Getting to *Hey* --
A fresh look at establishing a security vulnerability reporting program

Cristina Serban, PhD, CISSP
AT&T Security Research Center
cserban@att.com

ACSAC WiP – December 8, 2011
AT&T Security Vulnerability Reporting Program

➢ To facilitate external reports coming to AT&T
To facilitate **external** reports coming to AT&T

- AT&T - one of the first major global carriers to start such a program
- Needed
  - a practical, effective and visible way to report security issues
    - in our services, products, infrastructure
  - for security researchers and the public at large
- Also helps
  - responsible disclosure
  - shorten the time to find out about security issues
Our Experiences

• Non-trivial decisions
• Socializing it
• What’s showing up at the door now?
Our Experiences: Non-trivial decisions

• Design decision: Accept reports via web or email?
  – Not a trivial matter after all
  – Web seems obvious choice, but is a lot harder to secure
  – Email sounds out of fashion, but lower complexity has advantages
    ➢ We went with email (to secure@att.com per RFC) for reporting, and website for describing the program www.att.com/reportvulnerability

• Tool decision: Which tool for PGP/GPG?
  – Many do not work correctly on some machines
  – Some have serious conflicts with full-disk encryption tools
  – Open source is not always the best way
    ➢ We went with a commercial tool
Our Experiences: Socializing it

• Once built, how to socialize the program?
• Website www.att.com/reportvulnerability describing program is linked off several highly visible corporate sites, well tagged, etc.
  • Need to check periodically the links are still in place
• Program announced to customers, partners

➤ It is non-trivial to get people to say “Hey, you might have a vulnerability!”
Our Experiences: What’s showing up at the door now?

• Volume of received reports – on the light side so far
  – Mostly – reports on phishing emails received by customers
    • We forward to Abuse Team
  – Occasionally – customer service issues
    • Forwarded to appropriate teams
  – Rarely – the strange report

• Several real vulnerabilities reported
  • Being worked on / resolved
Finally...

If you plan to start a vulnerability reporting program or would like to revamp an existing one:

- Research what everyone else is doing and how they are faring
- Allow plenty of time for design and implementation decisions – most likely, the “easy” decisions will take a lot longer than predicted
- Have a plan to socialize the program
- Keep checking your website, links and inbox are still alive
- Have metrics to track success of program

➤ At the end of the day, the real vulnerabilities that are reported make it all worthwhile
Thank you

Cristina Serban
AT&T Security Research Center
http://src.att.com