DEFCON 2010 #18 - Notes - SDH (DRAFT)

Friday, 6/30/2010

** DNS SECURITY **

Two speakers from: http://www.ics.org

Passive DNS sensors monitor UDP broadcasts

Threats: cache poisoning, spoofing

Research effort: Kaspureff

DNS Servers: Active vs. Passive

Current project is tracking nine key fields for transition analysis between what was requested and what was responded. Differences or anomalies probably mean there is a problem.

Tools: nsmg/dnsqr, dnsdb
- apache cassandra database
- collects massive amounts of data
- distributed
- DNSTLD dumps are part of the data
- dnsdb.ics.org

One application is to use the DB to see who might be claiming you as a DNS authority.

ICS.org is working on a distributed authoritative DNS policy service that will allow DNS owners to implement 'bad' domain list blocking and pass those changes via zone recursion throughout the DNS Internet landscape.

You could use the database to examine covert channels being captured. These are not ending up in the normalized database as they screw up the caches. The are ultimately blacklisted but research could be done in this area before blacklisting occurs.

** CLOUD COMPUTING **

Couldn't attend, the session was completely full.

** BROWSER IDENTIFICATION **

Research was via http://www.eff.org.

ZIP code + DOB + gender has a good chance of identifying most people in the U.S.

If there are 7 billion people in the world, then LOG2 means there is 31 bits of distinct data representation of each person.

Currently sites use many ways of tracking (and they are sharing info between each other in many cases): cookies, IP address, SuperCookies (Flash)

Fingerprinting is another technique that can be applied to the browser. Biggest issue is all browsers generate a browser ID (that can be modified but that in itself is a bit of data that helps with fingerprinting).

Current 8 measurements are being taking. Biggest impacts are JavaScript, Flash, Java, and Fonts.

Check out the project at: paropticlick.eff.com

There are probably other things that could be tracked: OS TCP/IP, ActiveX, Quartz timing (processor), JavaScript implementation specifics, CSS, etc...

Things that make things more obscure: NAT, IP Address, Cookie Blocking. Things to mitigate for more anonymity: user agent, plugins, and fonts.

Fingerprint does start drifting about about 4 days.

Other solutions to consider: No JavaScript (No Script plugin), Tor button plugin, NAT, use a clone fingerprint across many systems

Bad news is IP + footprint = 99% uniqueness. People are too predictable.

** IPV6 **

SPEAKER: Sam Browne, http://www.samsclass.info

Reviewed the differences between IPv4 and IPv6

There will be a growing number of IPv6 gateways for use at home. ISPs like Cox Cable are moving to IPv6 in the next two years.

Running dual-stack on hosts is the best.

You can hook IPv6 networks together using tunnels.

GoGo6 is a good IPv6 VPN solution.

ICMPv6 (no ARP) must be enabled.

Many security appliances are not compliant or ready to monitor bother IPv4 and IPv6 traffic.

There is a potential probably to worry about having a "ping-pong" router setup that effectively creates a massive self-DOS.

** FINGERPRINTING VIRTUAL MACHINES (VMS) **

SPEAKER: Nguyen Ann Quynh (Japanese)

Slide presentation was on a system that crashed and he had no other copy to give.

How do you do normal OS fingerprinting:
- send packets
- analyze return
- how do you do this with a system running multiple OS VMs?
- the host OS fuzzes the analysis and makes this hard
- VM file systems look different than hardware based file systems
- Host OSes sometimes require the VM systems to have specialized software
- analysis of hypervisor systems is also an approach to look into
- key focus of Quynh's research is memory analysis of VM and host OS
- another area of focus is on CPU context and differences

- his tool is still under development and should come out soon.

** INTERNET SURVEILLANCE SYSTEMS **

SPEAKER: Decius

What types of surveillance is built into the Internet today? Review the previous history:
- Clipper Chip
- CALEA
- IETF agrees to no wiretapping in protocols

End to end encryption is one of the ways to protect against surveillance but it isn't always available for all protocols, processes, applications, and services.

Cisco created an architecture for Lawful Intercept that is SNMPv3 based. It is known as the the TAP MIB. It is specific to only certain devices running specific IOS. It is based on a model of mediation of roles to devices. It has two layers of focus: user and context. It uses UDP packets to send out requests for services.

What do you want in a successful surveillance system:
- Not discoverable by the target
- Target can not manipulate the data collected
- Prevent unauthorized use

Issues with current systems: only username and password based, configurations can be enumerated, audit data is incomplete, little use of encryption

Look up "Athens Affair".

These systems for lawful intercept need to be on their own SNMP Mgmt VLANs or dedicated networks. They need to use SNMPv3 encryption.

** NMAP SCRIPTING **

Latest release Nmap.org Scripting Engine (DEFCON RELEASE v5.35DC18)

Write and share scripts for automate scripts for network ops (130+ scripts included in the new version)
- Categories
  - authorization
  - default
  - discovery
  - dos
  - exploit
  - external
  - fuzzer
  - safe
  - etc

New versions:
- HTTP methods
- scripts are really powerful

Test of SMB scripts of Microsoft.com —
- Target Ips for ARIN DB (1 million plus)
- nmap -T4 —top-ports 50 -sV -O -ossscan-limit etc ….
- found 75,000K hosts out of 1M Ips in about 26 hours (output file was a 1 million lines

long)
    - eed to block 135 and 445 at the perimeter

Scripts use “Lua” language:
    - used in nmap, wireshark, snort
    - also used in the game industry: World of Warcraft, Crysis
    - fast, parallel networking libraries
    - secure code base
    - interpreted
    - protocol/help libraries (DNS, HTTP, etc)
    - brute force forcers (password enumeration)
    - SSL support

Scenario:
    - you scan a network
    - get results
    - find a lot of rpc open on port 111
    - then run another scan on for rpc on the host
    - etc
    - Script makes this possible in a single command

Live demo: build a script to find a specific vendor webcam that is using a dynamic IP address

A lot of new features planned for the future: pre and post rules, ZenMap, etc.

Saturday, July 31, 2010

** SCADA **

SPEAKER: Jeremy Brown @ Tenable

These systems support many OSes (from very old to very new). Now most are Windows based. The architecture is client-server. There is a great deal of longevity in hardware (tens of years). Updates may require hardware upgrades which are costly ($).

In the past a SCADA system was air-gaped from other networks but that is no longer true. Many have Internet access. At a minimum they need to be protected by a proxy or a firewall/guard.

Tool called Sploitware targets SCADA systems. CANVAS (a tool like Metasploit) has some SCADA specific options. These can be used by traditional vulnerability assessments but also the bad guys can use them. Most of the exploits against SCADA start with creating a known user or system admin account and then a password for that account.

Nearly all the SCADA exploits are zero day vulnerabilities with no known patch or possible mitigation option. The are focused on buffer overflow, memory cracks, etc.

Other attacks may just focus on Remote Control Exploitation (RCE).

In the future these tools will be come more "auto pown".

** CREATING A CYBER ARMY FOR NK **

SPEAKER: Charlie Miller <http://securityevaluators.com>

Former NSA. Slides are key.

A couple of highlights:

Focus your team on building as many 0-day vulnerabilities as possible. The average life of a 0-day vulnerabilities is 348 days. One of the quickest fixes was 98 days.

You need to work about making attribution easy for you but hard for your adversaries.

** CYBERWAR AND CYBERCRIME OVERVIEW **

SPEAKER: IAN AMT <http://www.iamit.org>

Read the NORTHRUP GRUMAN report on China
<http://news.techworld.com/security/3204712/china-is-probably-hacking-and-spying-on-us-report-finds/>

Reviewed countries: US, RUSSIA, CHINA, ISRAEL, etc

Definitely need to check out the slides to get the whole story.

There is a cybercrime toolkit called Zeus that builds weaponized ammunication using a GUI. A recent build from Zeus passed 42 virus/malware/etc engines.

For CyberDefense: You need to block all ports but those that you need. SSL is always going to be a big problem.

Iranian Hacker Forum is doing “training” on the Internet openily targeting U.S. Instructure sites in wargaming.

Cloud computing is trending to a cyberwar platform that offers a lot of power, distrubtion, and increased attribution.

** CHINESE SECURITY **

SPEAKERS: TOR, Univ. of Michigan, VXRL research group

Main focus of this talk is about censorship in China via the Great Fire Wall (GTFW). What is happening: blocking, redirection of DNS, SMTP server capture, TCP [RSTs] when something goes wrong.

The QQ.exe application looks to remove/screw up/hide Messenger and other chat clients. It has direct monitoring by Chinese authorities. It also has automatic upgrades.

Censorship resistance: TOR (2000+ central nodes) and growing number of bridges (both private and public).

Network censorship is hard so expect the Chinese to continue to move down the path of creating client/host censorware. If you don't have the censorware application then you won't get network access.

There is a 1st generation censorware tool called Greendam that is effectively a rootkit and there is also a first generation anti-rootkit called Damburst that eliminates the features in Greendam.

** ELECTRONIC DOORS ACCESS CONTROL (EDAC) **

SPEAKER: Shawn Merdanger (sp?). More info: scm@hush.com

Review of the “S2 Security Netbox” EDAC – reserached issues and looked at countermeasures

Other companies: Honeywell

These EDACs are moving into convergence with IP being the primary network. Capabilities video, DVR, door access, HVAC, etc

Big issue is the conflict between IT Security and Facilities.

Research on S2 Security resulted in several reproducable errors. The focus on the work was on the network controller and those devices, not the HID embedded devices.

Want to do this?!? Make sure you read through all the publically available documents from the vendor. From this type of research, Shawn turned up a great deal of technical information: OS, database software.

Shawn used “Shodan” (online web database of systems) to show that S2 Secuirty devices were on the Internet directly not always behind firewalls, VPNs, VLANs, etc.

** PHYSICAL SECURITY: HOW TO DO IT RIGHT **

SPEAKER: A.P. Delchi

The talk was about how to physical secuirty correctly. Good review. Slides are recommended.

Methodology: Assignment, Assignment (High, Medium, Low), Arrangement, Approval, Action.

Coordination job (getting Action done): Management, Vendors, Builders, etc

** KANTANA **

Bootable USB distro of secuirty tools. Read the website for details.

Remember if you are a company you should review the licenses. The Kantana distro is not built with that in mind.

Tools were evaluated by many different factors including how well supported the tool is. But some times they decided to use tools like netcat which works just fine and hasn't been updated for years.

Currently beta testing version 2.0.

** SOHO ROUTER **

A good number of the traditional home routers is susceptible of a combination of a cross-site request forgery and DNS rebinding (ie. DNS load balancing/redundancy).

Routers have two interfaces: eth0 (external) and eth1 (internal). Most routers have Port 80 on eth1 accessible for mgmt. But these are also binded to eth0 but not accessible from the outside world via a FIREWALL rule that drops those packets. But there is a process of having an internal client connect out to the Internet, run a bad JavaScript, and then using server side TCP RST have the session controlled externally via the internal accesses.

Thirty routers tested, and 17 have the vulnerability. Even some of the third party OSes: dd-wrt.com, openwrt, pfsense have this problem.

Tool: Rebind (uses DNS, Web, Firewall + JavaScript)

Recommend that all rebind be turned off including IP, SOAP, UPnP

You can mitigate your own systems by checking your interface: bindings, firewall rules, routing tables, and DNS.

Consider moving from HTML to HTTPS or SSH for all mgmt.

More info: http://rebind.googlecode.com

** .NET HACK @ RUNTIME **

This collection of attacks uses "reflection" within the .NET framework.

It is not focused on the code but what is happening at runtime: access, structure, and tools related to .NET.

Tool: DOTNETASPLOIT (framework + payloads) that is working with METASPLOIT for initial access.

Demo: Visual Studio Exploit

Anatomy of an attack: process space, modify the runtime object, make GUI changes, and change behavior.

Recommend reviewing the slides. Demo modifying SQL Server Mgmt Console "OK button to change running .NET applications. They also had a demo that changed the logic of an application to defeat "registration" and "license code" dialog boxes.

There are some legitimate uses: 3rd party patches, custom defensive payloads, bug hunting, application mashups, etc.

Presenters also are writing a book: Managed Rootkits that should be out soon.

Sunday, August 1, 2010

** POWERSHELL **

SPEAKER: David Kennedy

Microsoft's PowerShell appears to be a great system admin tool and an even greater security tool that can be used post exploitation of a system.

Many of the things that you can do in PowerShell are not picked up by anti-virus or Host-based IDS (HIPS).

PowerShell can use the full .NET framework.

Tool to check out: PowerGUI

They are working on a PowerShell Exploitation Framework (PEF).

More information at: http://www.social-engineering.org, http://www.secmaniac.com

** BROWSER-BASED DEFENSES **

SPEAKER: X06d <james@bluenotch.com>

Browsers are very quirky. They have a lot of problems: extensions, FLASH, etc.

The goal of X06d is to protect from attacks and provide anonymity. It follows a SARS approach: Sanitize input; Anonymize (look like everyone else); Randomize behavior (create line noise); and Sanitize output.

"No Script" is a great tool but is not the whole picture.

Whitelisting is hard; blacklisting works pretty good.

Check out DEFCON#17 - "De-Anonymizing You"

Cookie privacy is another good solution - clear on both open and close.

History - Make your system use Alexia Top 500 list (randomize)

Fonts - Create a Snapshot (basic VM look) / Randomize font collection

Check out: Proxify & ProxyChains

Links: http://sourceforge.net/projects/x06d

Also look at Fiddler (http://www.fiddler2.com), Blitzleiter, Proxifier

** IPV6: NO LONGER OPTIONAL **

SPEAKER: JOHN CURRAN, ARIN President & CEO

ARIN: Whois
- IPV4 started in 1978, biggest growth cycle started in 1992
- IPV6 forecasted depletion between 2010 to 2017; came out in 1999.
- IPV6 (128-bits) solves the problem of running out of IPV4 (32-bits) addresses

IPV4: Currently only 6.25% is available; 13.67% is unallocated (as of June 2, 2010) with the growth rate being about 5% a year over the last couple of years. So, in 2011 sometime there will be no more available unless there is a re-purpose of the unused IPV4.

Bottom line:
- We are running out of IPV4 address space
- Ipv6 adoption rates need to increase
- Ipv6 is not backward compatible with IPV4 (it is as if IPV4 was a 7 digit phone that could dial no more than 7 digits but the IPV6 is a 21 digit phone system)
- You can maintain IPv4 and Ipv6 at the same time
- All public interfaces need IPV6

IPV6 transition plans and processes are about 5 years old and there are many options.

You can learn more at: www.arin.net, www.getipv6.info, www.teamarin.net

** IPV6@ARIN **

SPEAKER: Matt Ryanczak, Network Operations Manager

Started work in 2003 (WWW, DNS, FTP) – Sprint, Worldcom, etc

The first rollout (SPRINT) was on a T-1 circuit with a Linux router and a OpenBSD firewall.

The also ran it as a complete v6 network (no dual stack). They were worried about security issues.

Next rollout was WORLDCOM – used a Cisco 2800 router, same OpenBSD, also a T-1. Network was segregated from IPV4.

When WORLDCOM went away, EQUI6IX came online – 100-MB via OCCAID, Cisco Router, OpenBSD, included dual stack and less security controls (limited segregation), the added external WWW support

In 2008, NTT and INET (both access to the Internet) – 1000-MBs with CISCO ASR 1000 and Foundry Load Balancers, offered: DNS, WHOIS, dual stack (stand alone network though)

Working Brocade now (bought Foundry) for improved IPV6 load balancers.
The also create adhoc meeting networks using IPV6 at locations where working groups were meeting. This also included NAT-PT, CGN, NAT-lite, wireless. It helped also for training staff.

SECURITY:
1. There is a transition period with the need for highlighted focus (many unknowns)
2. There is some Ipv6 security features can be used for good and bad
3. multiple protocols = multiple policies

Things you need for Ipv6 (network mgmt) – ICMPv6 (vs. ARP), DHCPv6 [need to have the right Cisco IOS feature).

There are not very many specific known Ipv6.

Security Features:
- cross-platform host to host encryption
- Improved VPNs
- enhanced routing
- application layer security

Currently there is now NAT options between IPV6. Hard to hide networks?

The address naming info is hard, complex, it will great errors, etc.

The multiple stack issue can cause problems: access control lists, firewall rules, parity between applications is not the same, network appliances will have parity issues also

** BLUETOOTH HACKING **

SPEAKER: JP Dunning (.ronin), http://www.hackfromacave.com

More info: IEEE 802.15.1. A low power, short range communication technology. It creates an ad-hoc (piconet) connection.

There are over 1 billion devices with Bluetooth (in 2006).

A devices profile can be cloned and spoofed.

Tool: SpoofTooph works on discoverable devices - scan, random profile creation, maunal configuration, clone, auto clone (incognito) & hidden

If you are going to get a device for testing get a Class 1 scanner (100-ft).

There is a new Bluetooth Profile Project (MAC Address ranges, 1500 devices). There are other collection efforts looking for more info.

Tool: RedFrang (DEFCON17) looks to try to find devices that are undiscoverable.

Tip: Once you have two devices discovered you should turn both devices to undiscoverable mode. They will still pair but won't broadcast in the same way.

What is exposed by Bluetooth: first name, last name, location, device/model, nickname/handle.

Tool: pwntooth (tool suite) for collecting name, place, device, other information

Tool: vCardBlaster (target device, finds devices in range, can send pictures in VCards, effects most contact applications, can send 10,000 contacts if you want)

Tool: Blueper (file transfer tool that is great for DOS - hardware reset or super prompts that make the device unusable).
** SECURITY MEASUREMENTS AND ASSURING RELIABILITY THROUGH METRICS TECHNOLOGY (SMART) **

Researchers who didn't come but sent their grad student: Wayne Zage (wmzage@bsu.edu) and Dolores Zage (dmzage@bsu.edu)

S2ERC Metrics – NSF funded for industry and university cooperative (50+ researchers)

Started at Purdue University – focus was on software programming languages, software engineering, focus on “reliability”. The basic notations:

De – an external view of the design complexity
Di – an internal view of design complexity

Trying to find errors and problems.

Using some of the research, if applied they have found between 80-90% of problems.

The external model monitors the inflows and outflows plus executable code (ie. Module).

The internal model looks at your “central calls”, “data structure manipulations” and “input/output”. You can also add weights if you find one of the areas more important.

How do you take the Design Metrics and apply this to a Software Systems Engineering Process. Complex design = many security issues and potential attack vectors. These defects = % of security faults that can be exploited both internally and externally.

Evaluated Firefox, Apache, Drupal, Open Solaris, OpenSSH, etc. Link CVEs to software component areas and determine if the components had a propensity for issues. If true, then if you apply the model to the project you are working on then you'd know where there is a high probably if a problem.

Apache had 131 files and 15 vulnerabilities. They found 87% of the vulnerabilities in the modules where they were by running the model.

The report from the model gives you the top ten areas where you need to do additional bug finding. Also the system builds a XML representation of the code and give you the model + metrics.

Maybe we should do this to the .NET frameworks at work?

Other Items To R&D

Seccubas

"Wily Insider" by Matius Madoa, Jacob West

"Hardware Hack" by Dave King

"Multiplayer Metasploit" by Ryan Linn

"Web-servers we don't need" by Mike Baily

Kartogrpah

"Open Source Framework for Adv. IDS" by Mullen Pentney

"Social Media: Data Visualization" by The Suggmeister

Shodan