A Peep Into the Iron Triangle: IoT Purchasing in a ‘Me First’ Society
Tyler Reguly, Manager, Security R&D, Tripwire
SecTor 2018
Who Am I?
@treguly

- Manager of Security R&D @ Tripwire
  - Over a decade of security research experience
  - Author of WebApp360 and current SSH implementation
  - Co-Founder VERT IoT Hack Lab

- Contributor to Industry Initiatives
  - Various OWASP / WASSEC Projects
  - CVSSv2 and CVSSv3

- Technical Editor
  - Practical Packet Analysis 2\textsuperscript{nd} and 3\textsuperscript{rd} Editions
  - Securing PHP Web Applications
  - Nmap Network Scanning

- Curriculum Developer
  - Developed two programs for Fanshawe College
  - Taught both courses

- Avid Gamer & Comic Enthusiast
IoT Hack Lab

Presented by Tripwire
The Iron Triangle and ‘Me First’ Attitudes

CONCEPT EXPLORATION
Iron Triangle
Cheaper, Faster, Better – Pick Two
Iron Triangle

*New and Improved* – Pick One!
How I feel

Peep Under the Iron Curtain

Daily Mail – March 6, 1946
Iron Triangle
The Insurmountable Divide

- First to Market
- Convenience
- Security
'Me First Attitudes'

Me! Me! Me

WHAT'S IN IT FOR ME?
The Story of Tiko

HOW FIRST TO MARKET AND EARLY ADOPTION BIT ME IN THE ASS
What is Tiko?

A Historic Failure

- Designed to be a game changer in 3D printing.
  - Unibody Design
  - Delta 3D Printer – 3 Arms controlling the print head
  - Enclosed print chamber
  - Wifi Capable
  - Browser-Based Software
- Kickstarter raised over $2.9M USD
Tiko’s Story
A Plagued Project

- Project plagued by development setbacks and funding misuse
- Missing shipping date by 1 year
- Many units were never shipped
- Ultimately, Tiko went under and most people did not receive their printers.
Tiko Security Implications

Do Bankrupt Products Matter?

1. Tiko was an AP – Did not support secure wireless communication.
2. Commands could be sent by anyone with device access, this included heat controls.
3. There was no method of manually update the firmware.
4. With bankruptcy, the servers shutdown. No more firmware updates.
Verified Response

CAN IOT IMPACT YOUR SAFETY?
Alarm Systems 101

“How Alarms Work in our Mind”
What is Verified Response?
Are you sure someone is breaking in?

- In order to avoid false alarms, alarm monitoring companies must verify alarm activations.
- Alarm verification methods:
  - Audio Device
  - Video Device
  - Multiple Zone Activations
  - Eyewitness
- False alarms are charged a fee, repeated false alarms face suspension.
Verified Response Opinions

Why Implement it?

- Police look to reduce false alarm calls.
- Increased workload on security monitoring companies.
  - Benefit for those with IoT Capabilities.
  - Loss for those with manual verification.
Security Implications

How does Verified Response Impact IoT?

VERIFIED RESPONSE

Eyewitness

IoT 50%

Multiple Activations
IoT Purchasing

DO PREVIOUS DISCLOSED VULNERABILITIES MATTER?
Baby Monitor Dilema

Past Research Considerations

* In 2015, multiple research teams announced vulnerabilities in baby monitors, including Tripwire’s Craig Young.
* Craig demonstrated the attack on Crime Watch Daily.

Captain Kuijt 7 months ago
To be fair, if you’re not gonna put a wireless in your house, just don’t put a wireless in your baby’s room.
Purchasing Decisions

Typical purchasing questions

- What did other users think?
- How many stars does it have?
- How frequently is it purchased
- Does it do everything I need?
- Does it have extra features?
- Do I need a warranty?
- Is it on sale anywhere?
Shopping for a Baby Monitor?

First Impressions?

6 results for "Summer Infant Baby Zoom Wi-Fi Video Monitor"

Showing selected results. See all results for Summer Infant Baby Zoom Wi-Fi Video Monitor.

Summer Infant Baby Secure 2.5" Pan/Scan/Zoom Video Baby Monitor
by Summer Infant
Eligible for Shipping to Canada
$99.98

Summer Infant Baby Pixel Video Baby Monitor with 5-inch Touchscreen and Remote Steering Camera, SleepZone Alerts, and Moonlite Night Vision Boost
by Summer Infant
Eligible for Shipping to Canada
$199.99

More options available:
$198.99 Other Sellers

Product Features
... when your baby exits their safe space. Voice Activated Video On/Off ...
Is your WIFI thermometer an IoT Device? Did you actually consider that when you bought it? Do you look up vulnerabilities reported in products before you buy? Does your significant other know what an IoT device is? How about your parent or child? Do they research before they buy?
Summary
Iron Triangle Redux
IoT Purchasing Checklist

Before You Buy

- Is the manufacturer reliable and likely to be in business for the lifetime of this product?
- Is the product competitive with similar offerings? Is it the first of its kind?
- How frequently does the vendor publish updates?
- Does the firmware auto-update or require manual intervention?
- Are there reported vulnerabilities?
- Does the vendor have a published security page?
IoT Purchasing Checklist
Within 30 days

- Does the wireless AP fail open?
- How robust is any related cloud interface?
- What data is transmitted to and from the cloud?
- How easy/difficult is it to actually update the firmware?
- Are adequate security measures protecting auth mechanisms?
- Port scan the device for interesting open services.
- Write a review!
Deep Dive Checklist
How well do you really know that smart outlet?

- Audit the firmware.
- Audit the WebUI.
- Reach out to the security team to test their responsiveness.
- Find other users investigating the same product line on mailing lists and forums.
- Take a training course