years

Multi-dimensional? ⚠️

- Only seven general security criteria were tested
- Unspecific test cases/control guidance published
- Assessment criteria not via standard/framework

Previous IoT Camera Research

Hacking IoT: A Case Study on Baby Monitor Exposures and Vulnerabilities
(Stanislav & Beardsley, 2015)

Broad Market? ⛔

- Baby monitors were only being assessed
- Only a total of nine cameras were evaluated
- Highly variable camera prices and release years

Multi-dimensional? ⚠

- Only seven general security criteria were tested
- Unspecific test cases/control guidance published
- Assessment criteria not via standard/framework

An IoT Analysis Framework: An Investigation Of IoT Smart Cameras' Vulnerabilities
(Alharbi & Aspinall, 2018)

Broad Market? ⛔

- 20% doorbell and 80% home security cameras
- Only a total of five cameras were evaluated
- No uniform camera selection criteria was used

Multi-dimensional? ⚠

- 13 test cases defined but inconsistently followed
- Pass/partial/fail criteria not clearly defined
- Test cases not mapped to standards/frameworks

Problem Statement

The Internet of Things is generally valued in usefulness, but also **generally deemed untrustworthy for security**, by consumers in the market (Cisco, 2017). With ongoing news stories covering compromised IoT cameras, ranging from baby monitors (Rascon & Aragon, 2018) to doorbells (Whittaker, 2019), trust will be difficult to establish **without a holistic approach** to securing these powerful devices.

While numerous IoT security frameworks have been released (OTA, 2015; IoTSF, 2016; CSA, 2019; U.K. DCMS, 2018), **consumers are unaware if that guidance has been realized** in the devices of today's market.

Previous research on IoT camera security has been **too shallow** in security control assessment & device sample size (Stanislav & Beardsley, 2015; Alharbi & Aspinall, 2018) and **did not reflect industry frameworks & standards**.

Objectives of the Researcher

1. A **multi-dimensional security-integrity analysis** – involving a technical assessment of industry-standardized security controls across IoT ecosystem components – of 40 connected cameras that are representative of the **broader market**, including security cameras, baby monitors, doorbells, pet feeders, & hidden cameras.

2. **Mapping of assessed IoT camera security properties** against two published IoT security frameworks that define their own criteria for what makes such a device secure.

3. **Quantified adherence** of each assessed device against the chosen IoT security frameworks to determine whether vendors are meeting such guidance in practice.

Research Methodology

A Quantitative Research Approach Using a Cross-sectional, Descriptive-analysis Survey Design with a Pragmatic Worldview

A **quantitative approach** "uses numerical, statistical, or mathematical analysis to provide results for the topic of study" (Babbie, 2014).

A **survey design** provides a "numeric description of trends, attitudes, or opinions of a population by studying a sample of that population. From sample results, the researcher generalizes or makes claims about the population" (Creswell, 2009).

A **cross-sectional** approach was selected for the survey as it addresses a point-in-time view of the sample, rather than longitudinal, which would require data collection over time (Creswell & Creswell, 2018).

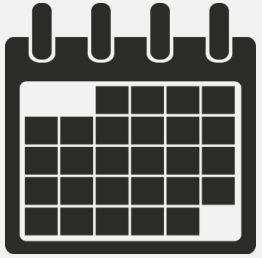
A **descriptive-analysis** approach to the survey helps to describe and summarize data points in a way which patterns may appear from the assessed sample (Rawat, 2021).

A **pragmatic philosophical worldview** allows a researcher to be free in their choices to address the study's topic in a manner that best meets its unique needs and purpose (Creswell & Creswell, 2018).

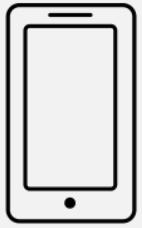
Sample Selection-Criteria

Purchased on Amazon.com

Native Wi-Fi Functionality



First Available During 2020



Supported Mobile Companion App

Retail Cost of ~$50 to ~$150

Unique Vendors Across Cameras

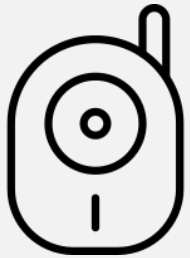
Sample Distribution

Security Cameras

20

Pet Feeders

5



Baby Monitors

5

Hidden Cameras

5

Doorbells

5

The Research Sample

How it Started

How it's Going

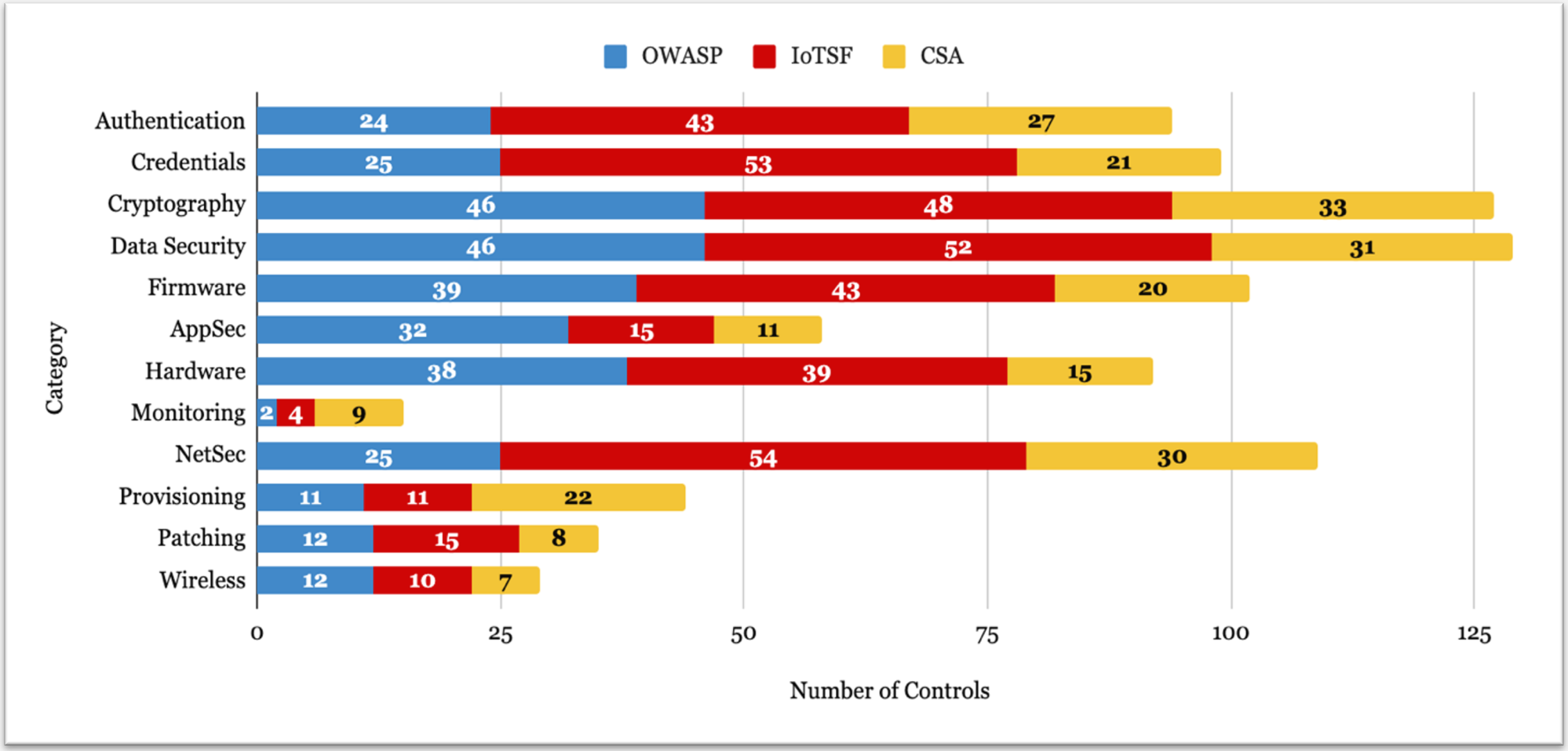
Industry Framework Controls to Generate Assessment-tracking Tool

Framework Controls in Scope

102/124 (82%)

139/239 (58%)

63/155 (41%)



Framework Evidence Gathering Test Matrix

68 total control tests were generated to source the evidence needed to populate the assessment-tracking tool data for the **304** in-scope framework controls

Sample Evidence Gathering Text

- **Description:** Determine if Wi-Fi usage is secured (e.g., non-generic passphrase, modern protocol) and disabled when not necessary for device functionality, without WPS

- **Evidence Needed:** Verification that Wi-Fi is at least WPA2, requires a custom passphrase, that WPS is disabled, and AES-CCMP used

Description	Steps	Example Step for Phase
Device Information & Artifacts	6	Locate an FCC entry for the device, if applicable, and archive posted device photos
Internal Device Analysis	7	Review data sheets for each chipset and document relevant features (e.g., Secureboot)
Mobile Application Information & Artifacts	14	Interact with the mobile application, taking screenshots and recording packet captures
Network Interface Configuration	9	Determine if the device supports the WPA3 protocol for Wi-Fi communication
Access the Running Device	8	Assess candidate UART interfaces to determine their baud rate, pin out, and use case
Network Service Analysis	12	Discover any FTP, Telnet, SSH, and/or RTSP services exposed on the local LAN
Firmware Upgrade Analysis	12	Determine if the mobile application allows users to check for new firmware upgrades
Linux-based OS Analysis	17	Determine if RELRO, stack canaries, NX, PIE, and/or Fortify are used on that binary
Privacy Analysis	6	If supported, attempt a factory reset of the device using the documented physical reset
Data Completeness & Quality Check	3	Review collected artifacts to populate missing data in the assessment-tracking mechanism

Data Collection Across 10 Phases

Assessment Hardware

Commonly Used Physical Tooling

- Multimeter
- USB to TTL serial cable
- Soldering iron
- Hot air gun
- eMMC breakout socket
- Soldering station
- Shikra
- Bus Pirate
- SOIC 8-pin clip
- Magnifying glass

Primary Assessment System

Raspberry Pi 4 B (Kali Linux 2020)

Secondary Assessment System

Apple MacBook Air (macOS 11)

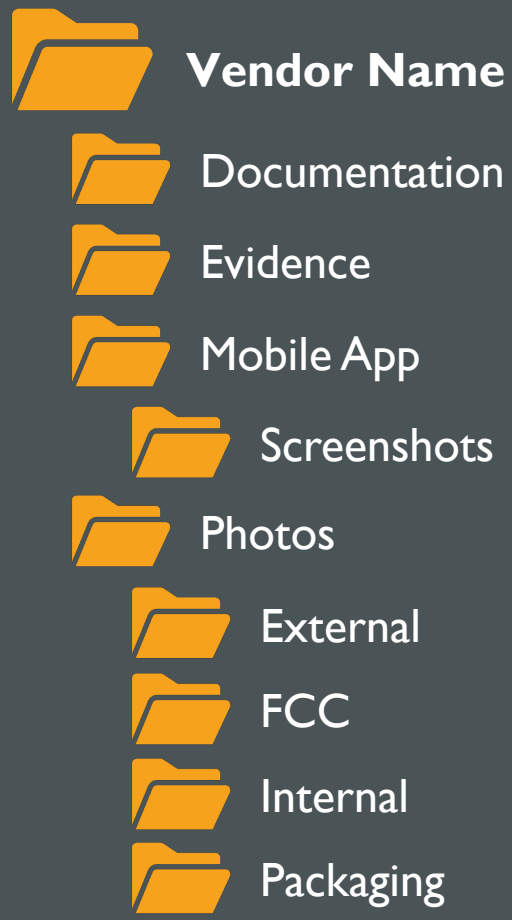
Mobile Assessment Device

Motorola Moto G7 Play (Android 10)

Assessment Wi-Fi Access Point

TP-Link WR841N (DD-WRT)

Instrumentation and Evidence Organization



Purpose	Utilities Used
Mobile Man-in-the-Middle	mitmproxy
Network Packet Capture	Wireshark
ARP Spoofing	bettercap
Extract APK	d2j-dex2jar & apktool
File Analysis	file, grep, hexdump
USB Listing	lsusb
Password Cracking	hashcat
Binary Security	checksec
SSL/TLS Security	sslyze & sslscan
Wi-Fi Analysis	kismet
Serial Console	GTKterm
Firmware Analysis	binwalk
Flash Dump	flashrom
Port Scanning	nmap
Android Debug	adb
RTSP Streaming	VLC & ffmpeg
MQTT Analysis	MQTT Explorer
Binary Analysis	IDA & Ghidra

Results

Organization	Publication Title	Controls Used
United Kingdom's Department for Digital, Culture, Media and Sport (DCMS)	Code of Practice for Consumer IoT Security	9/13 (69%)
European Telecommunications Standards Institute (ETSI)	Cyber Security for Consumer Internet of Things: Baseline Requirements, EN 303 645 V2.1.1	42/62 (68%)
N/A – Custom for this dissertation	My Proposed IoT Security Framework	66/66 (100%)

Mapping Assessment Findings to IoT Security Frameworks

Assessment-tracking Tool Data Mapping to Security Controls

Sample from DCMS

- **7: Ensure software integrity**
  - All firmware updates are sent over HTTPS
  - Secure Boot is available and actively in use
  - Firmware is digitally signed by the vendor

Sample from ETSI

- **5.1-2: Unique passwords per device**
  - No Linux accounts with passwords are set
  - No default device passwords are set
  - No hardcoded Wi-Fi pairing password is set

Industry frameworks often require *numerous* parts of the study's assessment-tracking tool's data structure to determine an outcome for that one control test to *Pass* or *Fail*

My Proposed IoT Security Framework

Example Control

Description: The device does not run a hosted web server that is network accessible (beyond localhost) that may support device management, streaming, or other features.

Test: If a device hosts a local web server that is network accessible, the device has failed the control.

66 controls spread across 10 categories that focus on meaningful quality over quantity

Categories (e.g., Mobile Security) try to cover gaps missed in other frameworks

The data structure of the assessment-tracking tool directly influenced test criteria

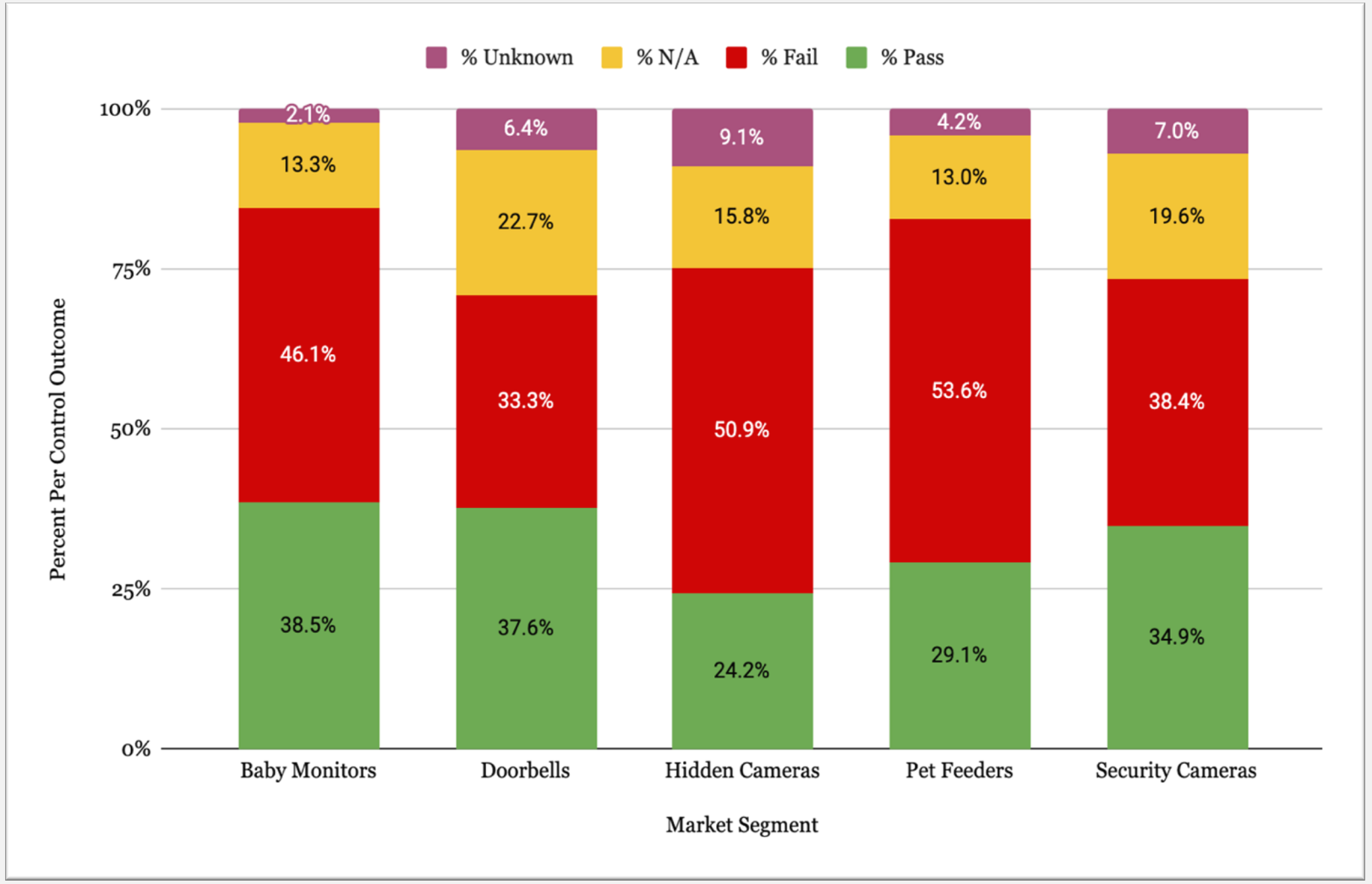
Wording for control descriptions and test criteria were kept as simple as possible

In circumstances that a control is reliant on another control, a dependency is clearly noted

Straightforward control testing allows for more accurate results to be defined

Results for
My Proposed Framework

Absolute Testing



My Proposed Framework

Roll-up by Camera Market Segment

Affirmative Testing

Market Segment	Pass / (Pass+Fail)	Fail / (Pass+Fail)
Baby Monitors	45.5%	54.5%
Doorbells	53.0%	47.0%
Hidden Cameras	32.3%	67.7%
Pet Feeders	35.2%	64.8%
Security Cameras	47.6%	52.4%
Average	44.4%	55.6%

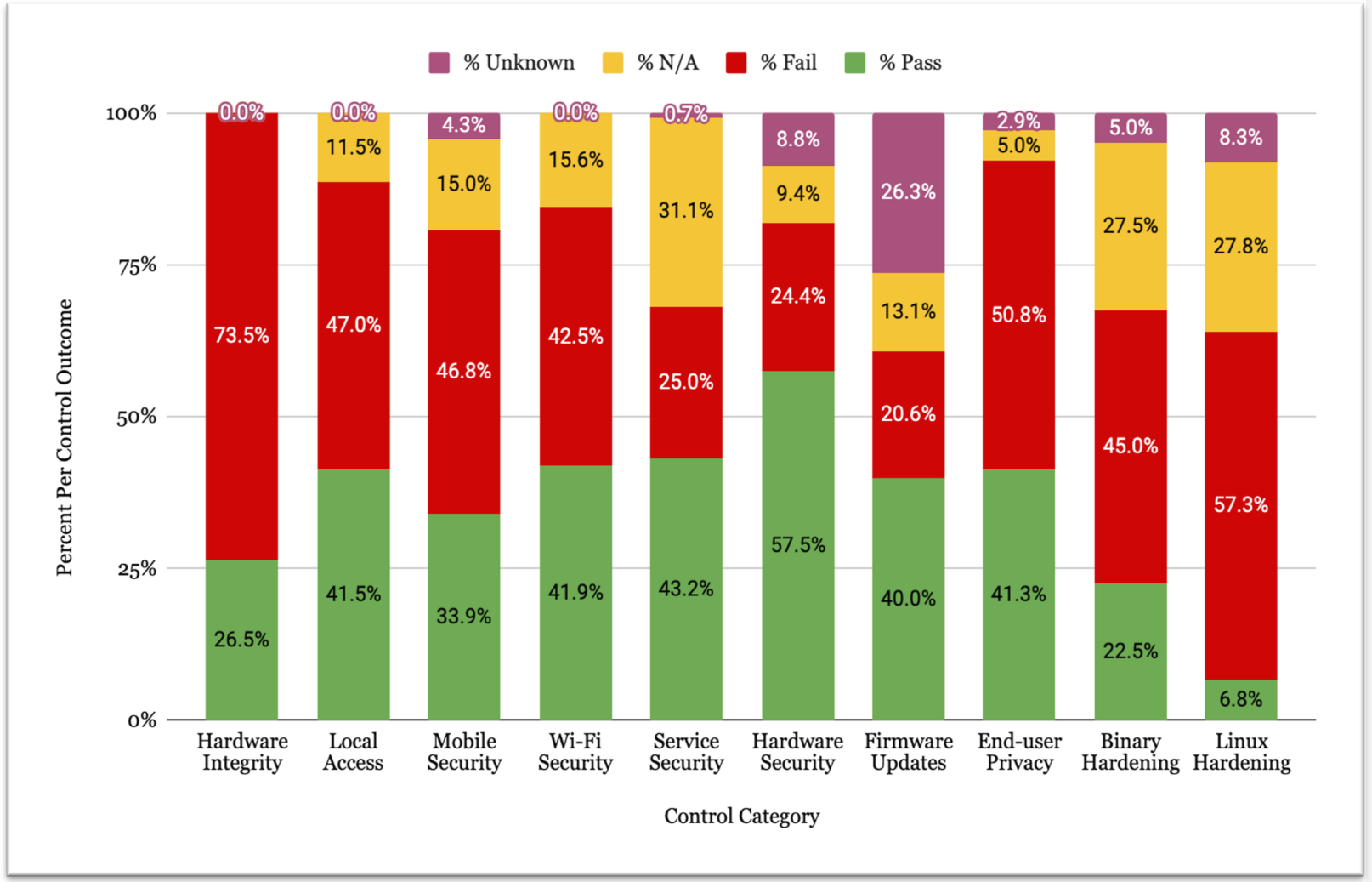
Most favorable (highest) pass rate…

Absolute: Baby Monitors (38.5%)
Affirmative: Doorbells (53.0%)

Least favorable (highest) fail rate…

Absolute: Pet Feeders (53.6%)
Affirmative: Hidden Cameras (67.7%)

Absolute Testing



My Proposed Framework

Roll-up by Control Category

Affirmative Testing

Category	Pass / (Pass+Fail)	Fail / (Pass+Fail)
Hardware Integrity	26.5%	73.5%
Local Access	46.9%	53.1%
Mobile Security	42.0%	58.0%
Wi-Fi Security	49.6%	50.4%
Service Security	63.3%	36.7%
Hardware Security	70.2%	29.8%
Firmware Updates	66.0%	34.0%
End-user Privacy	44.8%	55.2%
Binary Hardening	33.3%	66.7%
Linux Hardening	10.5%	89.5%
Average	45.3%	54.7%

Most favorable (highest) pass rate…

Absolute: Hardware Security (57.5%)
Affirmative: Hardware Security (70.2%)

Least favorable (highest) fail rate…

Absolute: Hardware Integrity (73.5%)
Affirmative: Linux Hardening (89.5%)

Affirmative Pass Rate

Category	Baby Monitors	Doorbells	Hidden Cameras	Pet Feeders	Security Cameras
Hardware Integrity	**44.0%**	32.0%	8.0%	4.0%	31.0%
Local Access	41.7%	**54.2%**	44.0%	44.0%	48.1%
Mobile Security	37.9%	**53.1%**	29.2%	35.7%	44.2%
Wi-Fi Security	**66.7%**	**66.7%**	20.0%	38.9%	53.7%
Service Security	**73.5%**	71.1%	50.0%	52.9%	64.6%
Hardware Security	68.4%	**75.0%**	70.6%	50.0%	74.6%
Firmware Updates	64.5%	**70.8%**	45.5%	56.5%	69.5%
End-user Privacy	50.0%	**51.7%**	32.1%	50.0%	43.8%
Binary Hardening	26.7%	33.3%	33.3%	30.0%	**37.9%**
Linux Hardening	**13.0%**	5.3%	10.5%	12.5%	9.5%
Average	48.6%	51.3%	34.3%	37.5%	47.7%

My Proposed Framework

Roll-up by Control Category, Cont.

Top* Result by Category…

- **Baby Monitors:** 4
- **Doorbells:** 6
- **Hidden Cameras:** 0
- **Pet Feeders:** 0
- **Security Cameras:** 1

* Tie for "Wi-Fi Security"

My Proposed Framework
Top 10 Results by Camera

AFFIRMATIVE PASS RATE

Vendor	Pass / (Pass+Fail)
Akaso	67.5%
StartVision	63.9%
WOHOME	62.9%
Anbes	62.5%
Eufy	61.9%
Ecobee	58.8%
Victure	57.5%
DCT	56.4%
Euarne	55.6%
Vacos	55.3%

ABSOLUTE PASS RATE

Vendor	Pass
Energizer	48.5%
Ecobee	45.5%
Feit Electric	45.5%
VTech	45.5%
Kami Baby	45.5%
TP-Link	45.5%
Motorola	43.9%
Akaso	40.9%
Eufy	39.4%
Aqara	39.4%

Ecobee had the <u>most favorable</u> composite result at #6 Affirmative and #2 Absolute pass rates

AFFIRMATIVE FAIL RATE

Vendor	Fail / (Pass+Fail)
Ecwey	74.1%
Pambrum	71.2%
VicZone	70.4%
Moonxiao	69.5%
iSmartPet	68.6%
Sense-U	68.6%
Jennov	67.3%
HONGSA	67.2%
HeimVision	66.7%
Didog	66.7%

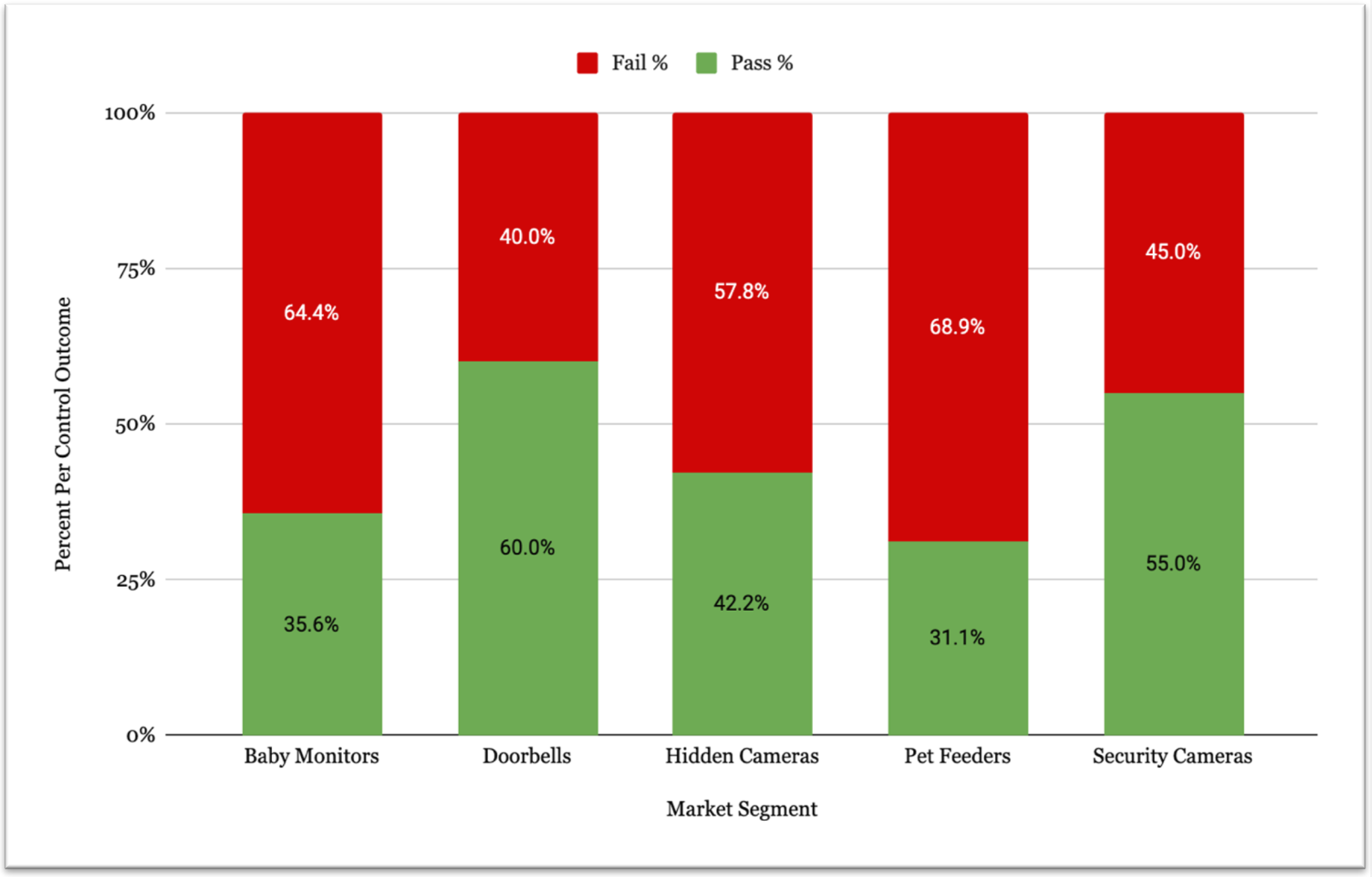
ABSOLUTE FAIL RATE

Vendor	Fail
Moonxiao	62.1%
Ecwey	60.6%
HeimVision	60.6%
HONGSA	59.1%
VicZone	57.6%
Didog	57.6%
Anran	57.6%
Pambrum	56.1%
Jennov	56.1%
CellBee	56.1%

Ecwey had the <u>least favorable</u> composite result at #1 Affirmative and #2 Absolute fail rates

Results for
DCMS

Outcomes by Market Segment



DCMS

Outcomes by Control Focus

Control Focus	Pass	Fail
No default passwords	35.0%	65.0%
Implement a vulnerability disclosure policy	10.0%	90.0%
Keep software updated	50.0%	50.0%
Securely store credentials and security-sensitive data	40.0%	60.0%
Communicate securely	37.5%	62.5%
Minimise exposed attack surfaces	47.5%	52.5%
Ensure software integrity	50.0%	50.0%
Make it easy for consumers to delete personal data	67.5%	32.5%
Make installation and maintenance of devices easy	100.0%	0.0%

Most favorable (highest) pass rate…

Doorbells (60.0%)

Least favorable (highest) fail rate…

Pet Feeders (68.9%)

DCMS
Top Results by Camera

HIGHEST PASS RATE

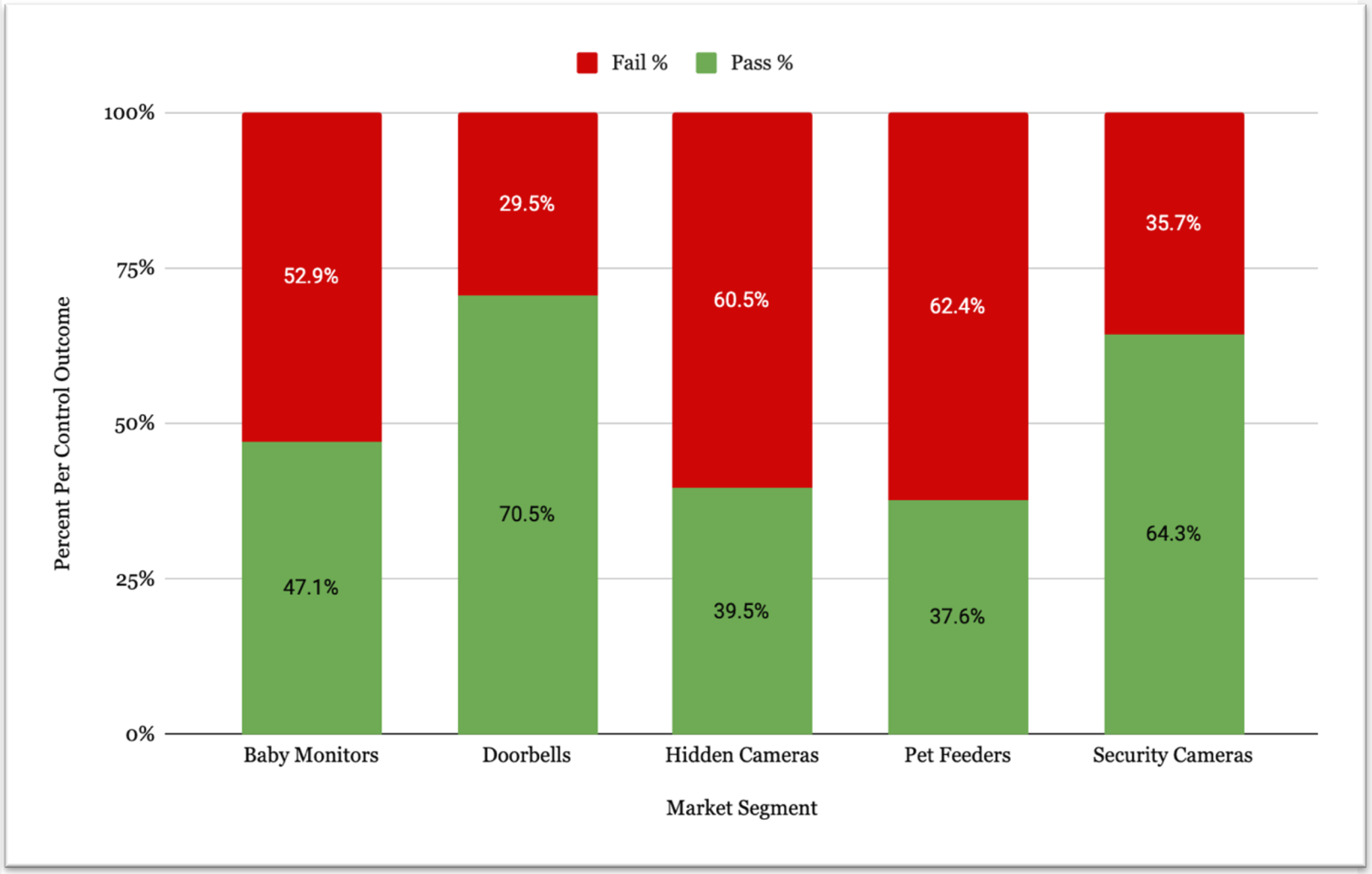
Market Segment	Vendor	Pass
Doorbell	Eufy	77.8%
Hidden Camera	Camakt	77.8%
Security Camera	Akaso	77.8%
Security Camera	Amcrest	77.8%
Security Camera	DCT	77.8%
Security Camera	Ecobee	77.8%
Security Camera	StartVision	77.8%
Security Camera	WOHOME	77.8%
Baby Monitor	Motorola	66.7%
Doorbell	Wuuk	66.7%
Security Camera	Anbes	66.7%
Security Camera	Conico	66.7%
Security Camera	Eversecu	66.7%

LOWEST PASS RATE

Market Segment	Vendor	Pass
Baby Monitor	CellBee	11.1%
Pet Feeder	HONGSA	11.1%
Baby Monitor	VTech	22.2%
Hidden Camera	Pambrum	22.2%
Pet Feeder	Didog	22.2%
Security Camera	Anran	22.2%
Security Camera	Jennov	22.2%
Security Camera	Moonxiao	22.2%

Results for **ETSI**

Outcomes by Market Segment



ETSI

Outcomes by Control Focus

Category	Pass	Fail
No universal default passwords	44.0%	56.0%
Implement a means to manage reports of vulnerabilities	20.0%	80.0%
Keep software updated	66.3%	33.8%
Securely store sensitive security parameters	16.3%	83.8%
Communicate securely	53.2%	46.8%
Minimize exposed attack surfaces	64.6%	35.4%
Ensure software integrity	67.5%	32.5%
Ensure that personal data is secure	45.0%	55.0%
Make it easy for users to delete user data	67.5%	32.5%
Make installation and maintenance of devices easy	100.0%	0.0%

Most favorable (highest) pass rate…

Doorbells (70.5%)

Least favorable (highest) fail rate…

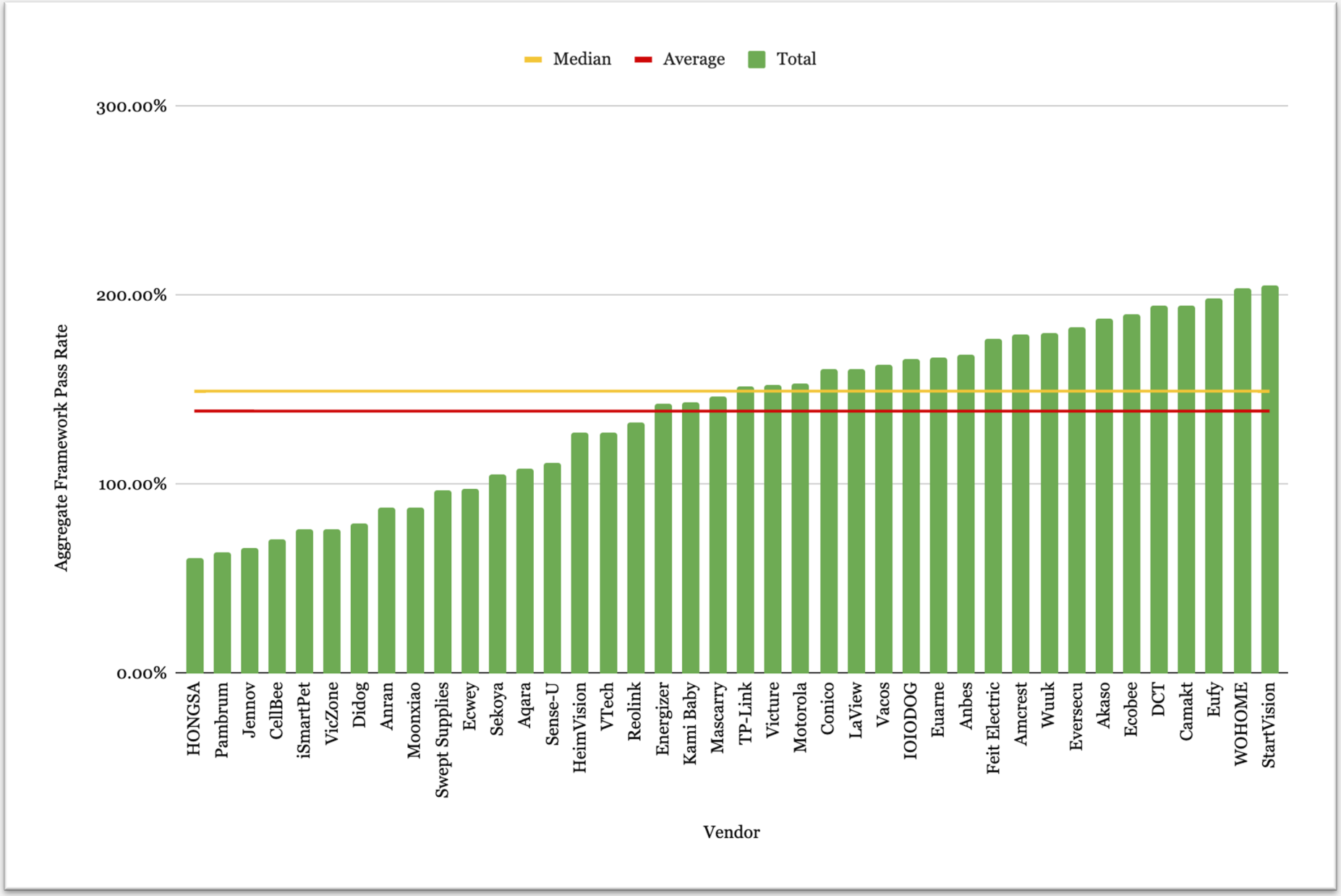
Pet Feeders (62.4%)

ETSI

RESULTS BY CAMERA

Aggregated Results

Aggregated Framework Pass Rate by Camera Vendor

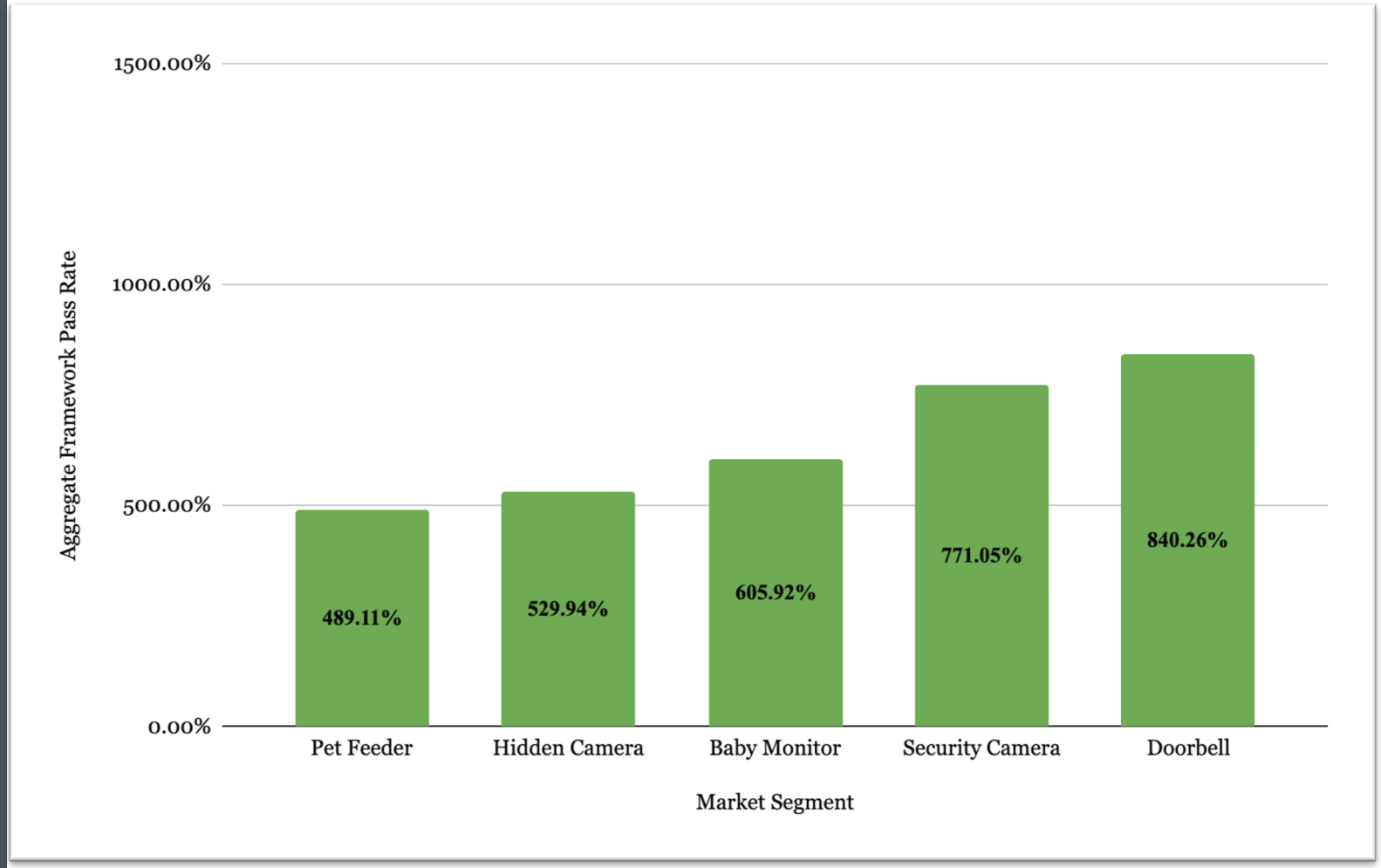


Each camera can achieve 100% adherence per framework – 300% in aggregate possible

Overall

Aggregated Pass Results by Segment

By aggregating the total achieved pass rate across each market segment*, the results of the three frameworks can be blended to minimize any bias



* Security Camera results are divided by 4 due to having a sample of n=20 instead of n=5

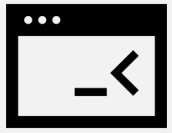
Overall Result Summary

Aggregate pass rate of cameras, plotted against their price

- **Doorbells** had the *most favorable* result for all three frameworks* and the highest aggregate pass rate overall
- **Pet Feeders** had the *least favorable* result for DCMS & ETSI, second least favorable result for my proposed framework, and the lowest aggregate pass rate overall

* Using Affirmative testing results for the Proposed Framework

Network-facing Services



Telnet listening on 9/40 (23%) of cameras

FTP listening on 2/40 (5%) of cameras

RTSP listening on 8/40 (20%) of cameras

Webserver listening on 15/40 (38%) of cameras

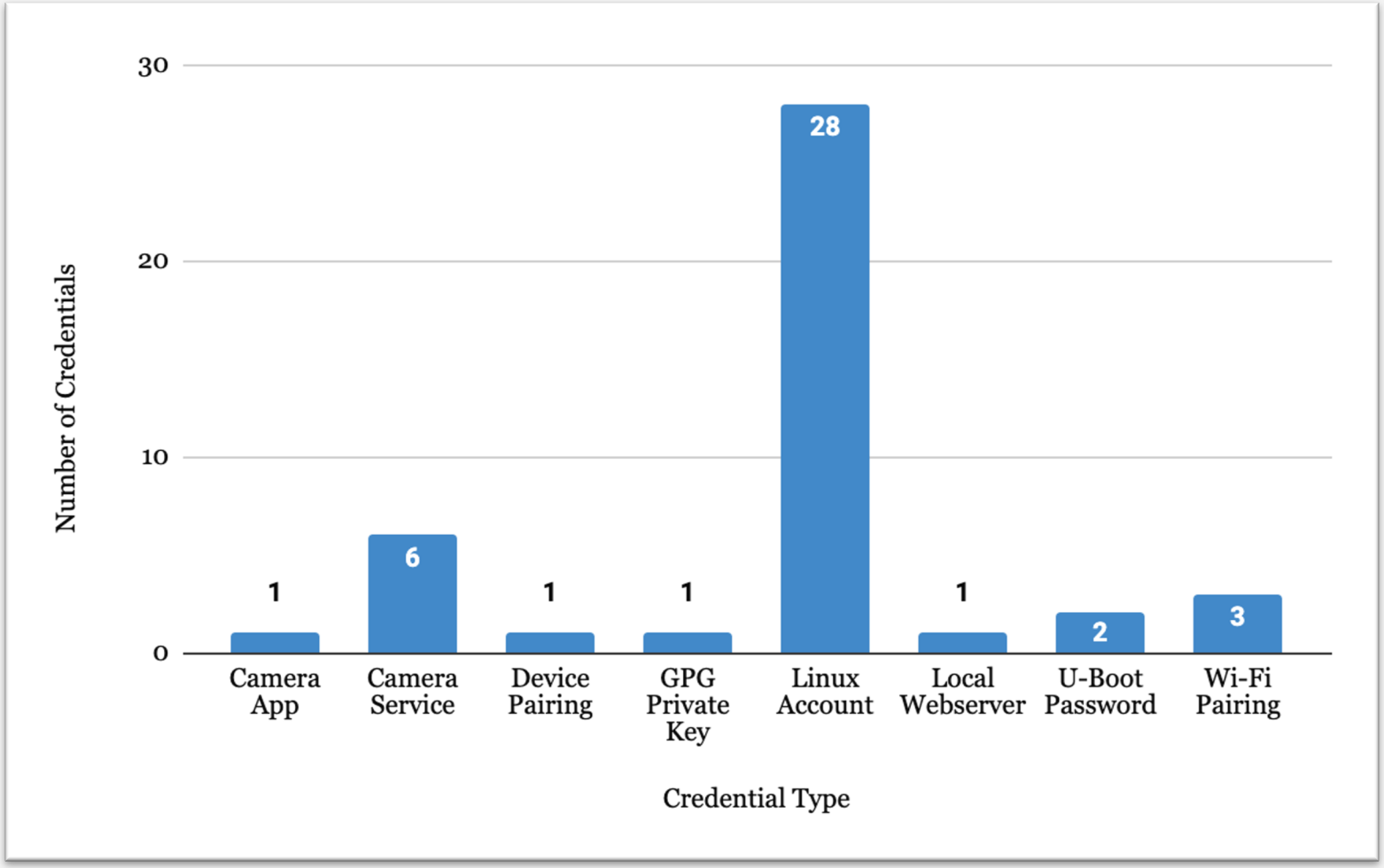
Linux Binary Hardening (n=27)

Binary Security Feature	# of Cameras
Relocation Read-Only (RELRO)*	7 (26%)
Stack Canaries	8 (30%)
Non-Executable (NX) Stack	13 (48%)
Position Independent Executables (PIE)	0 (0%)
Binary Symbols Removed	24 (89%)
FORTIFY_SOURCE Flag	2 (7%)
Address Space Layout Randomization (ASLR)*	7 (26%)

* RELRO is counted with 'Partial' and ASLR with '1' or '2' setting

- 23/29 (79%) of Linux-based cameras had their root account hash found
- Four root accounts had no password configured at all
- Linux Hash-type Usage
  - des-crypt: 11
  - md5-crypt: 9
  - sha-512: 4

Extracted Credentials



Conclusion

Contributions

Framework Mapping Results

Assessment Methodology

Gathered Device Data Set

Proposed IoT Framework

Extracted Device Credentials

Contribution resources available at https://github.com/mstanislav/phd-dissertation

Limitations

- Selection criteria led to the exclusion of notable brands (e.g., Nest)
- Devices were placed into one segment but may fit others, too
- Device variance (e.g., OS, hardware) limit full 1-to-1 comparisons
- Frameworks often require interpretation on how they may apply
- A control *Pass* result occurs if insufficient evidence exists to *Fail it*
- Device acquisition via Amazon is limited by availability/vendors
- Finite time & technical restrictions led to *Unknown* device results
- Unique vendors can still have full duplication (e.g., Anran & Jennov)
- If evidence sources are unretrievable less *Fail* results are achievable
- A single device is not sufficient to judge a vendor's product security

Future Research

Map the data set captured from this study's sample against other IoT security frameworks' controls, enabling additional analysis that will further enrich the conclusions that are able to be drawn via further industry-driven perspectives.

Utilize this study's data-gathering process to perform similar research against additional IoT cameras, which would increase the sample size from the larger population, allowing for more representative conclusions to be drawn overall.

The detailed data-gathering process was conducted through mostly manual steps but could be automated in numerous places to allow further devices to be added to the generated data set more quickly and with less potential for human error.

Vulnerability assessment, exploitation, and/or validation of security controls (e.g., firmware signing) were out-of-scope for the purpose of this study but would provide additional data points that would complement the analysis of these devices.

Audience Questions