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

- Problem Statement
- Objectives of the Researcher
- Contributions to the Discipline
- Literature Review
- Research Methodology
- Audience Questions

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 standards & frameworks have been released (Online Trust Alliance, 2015; IoT Security Foundation, 2016; Cloud Security Alliance, 2019; U.K. Department for Digital, Culture, Media & Sport, 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-published frameworks & standards.

Objectives of the Researcher

1. Perform 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. Map assessed IoT camera security properties against two published IoT security frameworks that define their own criteria for what makes such a device secure.

3. Quantify the adherence of each assessed device against the chosen IoT security frameworks to determine whether vendors have taken advantage of such guidance.

Contributions to the Discipline

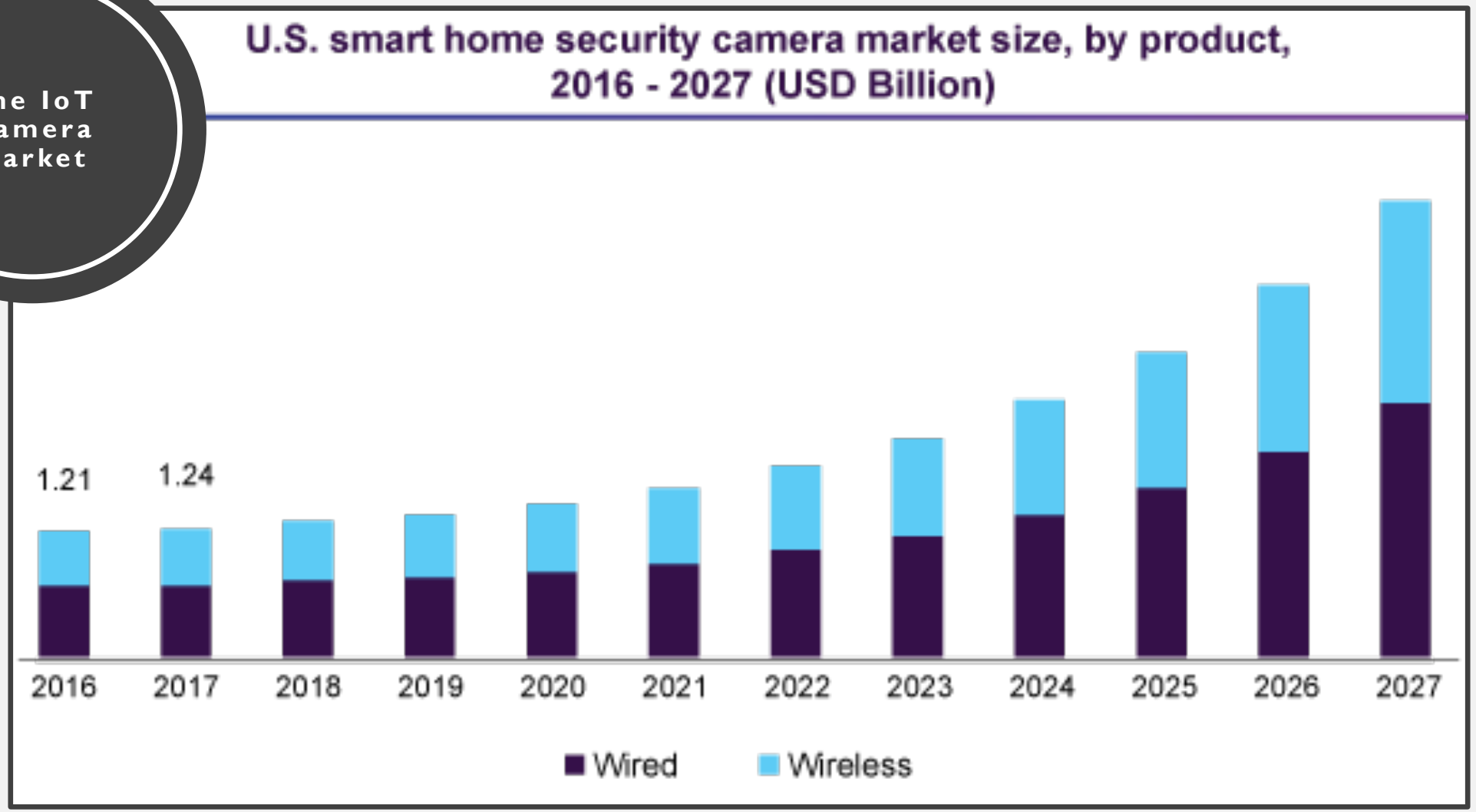
This research seeks to contribute a current, representative, and detailed analysis of Internet-connected camera security adherence to widely published IoT security standards.

Industry professionals, vendors, academics, and consumers alike will be able to determine if the broader IoT camera market space is maximizing the published guidance on providing secure products to the market, helping to assert whether consumer mistrust is warranted.

Literature Review

The IoT Camera Market

(Grand View Research, 2020)



The global smart home security camera market size was valued at USD 3.71 billion in 2019

Of 3,000 U.S. & Canadian Consumers Regarding IoT…

52% have either a low level of trust or no trust at all that their data is secure

Only **9%** have a high level of trust that their data is secure

(Cisco, 2017)

Trust is "a willingness to be vulnerable to another party" (Schoorman, Meyer, & Davis, 2007).

Opaque by Design

Common End-point

- Owner Customization
- Detailed Logging
- Anti-malware/virus
- Human-driven Interfaces
- Firewall Configuration
- Filesystem Accessibility
- Operating System Choice

Common IoT Device

- Restricted Customization
- Limited Logging
- Uncommon Anti-malware/virus
- Computer-driven Interfaces
- Minimal Network Security
- Obscured Filesystem Access
- Vendor Operating System

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 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).

“Console Cowboys posted its instructions on accessing the cameras on January 10, and over the next two days a list of links to over 1,000 camera feeds appeared on Pastebin” (Notopoulos, 2012).

“The "cgi-bin" directory is mapped to the root directory of http server of the camera, knowing this we can make a request to http://192.168.1.17/anony/mjpg.cgi and surprisingly we get a live stream from the camera” (Console Cowboys, 2012).

But Wait, it Gets Worse!

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)

..and 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

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)

U.S. Government Actions

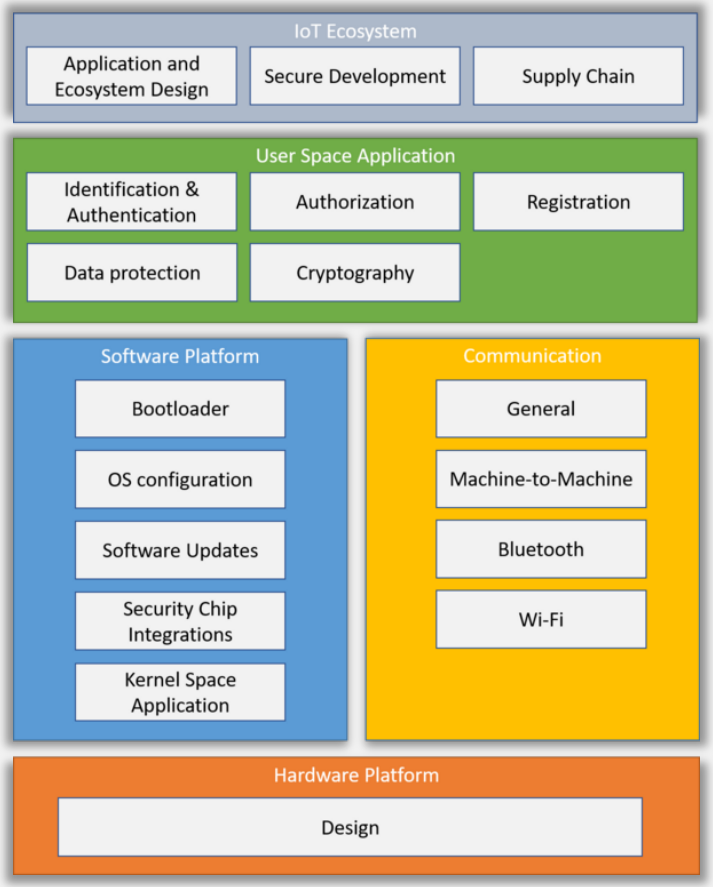
- **Federal Trade Commission (FTC)**
  - Settlement with TRENDnet (FTC, 2014) and D-Link (FTC, 2017) over each company failing to appropriately secure their Internet-facing cameras sold to consumers
- **New York Department of Consumer Affairs (NY DCA)**
  - Subpoenaed four IoT baby monitor vendors as a result of privacy abuses of cameras and security research findings published detailing weak protections (Greenberg, 2016)
- **Consumer Product Safety Commission (CPSC)**
  - Held a hearing on the safety hazards of IoT devices, leading to the publication by one of the CPSC commissioners regarding IoT safety practices (Kaye & Midgett, 2019)
- **U.S. Congress**
  - Passed the *IoT Cybersecurity Improvement Act of 2020* to have the National Institute of Standards and Technology (NIST) codify their security recommendations for IoT

IoT Security Frameworks, Standards, & Certifications

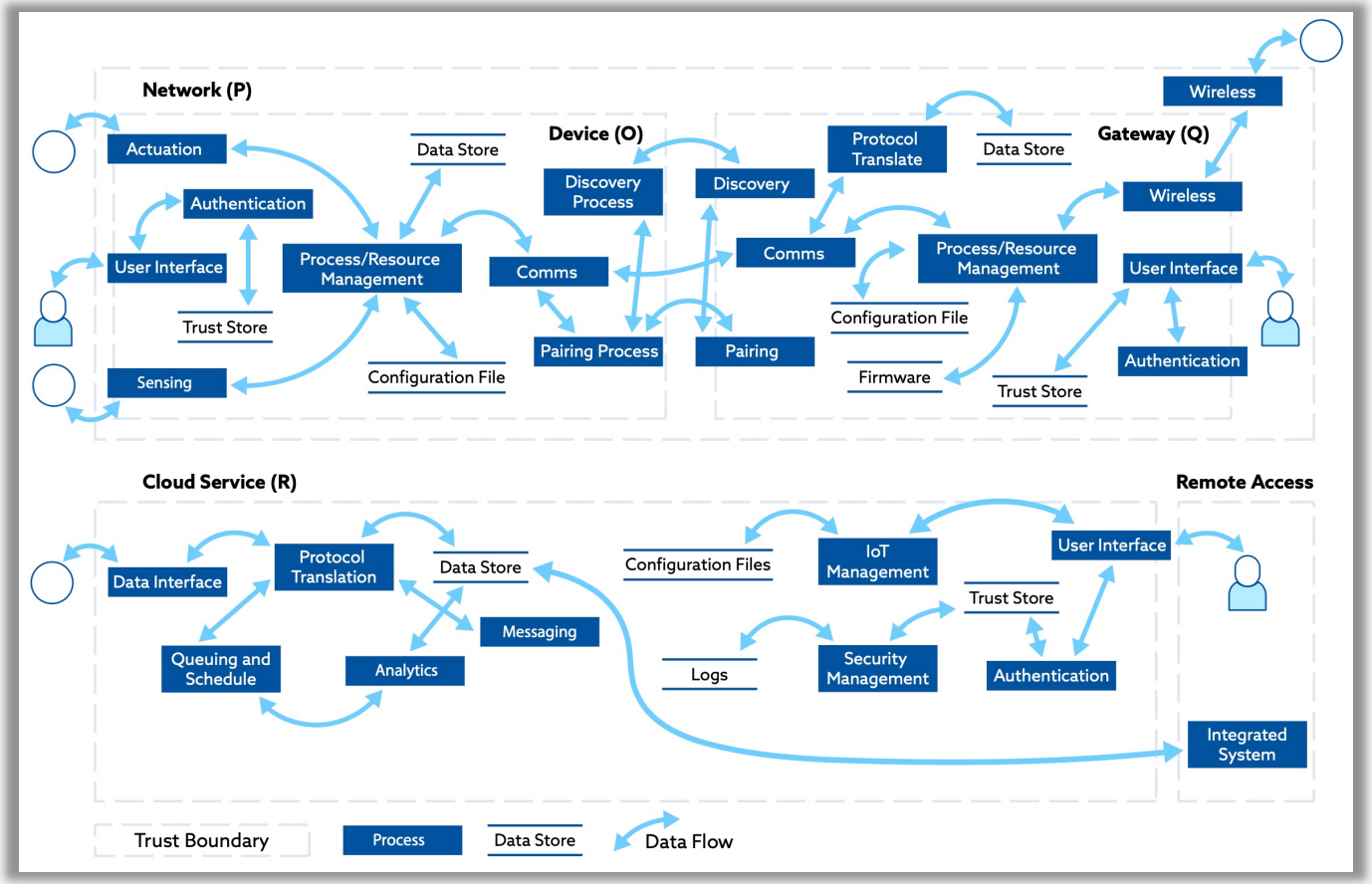
Year	Version	Organization	Title	Controls
2014	N/A	NCC Group	*Security of Things: An Implementers' Guide to Cyber-Security for Internet of Things Devices and Beyond*	82
2017	2.5	Online Trust Alliance	*IoT Trust Framework*	40
2018	N/A	UK DCMS	*Code of Practice for Consumer IoT Security*	13
2019	N/A	UL	*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)

Varied Framework Approaches



OWASP, 2021



Cloud Security Alliance, 2021

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

Research Methodology

Overview

The proposed research will present findings regarding which security properties from applicable IoT security standards & frameworks are being achieved, or missed, by camera vendors within the assessed device sample.

The research analysis will help to highlight industry trends for what the most commonly achieved security controls are, which controls have the least implementation, and how this data differs across market segments.

Quantitative Analysis Using a Survey Design

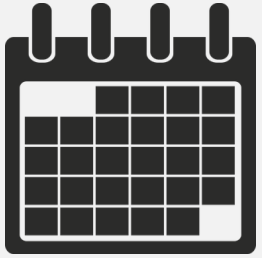
Quantitative research is "the process of collecting, analyzing, interpreting, and writing the results of a study" (Creswell, 2002).

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).

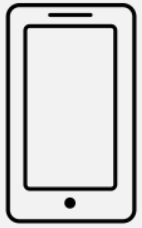
Sample Selection-Criteria

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

40 Distinct Sample Devices

Security

20

Pet Feeder

5

Baby Monitor

5

Hidden

5

Doorbell

5

The Research Sample

Assessment Tracking Tool

IoT Security Verification Standard

IoT Security Compliance Framework

IoT Controls Framework

1. Analyze Each IoT Framework
2. Consolidate Technical Controls
3. Deduplicate Guidance as Needed
4. Determine "Core" Technical Data
5. Define Necessary Test Procedures

Maximize breadth & depth of testing to avoid bias & "future proof" mapping

Gather Once, Reuse Many (…and Hedge Our Bets…)

OWASP	Cloud Security Alliance	IoT Security Foundation
IoT Security Verification Standard *(4.1.2)* *Verify that in case TLS is used, its configured to only use FIPS-compliant cipher suites (or equivalent).*	***IoT Security Controls Framework*** *(COM-07)* *Encrypt all transmission control protocol (TCP)-based communications*	***IoT Security Compliance Framework*** *(2.4.7.13)* *Where a TCP protocol, is used, it is protected by a TLS connection with no known vulnerabilities*

Representative Control Consolidation

Summary Control Text	Test Instrumentation	*Control Evidence*
Applicable network transmissions utilize TLS with modern cipher suites & protocol versions	***SSLyze*** or ***sslcli***	***Raw TLS scan results***

Ongoing Framework Mapping

Online Trust Alliance	UK DCMS	TBD
IoT Trust Framework *(Security #3)* *All IoT support web sites must fully encrypt the user session.*	***Code of Practice for Consumer IoT Security*** *(5)* *Data should be encrypted in transit, appropriate to the properties of the technology and usage.*	***Brand New IoT Security Framework*** *(2.3.4)* *There's no shortage of work in this space and this research will approach information gathering as such*

Mobile Applications

- dex2jar
- JD-GUI

Web Applications

- Burpsuite
- Arachni

TLS Configuration

- SSLyze
- sslcli

Wireless Analysis

- RTL-SDR
- Ubertooth One

Network Security

- mitmproxy
- Wireshark
- Nmap

Firmware Analysis

- Flashrom
- extractor
- hashcat

Hardware Analysis

- J-Link
- Shikra
- JTAGulator

Binary Analysis

- hardening-check
- IDA
- Ghidra

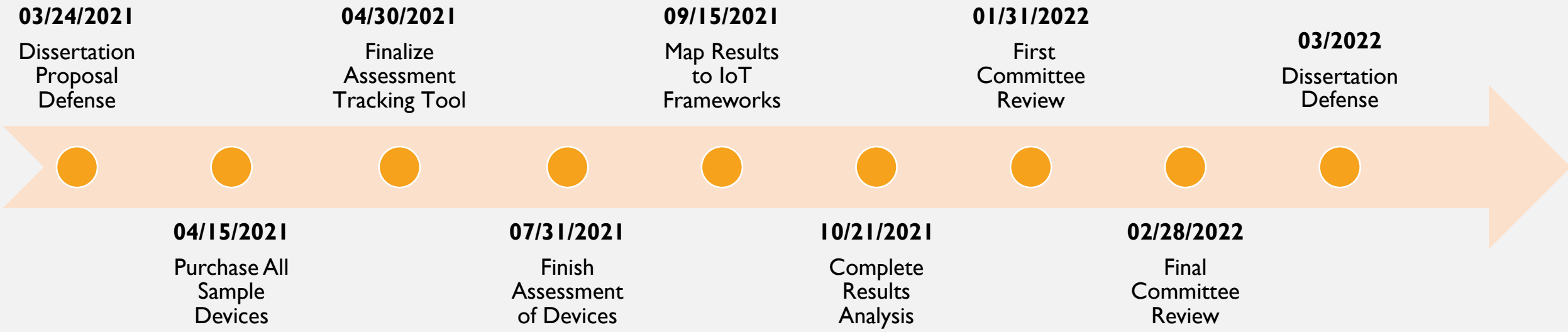
Testing Instrumentation

Legal Considerations

All assessment activities will be conducted in alignment to the U.S. Copyright Office's definition of "good-faith security research" as described in their security researcher exemption of the Digital Millennium Copyright Act (DMCA) for research conducted against consumer devices (U.S. Copyright Office, 2015).

In situations where material security flaws are noted in the course of this study, appropriate coordinated vulnerability disclosure (Carnegie Mellon University, 2017) will be conducted by the researcher to inform relevant vendor(s) of issues that require their action to mitigate risks posed to affected consumers.

Research Plan and Timeline



Audience Questions