



Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

March 10, 2010



ISOAG March 2010 Agenda

- | | | |
|-------|--|------------------------------------|
| I. | Welcome & Opening Remarks | John Green, VITA |
| II. | TaoSecurity – The Way of Digital Security | Richard Bejtlich, General Electric |
| III. | Layer-2 Security – Keeping the Man Out of the Middle | Bob Baskette, VITA |
| IV. | Where Do You Want <i>Your Packet</i> To Go Today? | Eric Taylor, NG |
| V. | Security Best Practices | Bob Baskette, VITA |
| VI. | Partnership Update | Don Kendrick, VITA |
| VII. | 2010 General Assembly Update | John Green, VITA |
| VIII. | Upcoming Events & Other Business | John Green, VITA |



Please Note!! SEC 501.1 Change

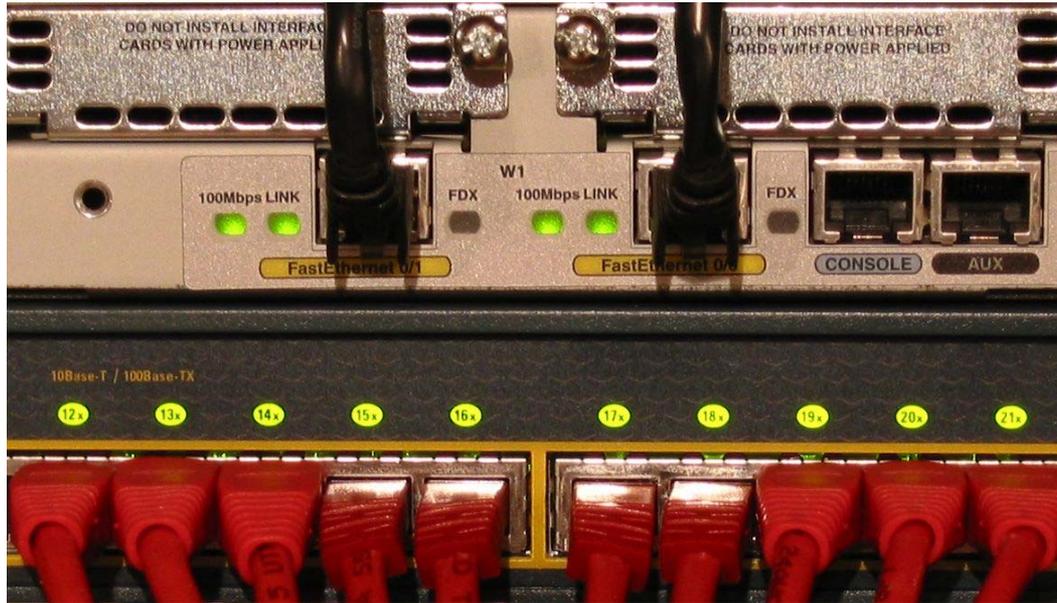
Effective **February 2, 2010,**

Section 5.3.2, # 8, page 29 –

“the requirement related to the frequency of changing user passwords for sensitive systems was changed from 42 days to 90 days to be consistent with current COV network password change frequency requirements.

Agencies may require users of sensitive systems to change their passwords on a more frequent basis.”

ISOAG

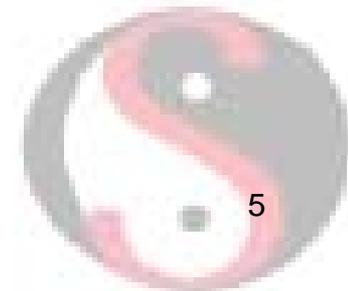
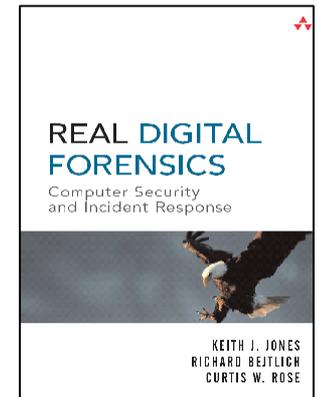
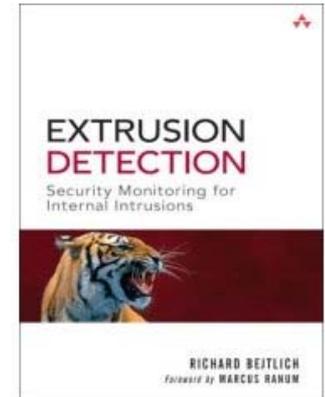
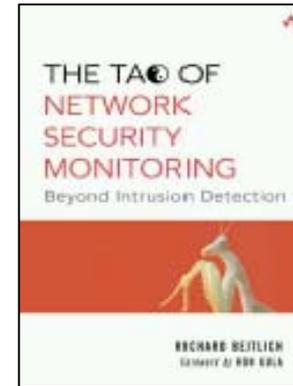


Richard Bejtlich
Director of Incident Response, General Electric
richard@taosecurity.com
taosecurity.blogspot.com



Introduction

- Bejtlich ("bate-lik") biography
 - General Electric, (07-present)
 - TaoSecurity (05-07)
 - ManTech (04-05)
 - Foundstone (02-04)
 - Ball Aerospace (01-02)
 - Captain at US Air Force CERT (98-01)
 - Lt at Air Intelligence Agency (97-98)
- Author
 - Tao of Network Security Monitoring: Beyond Intrusion Detection (solo, Addison-Wesley, Jul 04)
 - Extrusion Detection: Security Monitoring for Internal Intrusions (solo, Addison-Wesley, Nov 05)
 - Real Digital Forensics (co-author, Addison-Wesley, Sep 05)
 - Contributed to Incident Response, 2nd Ed and Hacking Exposed, 4th Ed
 - TaoSecurity Blog (<http://taosecurity.blogspot.com>)



Overview

- Still speaking Truth to Power
- Verizon Data Breach Report
- 7 Stages of Security Team Evolution and Cheap IT
- Defender's vs Intruder's Dilemmas
- Digital Situational Awareness
- Offense and Defense Inform Each Other



Bring them on! I prefer a straight fight to all this sneaking around.

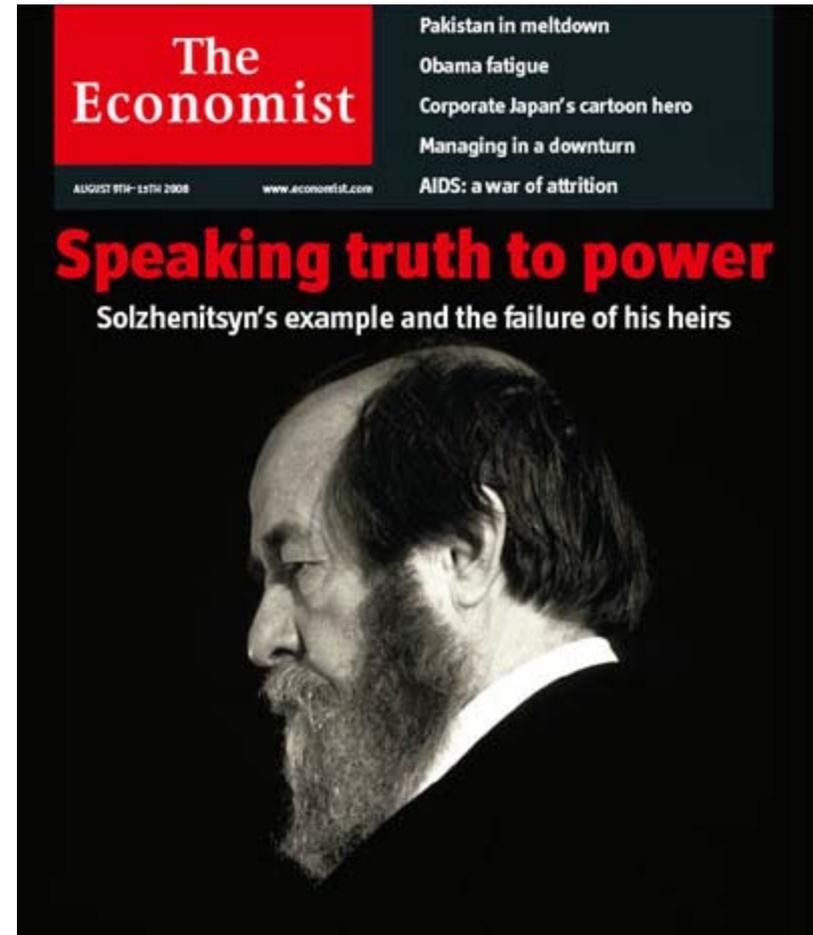
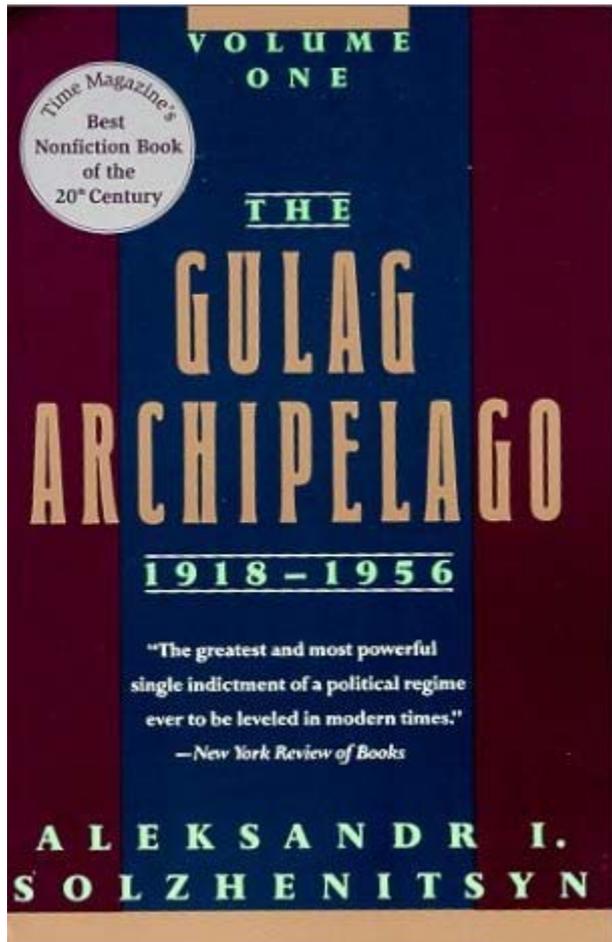
Han Solo, SWEPIV



Still Speaking Truth to Power

- Alexander Solzhenitsyn (1918-2008), author of The Gulag Archipelago: “Don’t lie! Don’t participate in lies! Don’t support a lie!”

Ref: 7 Aug 2008 *Economist* magazine

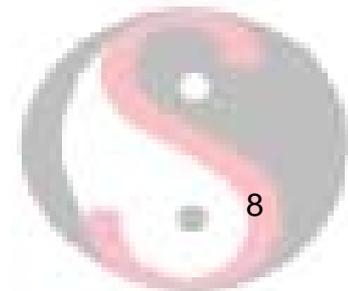
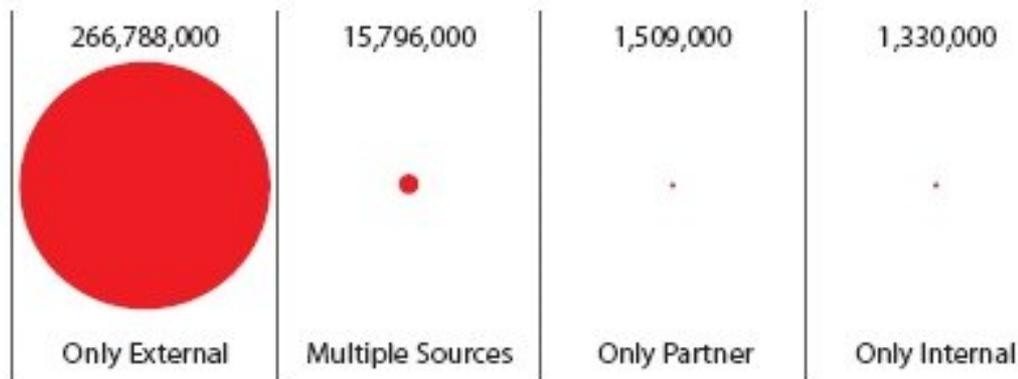


Highlights from 2009 Verizon Data Breach Report 1

Results from 600 incidents over five years make a strong case against the long-abiding and deeply held belief that insiders are behind most breaches.

Who is behind data breaches?	
74% resulted from external sources (+1%).	Closely resembling the stats from our 2008 report, most data breaches continue to originate from external sources. Though still a third of our sample, breaches linked to business partners fell for the first time in years. The median size of breaches caused by insiders is still the highest but the predominance of total records lost was attributed to outsiders. 91 percent of all compromised records were linked to organized criminal groups.
20% were caused by insiders (+2%).	
32% implicated business partners (-7%).	
39% involved multiple parties (+9%).	

Figure 8. Total records compromised by source



Highlights from 2009 Verizon Data Breach Report 2

Figure 6. Breach sources over time by percent of breaches

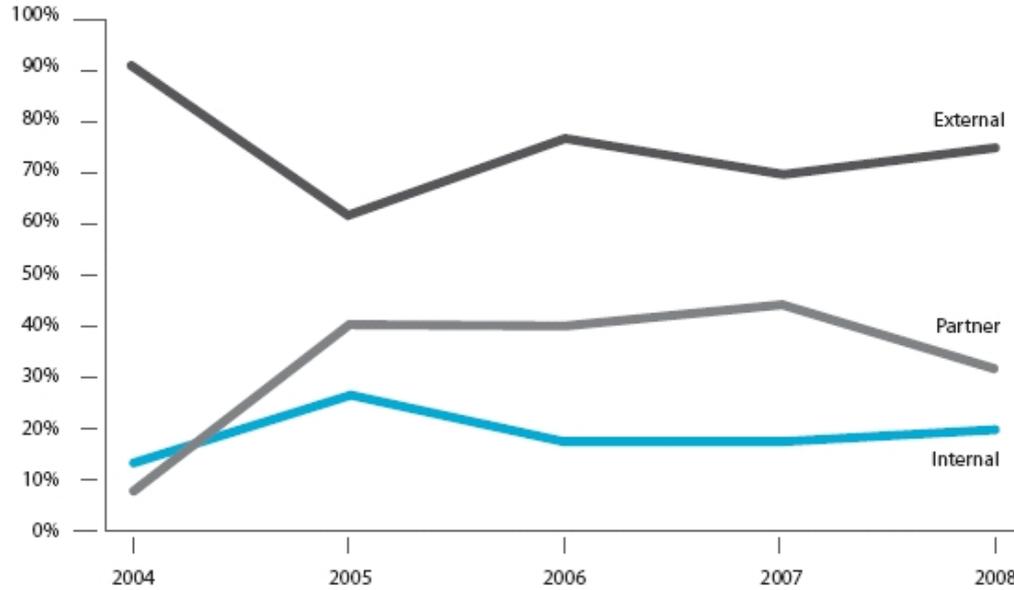


Figure 7. Median number of records compromised per breach

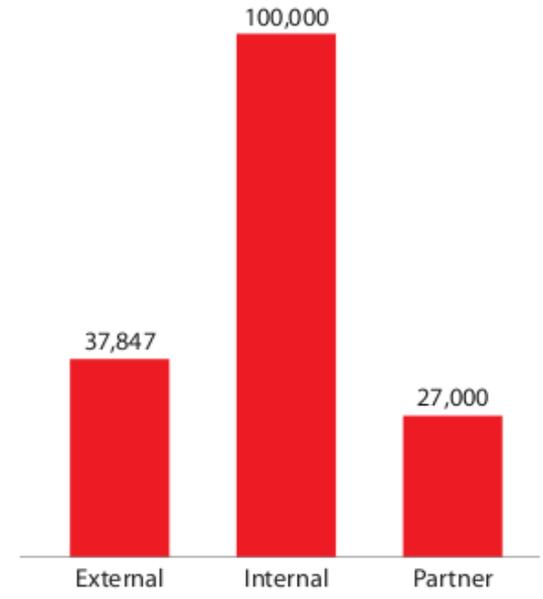


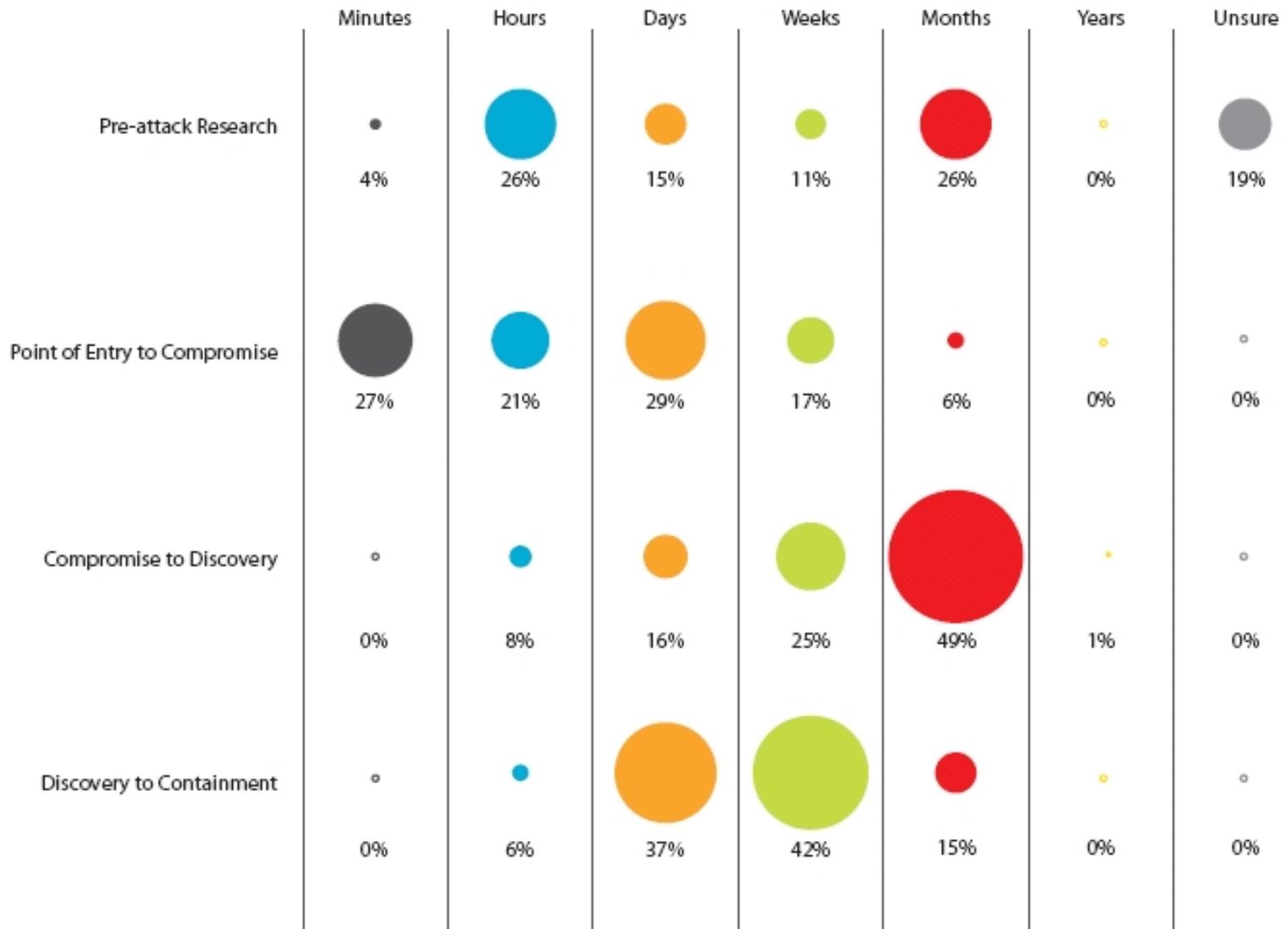
Table 1. Pseudo risk calculation

Source	Likelihood	Impact (number of records)	Risk (pseudo)
External	74%	37,847	28,175
Internal	20%	100,000	20,000
Partner	32%	27,000	8,700



Highlights from 2009 Verizon Data Breach Report 3

Figure 31. Time span of breach events by percent of breaches



Highlights from 2009 Verizon Data Breach Report 4

Figure 32. Breach discovery methods by percent of breaches

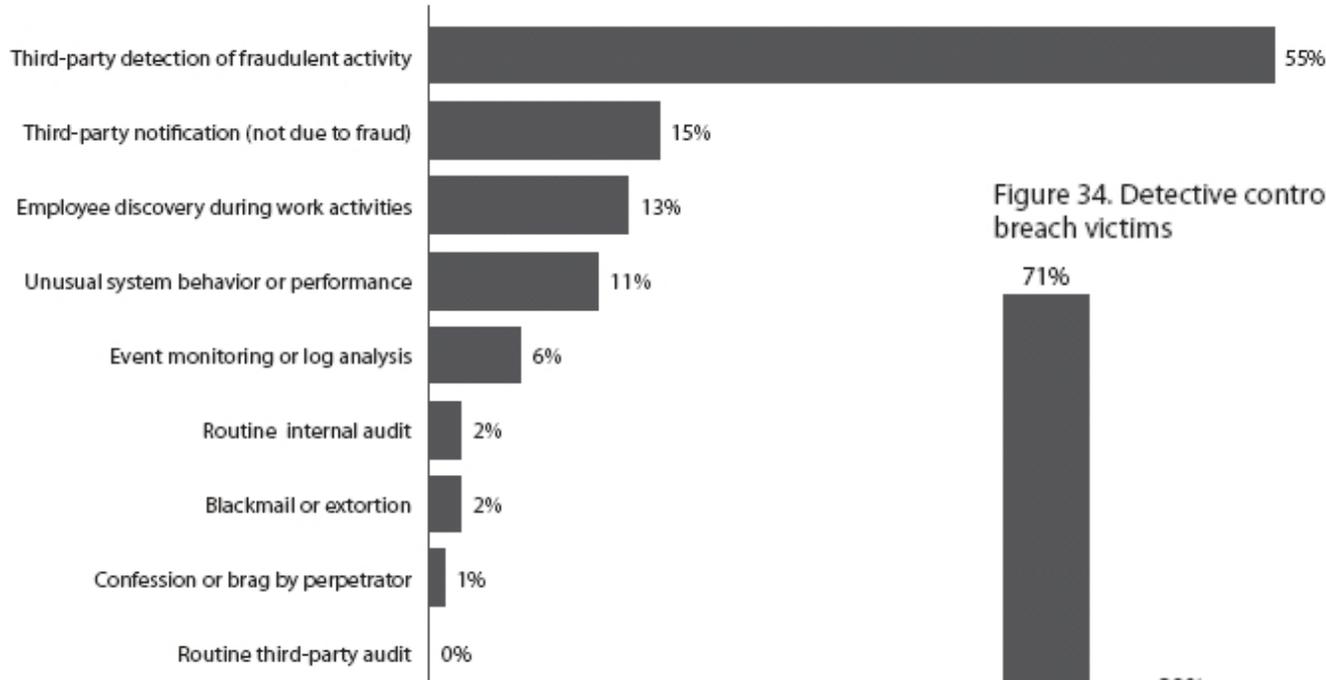
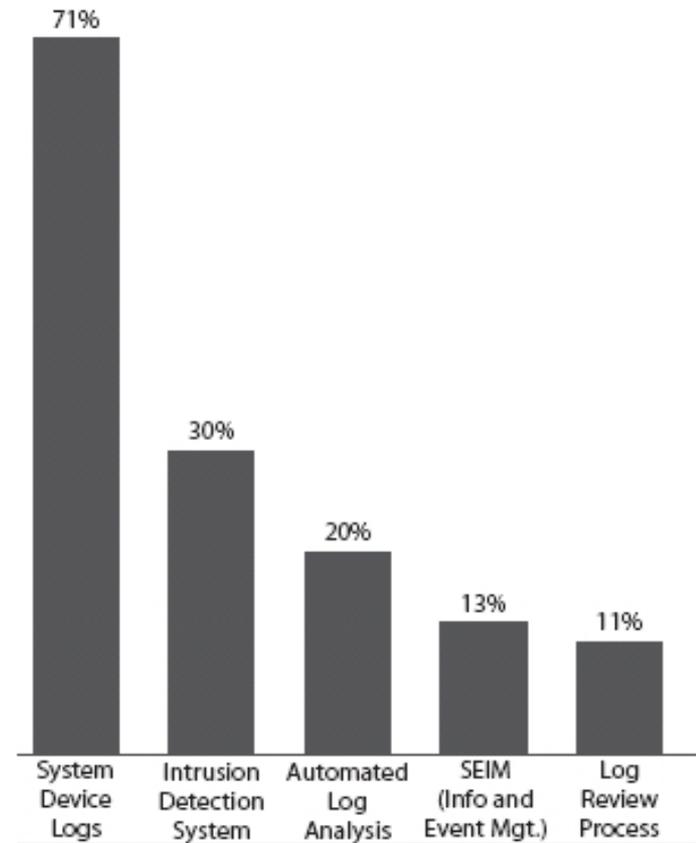


Figure 34. Detective controls by percent of breach victims



Highlights from 2009 Verizon Data Breach Report 5

Figure 35. Incident response practices by percent of breach victims

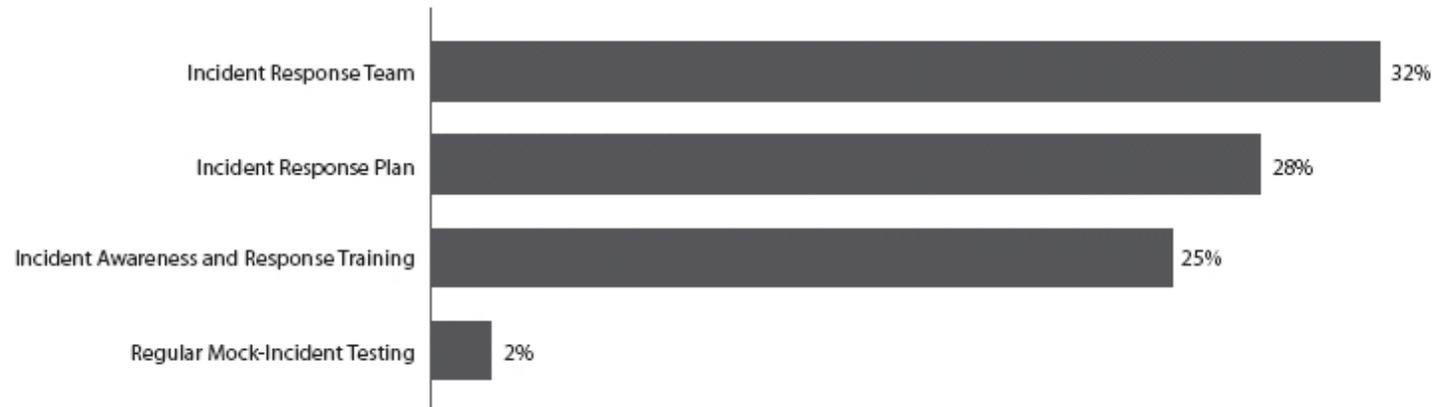
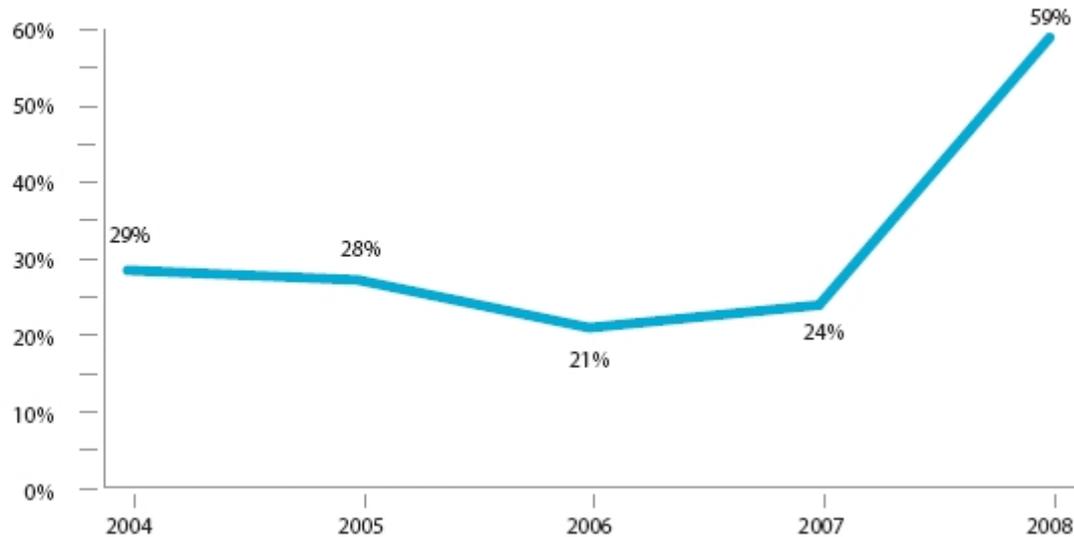


Figure 19. Malware customization by percent of breaches involving malware



Cheap IT Is Ultimately Expensive

- It is **not cheaper** to run legacy platforms, operating systems, and applications because "updates break things."
- It is **not cheaper** to delay patching because of "business impact."
- It is **not cheaper** to leave compromised systems operating within the enterprise because of the "productivity hit" taken when a system must be interrupted to enable security analysis.
- It is **not cheaper** to try to manually identify and remove individual elements of malware and other persistence mechanisms, rather than rebuild from the ground up (and apply proper updates and configuration improvements to resist future compromise).
- It is **not cheaper** to watch intellectual property escape the enterprise in order to prove that intruders are serious about stealing an organization's data.



7 Stages of Security Team Evolution

1. **Ignorance.** "Security problem? What security problem?"
2. **Denial.** "I hear others have security problems, but we don't."
3. **Incompetence.** "We have to do something!"
4. **Heroics.** "Stand back! I'll fix it!"
5. **Capitalization.** "Now I have some resources to address this problem."
6. **Institutionalization.** "Our organization is integrating our security measures into the overall business operations."
7. **Specialization.** "We're leveraging our unique expertise in X and Y to defend ourselves and contribute back to the security community."



Defender's Dilemma



The intruder only needs to exploit one of the victims in order to compromise the enterprise.



Intruder

Defender



Victims



Intruder's Dilemma



Intruder

The defender only needs to detect one of the indicators of the intruder's presence in order to initiate incident response within the enterprise.



Defender



Host security monitoring



Victims



```
D:\binaries\Volatility-1.3_Beta>python volatility -h
Error: Invalid module [-h].

Volatile Systems Volatility Framework v1.3
Copyright (C) 2007,2008 Volatile Systems
Copyright (C) 2007 Komoku, Inc.
This is free software; see the source for copying conditions.
There is NO warranty; not even for MERCHANTABILITY or FITNESS FOR A
PARTICULAR PURPOSE.

usage: volatility cmd [cmd_opts]

Run command cmd with options cmd_opts
For help on a specific command, run 'volatility cmd --help'
```

Live response and forensic analysis



Network security monitoring

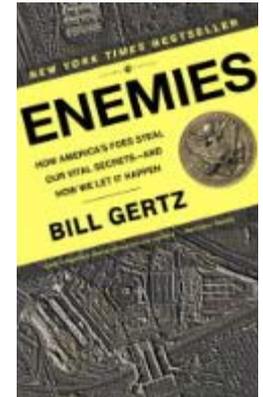


Enterprise log monitoring



Digital Situational Awareness Methods

- External notification
- Vulnerability assessment
- Adversary simulation or penetration testing
- Incident detection and response (3 paradigms)
 1. Detection is futile.
 2. Sufficient knowledge.
 3. Indicators plus retrospective security analysis.
- Counterintelligence operations
 - See who is selling or offering to sell your information or access to your information.
 - Solicit the underground for your organization's data or for access to your organization.
 - Penetrate adversary infrastructure.
 - Infiltrate the adversary group.
 - Pose as an individual underground member.



Offense and Defense Inform Each Other

Defense

- CIRT receipt of **external notification** reactively identifies problem not resisted or detected by proactive measures.
- **Blue Team** determines prevalence of vulnerabilities and exposures, helping Red Team determine level of effort required to penetrate target and nature of adversary to simulate.
- **Incident detection and response** collects and analyzes data on real intrusions, providing guidance to Red Team for improved adversary simulation.



Offense

- CIRT and/or law enforcement **counterintelligence** operations ascertain what the adversary knows about the target enterprise while learning adversary modus operandi.
- **Red Team** tests incident detection and response team's capability to discover and handle simulation intrusions.
- **Red Team** transforms theoretical intrusion scenarios into reality by exploiting vulnerabilities and exposures, helping Blue Team better prioritize findings.



Questions?

KNOW YOUR NETWORK BEFORE AN INTRUDER DOES

```
40.652146 10.145.15.100 -> 216.68.1.200 DNS Standard query A z3n.phatcamp.org
40.690278 10.142.1.89 -> 216.68.1.100 DNS Standard query A z3n.phatcamp.org
40.690291 10.142.1.89 -> 216.68.1.100 DNS Standard query A z3n.phatcamp.org
41.386313 10.145.15.98 -> 87.118.100.239 DNS Standard query A z3n.phatcamp.org
43.386117 10.145.15.100 -> 87.118.100.239 DNS Standard query A z3n.phatcamp.org
43.386248 10.145.15.100 -> 87.118.100.239 DNS Standard query A z3n.phatcamp.org
44.568156 10.142.1.97 -> 10.145.15.100 DNS Standard query A z3n.phatcamp.org
46.258206 10.142.1.89 -> 87.118.100.239 DNS Standard query A z3n.phatcamp.org
46.258210 10.142.1.89 -> 87.118.100.239 DNS Standard query A z3n.phatcamp.org
46.258292 10.142.1.89 -> 87.118.100.239 DNS Standard query A z3n.phatcamp.org
46.258306 10.142.1.89 -> 87.118.100.239 DNS Standard query A z3n.phatcamp.org
48.062938 10.142.1.97 -> 10.142.1.89 DNS Standard query A z3n.phatcamp.org
```

Richard Bejtlich

richard@taosecurity.com

taosecurity.blogspot.com



References

- <http://taosecurity.blogspot.com/2009/05/lessons-from-cdx.html>
- <http://taosecurity.blogspot.com/2009/05/highlights-from-2009-verizon-data.html>
- <http://taosecurity.blogspot.com/2009/05/cheap-it-is-ultimately-expensive.html>
- <http://taosecurity.blogspot.com/2009/05/defenders-dilemma-and-intruders-dilemma.html>
- <http://taosecurity.blogspot.com/2009/06/information-security-incident.html>
- <http://taosecurity.blogspot.com/2009/06/incident-detection-paradigms.html>
- <http://taosecurity.blogspot.com/2009/06/incident-phases-of-compromise.html>
- <http://taosecurity.blogspot.com/2009/06/offense-and-defense-inform-each-other.html>





Layer-2 Security: Keeping the Man out of the Middle

Bob Baskette
CISSP-ISSAP, CCNP/CCDP, RHCT
Commonwealth Security Architect

Data Networks or Seven-Layer Dip

- OSI = Open System Interconnection
- ISO = International Organization for Standardization
- Layer-1 and Layer-2 are implemented in hardware
- Layer-3 through Layer-7 are implemented in software
- Each layer has its own functions and interacts with the layer above and below
- Each layer communicates with the same layer on the other end

Application Layer

- Layer-7
- Identify and establish the availability of the intended communication peer
- Provides file transmission. Message exchange, terminal sessions
- Will check for available resources
- Applications access the Application layer via API
- HTTP, FTP, TFTP, LPD, SMTP, Telnet, SNMP



Presentation Layer

- Layer-6
- Presents data to the application layer
- Provides a common means of representing data in a structure that can be properly processed by the end system
- Put information from the Application layer into a format that all computers that follow the OSI model understand
- Concerned with the syntax and format of the data
- Functions as a translator, data compression, and encryption
- HTML, TIFF, JPEG, MIDI, GIF, ASCII, MPEG



Session Layer

- Layer-5
- Makes initial contact with the peer
- Responsible for establishing a connection between the two applications, maintaining it during the transfer of data, controlling release of connection
- Provides session restart and recovery
- Manages Session
- Modes are simplex(one-way), half-duplex, or full-duplex
- NFS, SQL, NetBIOS, RPC, SQL, H.323

Transport Layer

- Layer-4
- Segmenting upper-layer applications and establishing end-to-end connections
- Information sent as segments
- How to make the connection
- Host-to-host communications
- Provides reliable data transfers, error detection, error correction, error recovery, and flow-control
- Maintains end-to-end integrity
- TCP, UDP, RTP



Network Layer

- Layer-3
- Determines the best path, device addressing, packet fragmentation, location for connectionless protocols
- Handles routing of packets
- Message routing
- Error detection
- Control of node traffic
- IP, OSPF, ICMP, RIP



Data-Link Layer

- Layer-2
- Defines the protocol that the computer must follow in order to access the network
- Formats data and adds MAC address
- Flow control and error notification / focuses on reliability
- LLC sub-layer = manages and ensures communications between end devices
- MAC sub-layer = manages protocol access to the physical layer
- SLIP, PPP, ARP, RARP, L2F, Ethernet, FDDI, Token-Ring

Physical Layer

- Layer-1
- Bit ordering, bit transmission rates, connection types, is transmitted in binary
- Hex code converted to binary = RS232, V.35
- Defines the physical connection between the computer and the network
- Converts bits into voltages or light impulses
- Hardware/software drivers defined at this layer
- EIA/TIA-232 or 449, x.21, HSSI



Layer 2 Attack Considerations

- Layer-2 provides the functional and procedural means to transfer data among network entities with interoperability and interconnectivity to other layers
- Layer-2 attacks are difficult to achieve from outside the network
- Attacks must be conducted from within the network
- If layer-2 is compromised, other layers can be compromised
- Most attention is spent on Layer-3 with firewalls, IDS, and encryption technologies while Layer-4 and Layer-7 get application inspection

Layer-2 Attack Categories

- CAM Table flooding
- MAC Spoofing
- ARP Spoofing
- DHCP Starvation Attack
- VLAN hopping

CAM Table Overview

- Content Addressable Memory Table
- Storage locations that contain list of MAC addresses available on physical ports of the switch along with the associated VLAN parameters
- Similar to routing tables on a Layer 3 device
- All frames arriving on the switch are checked against the CAM table

CAM Table Overview

- If an entry is found corresponding to the destination MAC address of the frame the switch forwards the frame to the designated outgoing port
- If the destination MAC address is not found in the CAM table the switch forwards the frame out of every port, just like a hub
- Once the destination returns a frame the switch records the destinations MAC address in the CAM table

CAM Table Overflow

- Switches have finite memory storage and therefore the CAM table has a fixed allocated memory space
- Creates a vulnerability to sniffing by flooding the switch with a large number of randomly generated invalid source and destination MAC addresses to fill the CAM table so that no new entries can be accepted
- Will force the switch into Hub mode such that the switch will broadcast all received frames to all ports on the switch creating one big collision domain

CAM Table Overflow

- CAM table overflow attacks will only affect the local VLAN and the ports associated with the VLAN under attack
- DoS tools such as MACOF and DSNIFF can be used to perform MAC Flooding
- CAM table will eventually be purged by the switch as the older MAC Addresses are timed out

MAC Spoofing Attack

- Used to impersonate other devices in the network by convincing the switch that two ports have the same MAC address
- Different from ARP spoofing (switch is convinced that the MAC has moved through ARP cache poisoning)
- Switch will attempt to forward frames destined for the trusted host to the attacker
- Attacker crafts an Ethernet frame forging the source MAC address of the target host (victim)

MAC Spoofing Attack

- Switch will overwrite the valid value in the CAM table with the spoofed information (MAC to port mapping)
- Will create a tug-of-war between the targeted host and the attacker since the switch will update the CAM table each time either host sends a packet
- Could result in a DoS attack against the target and cause a performance impact on the switch
- The attacker may attempt to act as the default gateway



ARP Overview

- ARP is a Layer 2 protocol that is used by the IP protocol to map network addresses (32-bit IP addresses) to the hardware address (48-bit MAC)
- ARP provides IP-to-a-MAC resolutions
- ARP requests are broadcasts requests sent to all hosts on the network segment
- gARP messages are unsolicited ARP broadcasts containing the IP address and MAC address of a host
- gARP messages are used to announce the presence of a host to the network

ARP Spoofing Attack

- Attempts to disguise its source MAC address by impersonating another host on the network by poisoning the ARP Cache of other hosts
- Used for DoS and Man-in-the-Middle attack
- To perform a Man-in-the-Middle the attacker would send an ARP reply to the ARP request for the victim allowing the attacker to pose as the destination
- An attacker can also redirect traffic by sending gratuitous ARP messages
- An attacker would send the gARP message with the victim's IP-address and the attacker's MAC address
- gARP message will cause all receiving hosts and the local switch to update their ARP tables with the bogus entry

DHCP Process

- DHCP is a client/server architecture
- DHCP client collects DHCPOFFER messages over a period of time
- DHCP client selects one DHCPOFFER message from the incoming DHCPOFFER messages
- DHCP client extracts the server address from the server identifier option



DHCP Spoofing and Starvation Attacks

- Methods to exhaust the DHCP address pool on the DHCP server
- Attack works on MAC address spoofing by flooding a large number of DHCP requests with randomly generated spoofed MAC addresses to the target DHCP server
- After the attacker floods out the DHCP server, will introduce a rogue DHCP server to respond to client requests
- Will allow Man-in-the-Middle attacks
- Can also be used for a DoS Attack

VLAN Hopping Attack

- VLAN is a logical group of hosts that are created to limit the broadcast domain
- Inter-VLAN routing uses a Layer-3 device to allow a host in one VLAN to communicate with a host in another VLAN
- Method in which an attacker attempts to bypass a Layer-3 device to communicate from one VLAN to another for the purpose of compromising a device on another VLAN



VLAN Hopping attacks methods:

- **Switch Spoofing**

- Attacker impersonates a switch
- Must emulate either ISL or 802.1q signaling along with DTP signaling
- Attempts to become a member of all VLANs via a trunk port normally in Auto mode
- Once the trunk port is established can route traffic for multiple VLANS
- In multiple switch environments the trunk implementation can be exploited (by default are implicitly set to a native VLAN-ID = VLAN 1)
- Trunk ports have access to all VLANS by default unless pruning is configured
- If an access port (user) sends a packet encapsulated in an ISL or 802,1q format the packet will be forwarded to the distant switch if the packet is formatted with the native VLAN-ID

VLAN Hopping attacks methods:

- **Double tagging Attack**

- Also called Double Encapsulated VLAN Hopping Attack
- Tag the frame with two 802.1q headers to forward the frame to a different VLAN
- The embedded hidden 802.1q tag allows the frame to traverse a VLAN that the outer 802.1q tag did not specify
- Attack will work even if the trunk is set to off
- First switch to encounter the double-tossed frame strips off the first tag and forwards the frame
- Results in the frame being forwarded using the inner 802.1q tag out all switch ports including the trunk ports configured with the native VLAN-ID



Attack Tool Demonstration

- Break Time For Me
- Eric Taylor will now demonstrate how to attack Layer-2 Technology



MitM[®]

"Where do you want *your packet* to go today?" [™]

Eric Taylor

Northrop Grumman Enterprise Security Architect



NORTHROP GRUMMAN

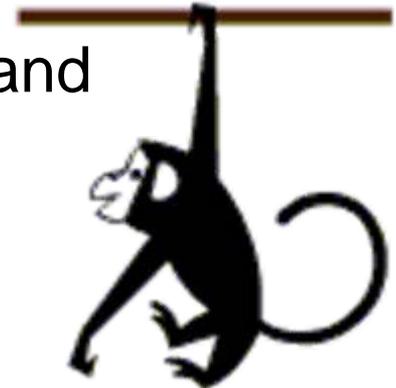
Toolz

- dsniff
 - <http://monkey.org/~dugsong/dsniff/>
- An oldie but a goodie
- Mostly mentioned here to give credit where credit is do
- Can still be useful...



Toolz

- dsniff
 - Passive
 - dsniff, filesnarf, mailsnarf, msgsnarf, urlsnarf, webspy
 - MitM
 - arpspoof, macof, dnsspoof, sshmitm and webmitm



Toolz

- Ettercap
 - <http://ettercap.sourceforge.net/>
- Powerful MitM framework
- Many, many features.
- Extensible with plug-ins and ettercap “filters” – stay tuned!
- Current development work??



Toolz

- Paros Proxy
 - <http://www.parosproxy.org/>
- Burp Suite
 - <http://www.portswigger.net/>
- Web application proxies with many desirable features for manipulating web traffic

Toolz

- IRS & Sterm
 - <http://www.oxid.it/>
- A powerful duo for exploiting IP-based trust and gaining access to systems with ACLs specifically designed to keep you out!
 - Can spoof telnet sessions on a switch

Toolz

- Cain & Abel
 - <http://www.oxid.it/>
- Deceptively easy – *oh so powerful!*
- Too many features to list.
- Stay tuned for Demo!



Toolz



- Metasploit
 - <http://www.metasploit.com/>
- Not a MitM tool per say but very helpful in this whole process.
- Some of the latest features in particular.
- MitM Framework modules anyone?

Toolz

- KARMA
 - <http://blog.trailofbits.com/karma/>
- Great for assisting you in attacking wireless clients.
- Features are included in Metasploit as of v3.2.

Toolz

- **tcpreplay** — edit and reply TCP packets
 - <http://tcpreplay.synfin.net/trac/>
- **nemesis** - network packet crafting and injection utility
 - <http://nemesis.sourceforge.net/>
- **scapy** - interactive packet manipulation program
 - <http://www.secdev.org/projects/scapy/>
- **sslstrip** — SSL man in the middle attack
 - <http://www.thoughtcrime.org/software/sslstrip/>

Toolz

- Hamster & Ferret - SideJacking
 - <http://erratasec.blogspot.com/>
- The Middler - protocol middling attacks
 - <http://www.inguardians.com/tools/>
- ISR-evilgrade– exploits updates (nasty)
 - <http://www.infobyte.com.ar/>

The Attacks and Demo

- Now for the fun stuff!
 - Credential Sniffing
 - **HTTP Using Windows Domain credentials**
 - LANMAN, NTLM, NTLMv2
 - Command Injection
 - `xterm–display [hackerIP]:0.0 &`
 - `iptables–F`
 - One-time password system over Telnet/HTTP
 - attacks on Cisco gear

The Attacks and Demo

- More of the fun stuff!
 - Re-Direction
 - **DNS Spoofing**
 - Breaking Crypto
 - SSHv1, **RDP**, PPTP
 - Downgrade attacks – NTLM to LM
 - Arbitrary Modification/Insertion
 - SMTP, **HTTP**, etc..
- Not theoretical! As you see, these all work today...

Back to Bob for Defenses....



Security Best Practices

Bob Baskette

CISSP-ISSAP, CCNP/CCDP, RHCT

Commonwealth Security Architect

CAM Table Overflow Attack Mitigation

- Configure Port Security
 - Can be enabled for static MAC addresses on a particular port or dynamic MAC addresses by specifying the number of MAC addresses that can be learned by a port
 - Can configure port violation when invalid source MAC address is detected (block the MAC or shutdown the port)

ARP Spoofing Attack Mitigation

- Configure the hold-down timers on the interface by specifying the duration of time for an ARP entry to stay in the ARP cache (not scalable to multiple devices)
- Can also use private VLANs to mitigate the attack
- Can enable Dynamic ARP Inspection



DCHP Attack Mitigation

- Enable Port Security to limit the number of MAC addresses on the switch port
- VLAN ACL can be used to prevent the rogue server from responding to DHCP requests
- Enable DHCP Snooping
- Filters untrusted DHCP messages by maintaining a DHCP snooping binding table

VLAN Hopping Attack Mitigation

- Explicitly turning off DTP on all access/user ports
- Disable all unused switch ports and placing the port into an unused VLAN
- To prevent double tagging ensure that the native VLAN-ID on all trunk ports is different from the native VLAN ID of the user ports
- Should use a dedicated VLAN-ID for all trunk ports
- Configure the native VLAN to tag all traffic



Dynamic Host Configuration Protocol Snooping

- Provides network protection from rogue DHCP servers
- Creates a logical firewall between untrusted hosts and DHCP servers
- Switch builds and maintains a DHCP snooping table called the DHCP binding database
- Switch uses the DHCP binding database table to identify and filter untrusted messages from the network
- DHCP binding database tracks the DHCP addresses that are assigned to ports as well as filtering DHCP messages from untrusted ports



Dynamic Host Configuration Protocol Snooping

- Untrusted packets received on untrusted ports are dropped if the source MAC does not match the MAC found in the binding table entry
- Can be configured for switches and VLANS
- On switches the interface acts as a Layer-2 bridge that will intercept and safeguard DHCP messages that traverse a Layer-2 VLAN
- On a VLAN, switch acts as a Layer 2 bridge within a VLAN domain
- For DHCP Snooping to function all DHCP servers must be connected to trusted ports



Dynamic ARP Inspection

- ARP attacks attempt to poison the ARP cache
- ARP poisoning normally uses gratuitous ARP
- To block ARP poisoning attacks the Layer-2 switch requires a mechanism to validate and ensure that only valid ARP requests and responses are forwarded
- DAI validates ARP packets in a network
- Determines the validity of packets by performing an IP-to-MAC address binding inspection stored in a trusted database such as the DHCP snooping binding database
- Will drop all ARP packets with invalid IP-to-MAC address bindings that fail the inspection
- Will only inspect the inbound packets



Dynamic ARP Inspection

- DAI safeguards the network from many man in-the-middle types attacks
- IP-ARP messages do not include an IP-header. Only includes:
 - Source MAC
 - Source IP-address
 - Destination MAC = field is empty
 - Destination IP-address
- Filtering criteria:
 - If ARP reply contains a source IP-address not assigned via DHCP to a device on that port drop the frame
 - For a received ARP reply, compares the source MAC address in Ethernet header to source MAC in ARP message. If they do not match drop the frame
 - For a received ARP reply, compares the destination MAC address in Ethernet header to destination MAC in ARP message. If they do not match drop the frame
 - Filters unexpected IP-addresses such as 0.0.0.0 255.255.255.255



IP Source Guard

- Security feature that restricts IP traffic on untrusted Layer-2 ports by filtering traffic based on the DHCP snooping binding database or manually configured IP source bindings
- Can prevent IP spoofing attacks when a host tries to spoof and use IP address of another host
- Any IP traffic coming into the interface with a source IP address other than that assigned will be filtered out on the untrusted Layer 2 port
- Should be enabled in combination with DHCP Snooping on untrusted Layer 2 interfaces
- IP source binding table learned by DHCP snooping or manually configured list = contains the IP address, MAC, and VLAN numbers
- Supported only on Layer-2 ports



Private VLAN

- PVLAN
- Provides Layer-2 solution to quarantine hosts from one another among ports within the same PVLAN
- Access ports in the PVLAN are allowed to communicate only with certain designated router ports (default gateway)
- Allows segregating traffic at Layer 2
- Transforms a broadcast segment into a non-broadcast multi-access like segment
- Allows the number of VLANS to be greatly reduced while still separating traffic



Private VLAN Port types

- **Promiscuous**
 - Can communicate with all interfaces including isolated and community ports within the PVLAN
 - Function is to move traffic between ports in community or isolated VLANS
 - Can use an ACL to identify what traffic can pass between the VLANS
 - Only one promiscuous port is allowed per single PVLAN
 - Serves all community and isolated VLANS in the PVLAN
- **Isolated**
 - Has complete Layer-2 segregation from ACL other ports within the same PVLAN, but not the promiscuous port
 - Traffic is only forwarded to the promiscuous port
- **Community**
 - Logically combined group of ports in a common community and can pass traffic among the other community ports and the promiscuous port
 - Ports are separated at Layer-2 from all other interfaces in other communities or isolated ports within the PVLAN



PVLAN Data Flow

- Primary VLAN
 - Carries traffic from a promiscuous port to isolated, community, or other promiscuous ports in the same primary VLAN
- Isolated VLAN
 - Carries traffic from isolated ports to a promiscuous/port traffic to any other port must be forwarded through the promiscuous port
- Community VLAN
 - Carries traffic between community ports within the same community VLAN and to promiscuous ports
 - Ports in the community VLAN can communicate at Layer-2 within the same community VLAN
 - Cannot communicate with ports in other community or isolated VLANS

Port Security

- Dynamic feature that prevents unauthorized access to a switch port
- Can be used to restrict input to an interface by identifying and limiting the MAC addresses of hosts that are allowed to access the port
- When configured, switch does not forward packets with the source MAC addresses outside the defined group of MACs



Port Security Implementation Methods

- **Static Secure MAC addresses**
 - Source MAC address
 - Manually configured using port-security mac-address <Mac> and stored in the MAC address table and in the configuration
- **Dynamic Secure MAC address**
 - Dynamically learned
 - Stored in the MAC address table not stored in the configuration
- **Sticky Secure MAC address**
 - Combination of Static and Dynamic methods
 - Can be learned dynamically or configured statically and are stored in both the MAC address table and in the configuration
 - Once stored in the configuration file, the switch does not need to relearn the MAC



Access Lists on Switches

- **Port-Based ACL**
- **VLAN ACL**
- **MAC ACL**



Port-Based ACL

- Similar to Router ACLs but are supported on the physical interfaces and configured on Layer 2 interfaces on a switch
- Provides only inbound traffic filtering
- Can use standard, extended, and MAC-extended access lists
- When applied to a trunk port the ACL filters traffic on all VLANS present on the trunk port
- When applied to a port with voice VLAN the ACL filters traffic on both the data and voice VLANS
- Can filter IP-traffic using IP access list and non-IP traffic using a MAC filtering list
- Not supported on Etherchannel interfaces



VLAN ACL

- VLAN map
- Provides packet filtering for all types of traffic that are bridged within a VLAN or routed into or out of the VLAN
- Not defined by a direction
- All packets entering the VLAN are checked against the VACL
- Processed in hardware so there is no performance penalty
- Wired-speed ACL



MAC ACL

- Ethernet ACL
- Can filter non-IP traffic on a VLAN and physical Layer-2 interface by using MAC addresses in a named MAC extended ACL
- Supports only inbound traffic filtering
- Several non-IP protocols are supported

Spanning Tree Protocol Features

- Spanning Tree Protocol resolves redundant topologies into loop-free, tree like topologies
- Used to improve the stability of Layer-2 networks

Dynamic Trunking Protocol

- Layer-2 protocol used to automate ISL and 802.1q trunk configurations between switches
- Supports auto negotiation of both ISL and 802.1q trunks
- Synchronizes the trunking mode on both sides of the link
- **DTP states:**
 - On
 - Off
 - Desirable
 - Auto (default mode)
 - Non-negotiate



Bridge Protocol Data Unit Guard

- BPDU
- Data messages exchanged between bridges using spanning tree protocol to detect loops in a network topology
- Contains management and control data information that is used to determine the root bridge and establish the port roles
- BPDU Guard is designed to keep the active topology predictable and enhance switch network reliability by enforcing the STP domain borders
- If BPDU are received, could indicate an error condition or the connection of an unauthorized device
- If triggered, BPDU Guard will put the interface in an error-disabled state

Loop Guard

- Provides an additional layer of protection against Layer-2 forwarding loops by preventing alternative or root ports from becoming designated ports because of a failure resulting in a Unidirectional link
- Should be enabled on all switches in the network
- By default spanning-tree does not send BPDUs on root or alternative ports

Root Guard

- Within Spanning-Tree any bridge in a network with a lower bridge ID can so assume the role of the root bridge
- A Layer-2 interface is set as the designated port
- Root Guard will prevent Spanning-Tree from converging incorrectly through a misconfiguration or malicious configuration
- Will put the interface receiving the false bridge ID into a blocked state (Root Inconsistent)
- Allows Spanning-Tree to select a new root switch



Layer-2 Security Best Practices

- Manage switches in a secure manner, use SSH, authentication mechanisms, access lists, privilege levels
- Restrict management access to the switch
- Always use a dedicated VLAN ID for All trunk ports
- Avoid using VLAN 1 for anything
- Disable DTP on all non-trunking access ports
- Deploy Port Security feature
- Use Private VLAN feature
- Use Hash-based authentication



Layer-2 Security Best Practices

- Disable CDP where possible
- Disable unused services and protocols
- Shutdown or disable all unused ports and place the ports into a VLAN not used for normal operations
- Use VLANs to separate logical components/workgroups
- Use a single IP-subnet per VLAN
- Enable BDPU Guard and Root Guard to prevent STP attacks
- Use DAI to prevent frame sniffing



Layer-2 Security Best Practices

- Use DHCP snooping and IP source guard to prevent DHCP DoS and Man-in-the-Middle attacks
- Use separate switches for each security level
- Restrict Layer-3 access to switch administrators
- Restrict trunking to specific ports. Use dedicated VLAN IP-addresses for trunks and trunk ports
- Use 802.1X user authentication (Next Month's Topic)



Questions???

For more information, please contact:
CommonwealthSecurity@VITA.Virginia.Gov

For more information on topics discussed in this
presentation:

Bob.Baskette@VITA.Virginia.GOV

Thank You!



Partnership Update

Don Kendrick
CNE, GCIA, CISSP
Senior Manager,
Security Operations Division



General Assembly Legislation Session 2010

John Green
Chief Information Security Officer





HB518

Freedom of Information Act; applicability; disclosure of criminal records; noncriminal incident information.

Clarifies that the Virginia Information Technologies Agency (VITA) is not the custodian of records stored or maintained by VITA on behalf of other state public bodies. Such records, however, shall be provided by VITA upon the request of any state public body for which VITA stores or maintains such agency's records in with FOIA. However, other records of VITA shall be public records and subject to FOIA. The bill also expands the exemption for criminal investigative files and clarifies that noncriminal incident materials held by any state or local law-enforcement agencies are exempt from the mandatory disclosure provisions of FOIA. ***Patron: Rust***

Status:

03/01/10 Senate: Passed Senate (40-Y 0-N)



HB 920

Computer Crimes Act; definition of computer and computer network.

Amends the definition of "computer" by adding cellular phones and other wireless telecommunications devices to the definition. The bill also clarifies that wired or wireless networks fall within the definition of "computer network." ***Patron: Bell***

Status:

02/03/10 House: Passed by in Science and Technology with letter by voice vote



HB1015

Secretary of Administration; telecommuting and alternative work schedules for state employees; effectiveness.

Provides that the Secretary of Administration, in cooperation with the Secretary of Technology, shall measure the effectiveness of the comprehensive statewide telecommuting and alternative work schedule policy. The bill provides that the head of each agency shall report annually to the Secretary on the status of any programs or policies developed and implemented pursuant to this section. Any agency head failing to comply with the requirements of this section shall forfeit one percent of the moneys appropriated for the operation of the agency as provided in the appropriation act. The Secretary shall so notify the Comptroller, who shall take such moneys and deposit them into the Literary Fund. The bill also requires the Department of Human Resource Management to notify state employees by email, or other method deemed appropriate by the Department, of the statewide telecommuting and alternative work schedule policy. *Patron: Hugo*

Status:

02/10/10 House: Continued to 2011 in Science and Technology by voice vote



HB1034

Information Technology governance in the Commonwealth; the Secretary of Technology; the Chief Information Officer; the Information Technology Investment Board; the Information Technology Investment Council, established.

The bill eliminates the Information Technology Investment Board (ITIB) and replaces it with the Information Technology Investment Council (ITIC), which is established as a policy council under the Governor with the power and duty to advise the Chief Information Officer (CIO) on: (i) development of all major information technology projects; (ii) strategies and standards regarding state agency use of information technology; and (iii) the development of enterprise applications, application budgets, and infrastructure expenditures. The ITIC also has the power and duty to approve the statewide four-year strategic plan developed by the CIO and approve statewide technical and data standards. The ITIC is composed of 10 agency representatives from each Cabinet Secretary, the Secretary of Technology, the CIO, the APA, and no more than two citizens, all to be appointed by the Governor. The Secretary of Technology serves as chair and the CIO as vice chair.

The bill requires the Secretary of Technology, in addition to existing duties, to develop criteria defining a "major information technology project" and, upon recommendation of the CIO, approve the procurement of such projects.

The bill grants the Governor the power to appoint the Chief Information Officer (CIO), who shall serve as the head of the Virginia Information Technologies Agency (VITA). The CIO reports to the Secretary of Technology and is responsible, through his role as head of VITA, for planning, developing, and procuring enterprise applications and infrastructure services. The CIO is also responsible for planning, developing, and soliciting contracts for major information technology projects. The CIO may enter such contracts only upon approval of the Secretary of Technology. The CIO may suspend a major information technology project but such project may only be terminated by the Secretary of Technology. The CIO appoints a Chief Applications Officer (CAO) subject to the approval of the Secretary of Technology. The CAO oversees, but the CIO approves, annual agency technology application budgets and expenditures.

This bill contains additional substantive changes to information technology governance in the Commonwealth as well as numerous technical changes. **Patron: Byron**

Status:

03/04/10 Senate: Signed by President



HB1035/SB236

Information Technology governance in the Commonwealth; the Chief Information Officer; the Information Technology Investment Board; the Department of Technology Management, established; the Information Technology Investment Council, established; and the Council on Technology Services, established.

The bill eliminates the Information Technology Investment Board (ITIB) and replaces it with the Information Technology Investment Council (ITIC), which is established as a policy council under the Governor with the power and duty to (i) approve the recommended technology investment projects report prepared by the Project Management Division; (ii) approve plans for the development, maintenance, and replacement of enterprise and multiagency applications developed by the Council on Technology Services (COTS); and (iii) advise the Secretary of Technology on the termination of major information technology projects. The ITIC is comprised of each Cabinet Secretary, the Directors of the Senate Finance and House Appropriations Committees, and three non-legislative citizen members, all of whom to be appointed by the Governor. The Governor's Chief of Staff serves on the ITIC as chairman.

The bill grants the Governor the power to appoint the Chief Information Officer (CIO), who shall serve as the head of the Virginia Information Technologies Agency (VITA). The CIO reports to the Secretary of Technology and is responsible, through his role as head of VITA, for planning, developing, and procuring enterprise applications and infrastructure services.

The bill establishes the Department of Technology (DTM) with the power and duty to (i) develop regulations, standards, policies, and guidelines for management of information technology in the Commonwealth; (ii) oversee information technology security, procurements, projects, investments, planning, and budgeting; (iii) report on information technology status and trends in the Commonwealth; and (iv) in consultation with VITA, identify and plan for the information technology needs of the Commonwealth. The Department is led by a Director who is appointed by the Governor, confirmed by the General Assembly, and reports to the CIO. The Department includes the Project Management Division, the Virginia Geographic Information Network, and the Public Safety Communications Division, all of which were previously under the supervision and responsibility of VITA.



HB1035/SB236 (con't)

The bill establishes the Council on Technology Services (COTS) as a policy council under the Governor with the power and duty to (i) advise the CIO on the application and infrastructure services provided by VITA; (ii) advise the Director of DTM on the development of information technology regulations, standards, policies, and guidelines; the list of recommended technology investment projects and proposed uses of state funds resulting from agency budget reviews; and (iii) develop, for approval by the ITIC, plans for the development, maintenance, and replacement of enterprise and multiagency applications. COTS is comprised of agency representatives from each of the Cabinet Secretaries and the legislative and judicial branches of state government.

The bill creates a new requirement that the Secretary of Technology develop a comprehensive statewide two-year strategic plan for information technology that addresses application and infrastructure needs, the use of information technology across state government, and information security issues. The Secretary is also responsible for the newly created DTM and shall coordinate and resolve any conflicts between DTM and VITA.

The bill contains several enactment clauses, including the provision that no additional funds from the general appropriation act passed by the 2010 Session of the General Assembly shall be used to implement the provisions of this act. Any additional funding necessary to implement the provisions of this act shall be provided from internal service funds maintained by VITA. This bill contains other substantive provisions and includes numerous technical changes necessary to update obsolete references. **Patron:** *Byron/Howell & Stosch*

Status:

02/03/10 House: Incorporated by Science and Technology (HB1034-Byron) by voice vote

03/04/10 House: Signed by Speaker



HB1039

Notification of breach of medical information.

Requires notification to residents of the Commonwealth if their unredacted or unencrypted medical information or insurance information is the subject of a database breach. The notification required by this section would apply only to entities not subject to federal medical information database breach notification regulations. ***Patron: Byron***

Status:

03/03/10 Senate: Signed by President



HB1144

State employee telecommuting and alternative work schedule goals.

Increases the target for eligible state employee participation in telecommuting and alternative work schedules to 40 percent in each respective program by January 1, 2012. ***Patron: Scott***

Status:

02/10/10 House: Continued to 2011 in Science and Technology by voice vote



HB1207

Computer trespass; penalty.

Expands the crime of computer trespass to include video and image capture software (screenshots) in addition to keyboard loggers. The provision does not apply to certain Internet, software, and hardware providers that provide network and data security services, technical assistance, or network management. The bill also authorizes recovery of damages in civil actions, including lost profits. ***Patron: Albo***

Status:

03/08/10 Senate: Continued to 2011 in Finance (12-Y 0-N)



HB1361

Computer and digital forensic services; exempt from regulation as a private security service business.

Exempts from regulation as a private security service business any individual engaged in (i) computer or digital forensic services or in the acquisition, review, or analysis of digital or computer-based information, whether for purposes of obtaining or furnishing information for evidentiary or other purposes or for providing expert testimony before a court or (ii) network or system vulnerability testing, including network scans and risk assessment and analysis of computers connected to a network. ***Patron: Keam***

Status:

02/10/10 House: Continued to 2011 in Courts of Justice by voice vote



SB242

Intellectual property created by state employees.

Adds new reporting requirements for agencies that seek patent protection or seek to license or transfer any interest in intellectual property developed by state employees. The bill also makes several technical changes to the requirements of the intellectual property policy developed by the Secretary of Administration. To accommodate the technical changes, the bill also extends the reporting deadline for the Secretary of Administration in developing a statewide policy and guidelines.

Patron: Watkins

Status:

03/03/10 House: Passed by in Science and Technology with letter by voice vote



SB332

Virginia School for the Deaf and the Blind; VITA exemption.

Exempts the Virginia School for the Deaf and the Blind from provisions related to the Virginia Information Technologies Agency. *Patron: Hanger*

Status:

02/10/10 Senate: Continued to 2011 in General Laws and Technology (15-Y 0-N)



SB390/SB480

Information Technology governance in the Commonwealth; Chief Information Officer and the Information Technology Investment Board; emergency.

Eliminates the Information Technology Investment Board. In its place, the Governor will appoint the Chief Information Officer of the Commonwealth, subject to confirmation by the General Assembly. The bill contains an emergency clause. ***Patron: McDougle/Howell & Stosch***

Status:

***02/10/10 Senate: Incorporated by General Laws and Technology
(SB236-Howell) (15-Y 0-N)***

***02/10/10 Senate: Incorporated by General Laws and Technology
(SB236-Howell) (15-Y 0-N)***

QUESTIONS?





Virginia Information Technologies Agency

Upcoming Events





Kids Safe Online Poster Contest

2010 Cyber Security Awareness *Kids Safe Online* Poster Contest

The Multi-State Information Sharing and Analysis Center (MS-ISAC) is conducting a national K through 12th grade poster contest. The goal of the contest is to encourage other young people to use the Internet safely and securely. All public, private or home schooled students in K through 12th grade are eligible to participate.

The top three winners from each state competition will be entered into the National competition. Entries received may be used in national, regional and state cyber and computer security awareness campaigns.

How to Enter:

Schools may submit entries to the Virginia state competition by emailing submissions to vita-access-training@vita.virginia.gov. (A parent may submit for home schooled students.) Please include the following information with your submittals: School, School Address, Teacher/Contact Person, Contact Phone Number, Student Name and Student Grade.

Virginia state submittals must be received by March 26, 2010. (Winners of the state contest will be automatically submitted to the National Contest by March 31, 2010.)

Entry Requirements:

Please see the MS-ISAC National Contest website for "Entry Requirements" and "Judging Criteria":
<http://www.msisac.org/awareness/poster2010/index.cfm>

For more information or questions, please email or call Nakita Albritton, Information Security Manager at vita-access-training@vita.virginia.gov or 804-416-6032.



Future ISOAG's

From 1:00 – 4:00 pm at CESC

(please let us know if you want to host in the Richmond area!)

Wednesday - April 22, 2010

Wednesday - May 12, 2010

Wednesday - June 16, 2010 - @ DMV!

(Thank you Norm Hill for coordinating this!)



Future IS Orientation Sessions

- | | | |
|-----------|-------------------|---------------------|
| Monday - | May 3, 2010 | 1:00 – 3:30 (CESC) |
| Tuesday - | July 6, 2010 | 1:00 – 3:30 (CESC) |
| Monday - | September 7, 2010 | 9:00 – 11:30 (CESC) |
| Monday - | November 1, 2010 | 1:00 – 3:30 (CESC) |



DHS/FEMA State Cyber Security Training Program

The Adaptive Cyber-Security Training Online (ACT-Online) courses are now available on the TEEEX Domestic Preparedness Campus. This training is designed to ensure that the privacy, reliability, and integrity of the information systems that power our global economy remain intact and secure.

Cost is Free!! And students earn a DHS/FEMA Certificate of Completion along with Continuing Education Units (CEU) at the completion of each course.

Registration is available at the host site:

<http://www.teexwmdcampus.com/index.k2?CFID=113796&CFTOKEN=92869629>

Thanks to Cameron Caffee, VDOT, for this information!



DSIA Training

Division of State Internal Audit Training: Introduction to IT Auditing

When: April 13 & 14, 2010

Where: James Monroe Building

PDS Room #1

101 N. 14th St, Richmond

Cost: \$380

Participants will earn 16 CPEs for taking the class.

Please register at:

<https://secure.doa.virginia.gov/hrtraining/login.cfm>



Information Security System Association

ISSA meets on the second Wednesday of every month

DATE: Wednesday, April 14, 2010

LOCATION: Maggiano's Little Italy, 11800 W. Broad St.,
#2204, Richmond/Short Pump Mall

TIME: 11:30 - 1:30pm. Presentation starts at 11:45 &
Lunch served at 12.

PRESENTATION: Database Security by Application Security Inc.

COST: ISSA Members: \$10 & Non-Members: \$20



MS-ISAC Webcast

National Webcast!

Wednesday, April 21, 2010, 2:00 to 3:00 p.m.

Topic: Cloud Computing

The National Webcast Initiative is a collaborative effort between government and the private sector to help strengthen our Nation's cyber readiness and resilience. A number of vendors have offered their services at no cost, to help develop and deliver the webcasts.

Register @: <http://www.msisac.org/webcast/>



UPCOMING EVENTS - CIO-CAO Mtg.

- **CIO-CAO Communications Meeting:**

Wednesday, March 24th

8:30 am – 9:00 am: Networking

9:00 am: Meeting start

Location: CESC



Identity Theft Red Flags Rules Extended Until June 1, 2010

The Red Flags Rule requires many businesses and organizations to implement a written Identify Theft Prevention Program designed to detect the warning signs – or “red flags” – of identity theft in their day-to-day operations.

At the request of members of Congress, the Federal Trade Commission is delaying enforcement of the “Red Flags” Rule until June 1, 2010. Read the FAQ at:

<http://www.ftc.gov/bcp/edu/microsites/redflagesrule/index.shtml>



Security Awareness Tools

For those of you here in Chester, we have Security Awareness Tools available for you!

Security Bookmarks!
Security Brochures!
Security Posters!
Duh's of Security DVD!

- All of these tools and many more can be downloaded from the toolkit website

<http://www.vita.virginia.gov/security/default.aspx?id=5146>



Any Other Business ???????



ADJOURN

THANK YOU FOR ATTENDING

