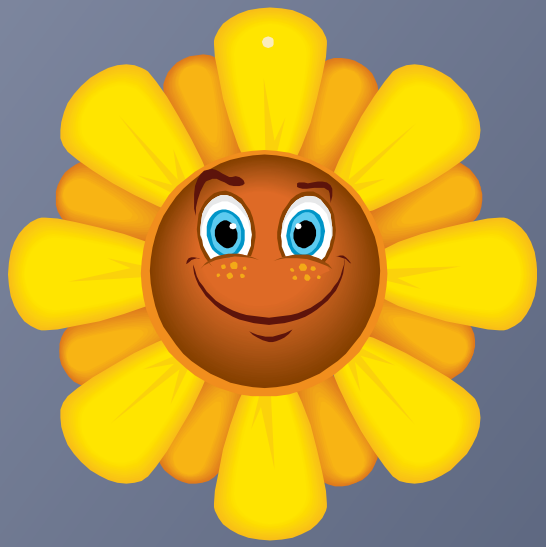


August IT Security Seminar

SUMMER 2009 SECURITY ROUNDUP

Carl Ness
IT Security Office

August 12, 2009

Today's Agenda

- Review some of the recent research from:
  - BlackHat 2009
  - DEFCON 2009
  - Things-that-didn't-make-it-to-a-con

- Security trends observed at UI

SSL Uh Oh Number 1

- X.509 Certificate Issuing
- MD-2 signed root certificates cryptographically feasible to attack
- 6 month window
- May be possible to generate a fraudulent SSL cert of any domain
- Possible to bypass smartcard auth

SSL Uh Oh Number 2

- Null characters inserted into certs can fool many SSL implementations
- Corrupts verification and trust chain
- Potential to confuse automated approval processes at CA

SSL Uh Oh Number 3

- Bypass system for checking for revoked SSL certs attack (OSCP)
- Requires a man-in-the-middle posture
- tryLater responses are generated
- Client skips OSCP checks
- Malware exists today

SSL Uh Oh Number 4

- EV certs susceptible to man-in-the-middle attacks:
  - Mixed content
  - Popups and page refreshes
  - SSL rebinding (switch between EV and non-EV connections) maintains appearance
  - SSL cache poisoning by modifying Last-Modified HTTP header, post-date non-EV content so that EV-cert isn't revalidated

SSL Implications

- How do we view trust?
- SSL libraries and client applications need to be updated
- Some are in progress, some will take time (end of the year)
- CAs are in motion
- Firefox patch issued
- EV practices being re-visited, including coding recommendations
- Bottom Line: Progress is being made

OS X: Not safe again

- Machiavelli rootkit for OS X
- Mostly proof-of-concept (read: not easy nor practical)
- Disguised as RPC subsystem
- Burrows into Mach kernel (OS X foundation) and installs local agent
- Bottom Line: As Mac install base grows, so will attack surface

Speaking of Apple…

- iPhone SMS vulnerability
  - Delivered by SMS
    - Create a malformed txt message
    - Add errors and send
    - Rinse and repeat
  - Creates a DoS condition (pwn-a-fone)
  - Jailbreaks the phone
  - Tracks location
  - Status: Fixed with a patch 24h later
  - PoC: WinMo & Android

Oh, and another thing…

- Ever seen an update on your WinMo "Windows Update?"
- Smartphone patches take months of QA
- Must pass through each manufacturer's approval process
- Must pass through QA cycle for 133 carriers
- Bottom Line: Epic FAIL

DEFCON Funny #1

- Between 2 and 5% of luggage just “disappears”
- Add in TSA “disappearing stuff”
- Plus TSA convicted eBaying employees
- Equals an interesting recommendation
  - Carry a firearm
  - You get to use your own lock
  - ☺

DNS....again

- DNSSEC (digitally signing DNS)
  - .gov is signed
    - US Government mandated 2009 completion
  - .edu “working on it”
- DNS-changing trojans
  - OS X especially vulnerable

Other Notable Research

- Rootkits designed to defeat forensics
- Video card GPU = supercomputer!
- Burrowing rogue VM guest agents
- MS OOB advisories (ATL/Visual Studio)
- It’s 10pm, do you know where your API is?
- Just how dumb are APs?
- DoS’n the FAA

Remember:
All is not lost!

DEFCON Funny #2

- Hey, look, an ATM…
  - at a hacker conference…
    - away from the cameras…
      - and I've never heard of this bank.
- What could possibly go wrong with this?

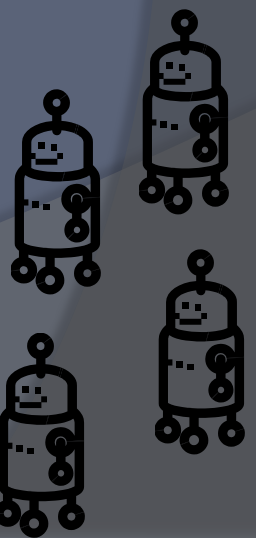
So….

University of Iowa Status Report

Top 5 Observed Attacks (and what to do about them)

1. Bots! (Flowbot/IRCbot)
2. SQL Injection
3. SSH brute force
4. OWA compromises
5. Thanks for all the phish

1. Update, update, update
2. Request a scan
3. Scope your services
4. Beware of inactive accounts, weak passwords
5. Education



Questions?

Thank you for coming!

IT Security Office
University of Iowa
security@uiowa.edu