TCIPG

ADVANCED ASSESSMENT PITFALLS

NOVEMBER 2013

TIM YARDLEY

UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

FUNDING SUPPORT PROVIDED BY DOE-OE AND DHS S&T

ADVANCED ASSESSMENT PITFALLS

- "Locked down" SSL
  - Client and server side certs
- Proprietary applications
  - No known public issues
- Proprietary protocols
  - What is this thing talking?
- Black boxes
  - How do you assess something that is dropped on your desk?
- Network appliances
  - A box on the network intended to do a specific function, likely not under the control of mgmt. Gold mine?
- Encryption
  - Harddrive? Communications? TPM? Let's see…
- Limited scoping/engagement
  - I can only do X, but need to do Y… how do I do this creatively through X?
- No access
  - Can't get anywhere?

ADVANCED ASSESSMENT APPROACHES

- "Locked down" SSL certs
  - Reverse the application that is being used
    - C#: reflector.net, etc.
      - Execute portions via mono or direct Visual Studio
    - Java: JAD, JD, etc.
      - Execute directly with jruby or jython
    - Scripts: Really?
    - Other: IDA Pro, OllyDbg, oSpy, etc.
      - Read and learn
  - Leverage stunnel once you have certs
- Proprietary applications
  - See above & poke and prod
  - Fuzzing
    - Bunny, skipfish, SPIKE, etc.

ADVANCED ASSESSMENT APPROACHES

- Proprietary protocols
  - Observation, Fuzzing
    - Peach, Sulley, zzuf, mangle, etc.
  - Proxying
    - Ratproxy, ZAP, arachni, etc.
  - Similar to looking at an application itself

ADVANCED ASSESSMENT APPROACHES

- Black boxes
  - Analyze traffic
  - Firmware available somewhere?
    - Yes?
      - Profit
    - No?
      - Does the device have a firmware update mechanism? If so, trigger it.
      - Can you extract it?
- Network appliances
  - See above
  - Often not patched as quickly (or at all due to product release cycle), so might have vulnerabilities present that the rest of the organization has long since patched

ADVANCED ASSESSMENT APPROACHES

- Encryption
  - Harddrive
    - Leverage older BIOS systems to clear it via hotswapping unprotected drive with protected drive
    - Steal it from memory via extended PCI interfaces (express card, firewire, thunderbolt, etc)
  - Filesystem
    - Password crackers
  - Communications
    - Scour for keys, see previous reversing discussion
  - Hardware
    - Hot boot a device and steal the RAM image
    - Take it apart and extract information
      - Remember, anything for storage may have latent footprints of what was there at some point

ADVANCED ASSESSMENT APPROACHES

- Limited scoping/engagement
  - Think outside of the box
    - What non-obvious item can be abused in a way that benefits you
      - Find a javascript inject, inject a javascript trojan that helps accomplish your goal
        - » And then wait for it to be triggered

ADVANCED ASSESSMENT APPROACHES

- No access
  - Search for WiFi (and crack it)
  - Deliver a package and plug your obscured device into an available ethernet port on the way
    - Ever see a computer that matches the faceplate of an ethernet jack? I've made one.
  - Drop a USB key, iPod, etc. in the doorway and make them have a special payload
  - Ship a trojan'd mouse to a secretary of someone important
  - Cause a disruption to result in a response action that benefits you
    - Fire alarm? Car alarms outside? Take over the video system and display a strange clip?
    - Network outage due to ARP related issue, MAC/IP conflict with internal router interface, etc.
  - Be someone else and know your targets
    - Social engineering
    - Social engagements (company parties, the local bar hotspot)
  - If allowed, steal the target device

HOW TO PROTECT YOUR SYSTEMS

- Pay attention to details
  - The lack of which is what attackers exploit
- Secure your physical access
- Be careful about what you say
- **ACTIVELY** monitor for changes on your infrastructure
- Patch widely and push your vendors to patch as well
  - You must know/determine details about those proprietary boxes in terms of external exposure
- Process!
  - Penetration is only part of the game, the process of how you address attacks (actively or post-event) is just as critical

SOME EXAMPLES

EMBEDDED DEVICE AUDIT

- Strengths
  - Strong architecture
  - Decent security deployed on central systems
  - Decent security precautions on edge devices
- Weaknesses (to explore)
  - Roll your own crypto
  - Process
  - Access control
  - Development environment

HARDWARE AUTHENTICATION TOKEN & CLIENT

- Strengths
  - Leverages standards
  - Relatively decent protocol and architecture model
- Weaknesses (OSX)
  - Encryption is a checkbox away from being disabled
  - Upgrade scripts call out to a web host to get updates and then process an update.sh on the system
  - Interfacing with applications is done via modifiable javascript
  - Software compiled with verbose debugging enabled, exposing (trivially) much of what the application does behind the curtain

QUESTIONS?