Friends, Not Foes: Rethinking the Vendor-Reseacher Relationship

Presented By: Rick Ramgattie (@rramgattie)

KEYNOTE
./whoami

• Rick Ramgattie
  – Building / Hacking Web Apps
  – Reverse Engineering Mobile Applications
  – IoT Security
  – Reading

• Security Analyst @ Independent Security Evaluators
Independent Security Evaluators

• Where:
  – Baltimore, MD and San Diego, CA

• What:
  – Security Assessments
    • Web
    • Mobile
    • Infrastructure
    • Native Applications

• How:
  – Whitebox, Blackbox, and everything in between
Outline

• The IoT Village.
• CTF Intro.
• Disclosure Models.
• Full vs. Responsible Disclosure.
• What can we do to make things better?
• Questions?
IoT Village Origin Story
IoT Village Origin Story

- Research:
IoT Village Origin Story

• Research:
  – Small Office Home Office (SOHO) Routers
• Research:
  – Small Office Home Office (SOHO) Routers
  – Network Attached Storage (NAS) Devices
IoT Village Origin Story
IoT Village Origin Story

• First SOHOelessly Broken:
  – 2014
  – DefCon 22

IoT Village Origin Story

• First SOHOpelessly Broken:
  – 2014
  – DefCon 22
  – 56 CVEs

IoT Village Origin Story
IoT Village Origin Story

• First IoT Village:
  – 2015
  – DefCon 23
  – Expanded SOHOpelessly
    Broken
IoT Village Origin Story

- SoHo – DefCon 22
- IoT Village – DefCon (23 – 25)
  - 30+ Devices CTF
  - 60+ Devices ZeroDay Track
  - 38 talks
  - 113 vulnerability disclosures
IoT Village

• DefCon 22 - 25
• DerbyCon 5 – 6 (2015-2016)
• RSA 2017
• BSides DC 2015 – 2016
• BSides Charm 2016 – 2017
• CypherCon 2017
• ToorCon 2015 – 2016
• HackerLabs Puerto Rico 2017
1. The Stage
2. The Zero Day Track
3. The CTF
CTF TIPS!

[1] Logo from a PSA Broadcast on the NBC
CTF Tips

1. Map the network:
   – Where are the devices?
   – What are the devices?
   – What is NMAP?
CTF Tips

2. Search all the surfaces:
   - Web App
   - Services (Ports)
CTF Tips

3. Think outside the box:
   – Be creative
   – Search for canned exploits. (The Documentation is out there.)
   – Linux Kung-Fu.
CTF Tips

4. Try not to project.
   – Try another device.
   – Research
   – Share
Helpful Links:

- Practical Reverse Engineering Pt. 4 (https://goo.gl/4FtYzd)
- Cameras, Thermostats, and Home Automation Controllers (https://goo.gl/1NpyyN)
- Hacking the D-Link DSP-W215 Smart Plug (https://goo.gl/9H8n8D)
- Multiple Vulnerabilities in ASUS Routers (https://goo.gl/fnGWoB)
- Samsung SmartCam (https://goo.gl/Kp1hRL)
- https://twitter.com/RRamgattie
You got this!
But why?

???
IoT Devices
IoT Devices
IoT Devices
IoT Devices
“Our bottom-up analysis for the applications we size estimates that the IoT has a total potential economic impact of $3.9 trillion to $11.1 trillion a year by 2025.”

“[B]y the end of 2017, over 20 per cent of organizations will have digital security services devoted to protecting business initiatives using devices and services in IoT.”

Vulnerability Disclosure?

???
Disclose or nah?

A. Disclose
Disclose or nah?

A. Disclose
B. Not Disclose
Disclose or nah?

A. Disclose
B. Not Disclose
Full Disclosure vs. Responsible Disclosure
Full Disclosure vs. Responsible Disclosure

Responsible Coordinated

Full

Full Disclosure vs. Coordinated Disclosure

- “… [Full Disclosure] provides all vulnerability details to everyone at the same time, a move designed to make vendors provide updates faster.”¹

“…one general definition of [Coordinated Disclosure] as most vendors define it is that the issue is reported privately to the vendor *and no one else* until the vendor issues a patch.”¹

Full Disclosure vs. Coordinated Disclosure

Full Disclosure
• Discloses all details of the vulnerability to Everyone.
• Goal is to improve security by bringing attention to the vulnerability and making everyone aware of the flaw.
• Disclosed at the researchers discretion.

Coordinated
• Discloses all details of the vulnerability to the Vendor.
• Goal is to help the vendor improve the products security by informing them of the vulnerability and giving time to fix the issue before it is publicly disclosed.
• Disclosed after the agreed disclosure date.
Full Disclosure vs. Coordinated Disclosure

Full Disclosure
• Discloses all details of the vulnerability to Everyone.

• Goal is to improve security by bringing attention to the vulnerability and making everyone aware of the flaw.

Coordinated
• Discloses all details of the vulnerability to the Vendor.

• Goal is to help the vendor improve the products security by informing them of the vulnerability and giving time to fix the issue before it is publicly disclosed.
Full Disclosure vs. Coordinated Disclosure

Full Disclosure
• Discloses all details of the vulnerability to **Everyone**.

• Goal is to improve security by **bringing attention** to the vulnerability and **making everyone aware** of the flaw.

• Publicly Disclosed at the researchers discretion.

Coordinated
• Discloses all details of the vulnerability to the **Vendor**.

• Goal is to **help the vendor improve the products security** by informing them of the vulnerability and giving time to fix the issue before it is publicly disclosed.

• Publicly Disclosed after the agreed disclosure date.
Well, what can go wrong?
Full Disclosure Example: The Witty Worm Attack

• On Friday March 19, 2004 it began to spread.
Full Disclosure Example: The Witty Worm Attack

• On Friday March 19, 2004 it began to spread.
• It targeted a buffer overflow vulnerability in Internet Security Systems (ISS) products.
Full Disclosure Example: The Witty Worm Attack

• On Friday March 19, 2004 it began to spread.
• It targeted a buffer overflow vulnerability in Internet Security Systems (ISS) products.
  – ISS RealSecure Network
  – RealSecure Server Sensor
  – RealSecure Desktop
• Within a half-hour it infected 12,000 computers
Full Disclosure Example: The Witty Worm Attack

• On Friday March 19, 2004 it began to spread.
• It targeted a buffer overflow vulnerability in Internet Security Systems (ISS) products.
  – ISS RealSecure Network
  – RealSecure Server Sensor
  – RealSecure Desktop
• Within a half-hour it infected 12,000 computers
• The worm took advantage of a flaw that was disclosed by a security company that believed in **full disclosure.**
Coordinated Disclosure Example: Brute Logic vs. Group On

- BruteLogic reported 32 instances of XSS in GroupOn.
- Responsible disclosure policy.
- He tweeted about the vulnerability after reporting it.
- Did not get the Bug Bounty payout.
Coordinated Disclosure Example: Brute Logic vs. Group On

- BruteLogic reported 32 instances of XSS in GroupOn.
- Responsible disclosure policy.
Coordinated Disclosure Example: Brute Logic vs. Group On

• BruteLogic reported 32 instances of XSS in GroupOn.
• Responsible disclosure policy.
• He tweeted about the vulnerability after reporting it.
  – He said that he found instances of the vulnerability.
Coordinated Disclosure Example: Brute Logic vs. Group On

- BruteLogic reported 32 instances of XSS in GroupOn.
- Responsible disclosure policy.
- He tweeted about the vulnerability after reporting it.
  - He said that he found instances of the vulnerability.
- Did not get the Bug Bounty payout.
Need help?
What we do to make things better?
A. What can vendors do to make things better?
What we do to make things better?

A. What can vendors do to make things better?
B. What can researchers do to make things better?
What can vendors do to make things better?

• Problems:
  – Availability.
  – Combativeness.
  – Naivety. (Unfamiliar with security)

• The Solution:
  – Bug bounty program.
  – Security related issues contact.
  – Finding vulnerabilities is good not bad.
  – Train your team. (Expose them to security mindset.)
  – Become part of the security community.
What can vendors do to make things better?

• Problems:
  – Availability.
  – Combativeness.
  – Naivety. (Unfamiliar with security)
What can vendors do to make things better?

- **Problems:**
  - Availability.
  - Combativeness.
  - Naivety. (Unfamiliar with security)

- **Solutions:**
  - Bug bounty program.
  - Contact for security related issues.
  - Finding vulnerabilities is good not bad.
  - Train your team. (Expose them to security mindset.)
  - Become part of the security community.
What can researchers do to make things better?

• The Problem:
  – Arrogance.
  – Not understanding the complexity of a problem.
  – Fear mongering? (Sometimes issues aren't as impacting as people think they are.)

• The Solution:
  – Bug Bounty Program, contact for reporting security vulnerabilities. (Adopt a security focused mindset.)
  – Finding vulnerabilities is not a bad thing, it is good thing. Then issues are fixed. (good guys finding issues is always a good thing.)
  – Train your team. (Expose them to security mindset.)
  – Become part of the security community.
What can researchers do to make things better?

• **Problems:**
  - Arrogance.
  - Not understanding the complexity of a problem.
  - Stop fear mongering?*
What can researchers do to make things better?

• Problems:
  – Arrogance.
  – Not understanding the complexity of a problem.
  – Stop fear mongering?*

• Solutions:
  – Play by the rules.
  – Work with companies to understand the complexity of an issue.
  – Understand that some issues have different impact.
Let’s wrap up!
Questions??