Issues with Embedded Device Disclosures:

Helping the Vendors and Recognizing the End-Users

Jerome Radcliffe
Security Researcher/Threat Analyst
@jradcliffe02

New Era In Disclosure

- Experienced companies have embraced security researchers
  - Pay Bounties on Reported Vulnerabilities
  - Encourage Security Research
- Inexperienced companies struggling
  - Taking the same actions that companies abandoned
  - Embedded Device engineers unaware of security implications

Mo’ Devices, Mo’ Problems

- Market demands devices be more connected
  - Tweet, e-mail, status updates, Bluetooth
- Explosion of Data
  - Data Mining, Smart-Grid, Environmental
- Everything has a CPU, Everything is connected
  - …Everything is vulnerable

No Protection

- Desktop Systems, Servers have protection
  - Firewalls, IDS, IPS, Vulnerability Scanners,
- New devices “Outside The Frame”
  - Lack well defined perimeter
  - Not Stationary
- No Standards
  - TCP, UDP, 802.11, etc – Well Defined
  - *Many* Proprietary Methods

Disclosure Guidelines

- Rule #1: Do No Harm.
  - If there is a vulnerability that puts those in harm, then telling others how to replicate it would be a problem
- Rule #2: Make Others Aware
  - If it exists others will find it, hopefully not “bad guys first”
  - Difficult path to find, let alone follow

Scenario #1

- Traditional Vulnerability Found
  - Company is well established, Offers $500 Bounty on Vulnerabilities Found, Has PSIRT Team.
  - Disclosure Found Vulnerability to Company, not Publically.
  - Company asks for 2 Months to address problem, works with researcher to understand vulnerability.
  - Company Releases Patch to fix Vulnerability in 1.5 months.
- Easy Decisions, Good Results

Experience Counts

- Experienced companies have developed a process to handle vulnerabilities
  - Incident Response Teams to interact with outside security researchers
  - Internal researchers to verify reported issues
  - Rewards for reported vulnerabilities
- Fast turn-around addressing the issue publically
  - No need for partial disclosure, or non-disclosure options

Scenario #2

- Embedded Device Vulnerability Found
  - Company has no PSIRT, no previous history of Vulnerability Handling
  - Disclosure to the company could be risky, after advisement they could take legal action to bury the issue
  - Full Disclosure publically could put people at risk
  - Partial Disclosure invites criticism from all sides

Lack of Experience, Erratic Response

- Limited or no experience, so no idea how company will react.
- Companies have a lot of risk on the line (PR, Shareholders, Profits)
- Very Defensive, Usually lawyers take over.

Company A – The Bully

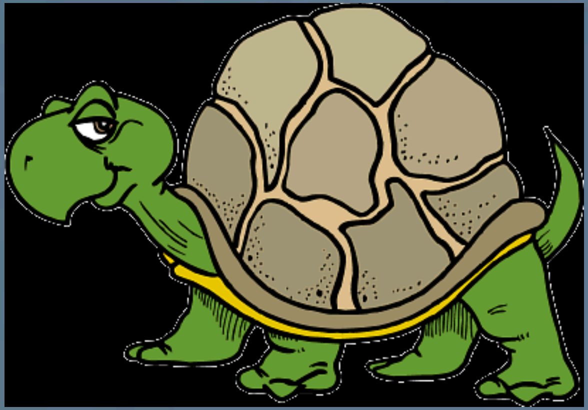
- Legal tactic of issuing a “Cease-and-desist” letters
  - Claims of violating copyright, false allegations, demands to take down materials, etc
- Researchers should seek out legal advice when/if they receive one
  - EFF is a great source of help

Company B - Hide

- Some companies will not return your calls, or anyone's calls on the issue
  - Very Frustrating, puts researcher in a disclosure bind
- Also, might issue public comments while never talking to you
  - Often, has bad information due to not talking with security researcher
  - Misleads customers, causes more problems

Company C - Sloooooooow

- Company responds, but is quite slow in all actions
  - Might ask for 1+ years to address vuln
  - Takes weeks/months to get back to researchers
- If public heath/welfare at risk, what is the ethical obligation?
  - Company might not be open to partial disclosure, or published work around
- Might be legitimate
  - Gov't regulations, Old systems
  - Be patient, communicate



How Security Researchers can help

- Seek out a trusted intermediary
  - ICS-CERT, DHS, US-CERT, INL
  - We need to develop more of these
    - SCADA has good coverage, Medical limited
- Increased Professionalism
  - Your visiting there trying to get their help
  - Can’t wear defcon 3 t-shirt and camo pants.
  - Listen to companies concerns, be flexible.

How Security Researchers Can Help

- Stress being on the good side
  - Show up with ideas on how to address issue
  - Share all of the findings
  - Avoid calling the baby ugly: it’s their baby, they will react poorly

How Companies Can Help

- Have a plan
  - Scenario Role play. Just like your Business Continuity plans
  - Be sure you have options, plan like you *will* have a vulnerability to address
- Don’t get cute re-inventing the wheel
  - Use standard, well tested methods. Don’t try and create your own key exchange and encryption system
  - Hiding behind obscurity will not help you

How Companies can help

- Create an IRT
  - Or at least a policy. Let Researchers know what to expect.
  - Publish a point of contact, and assure a response time, even if it’s long.
- Be Professional
  - Don’t call out work as being “garbage” or “obscure”
  - Listen to us, you don’t have to take our advice, but at least listen
- Professional Security Researchers are your friend
  - Most of us just want to make things better, not try and destroy you

You Can’t Always Get What You Want

- Some things can not be fixed
  - Crazy costs
  - Age
- Alternate Plans
  - Work Arounds
  - Containment
- Bury It
  - Worst Option, but in some cases needed
- Important to Communicate

End Users – New Players

- End users have had little personal impact on vulnerability disclosure
  - Web Servers, Email, etc: all contained in a virtual world
- New Class of Devices
  - People have higher degree of dependence on them
  - Needed in some cases to live or maintain civilized life

Kerri Sparling – SixUntilMe

Contact

- Jay Radcliffe
  - @jradcliffe02
  - jradcliffe@mocana.com
- Kerri Sparling
  - kerri@sixuntilme.com
  - @SixUntilMe