



Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

August 8, 2007



WELCOME to the AUGUST MEETING!





ISOAG August 2007 Agenda

- | | | |
|-------|---|--|
| I. | Welcome | Peggy Ward, VITA |
| II. | Security Awareness Months | Peggy Ward, VITA |
| III. | Security Operations Center | Don Kendrick, VITA |
| IV. | Computer Evidence Recovery Unit | Richard Seweryniak, VSP |
| V. | Threat Management Guideline | James Philput, VITA |
| VI. | IT Partnership Infrastructure Assurance | Benny Ambler, VITA &
Rodney Chisolm, NG |
| VII. | The State of Malware | Tripp Sims, VITA |
| VIII. | ISO Orientation | Peggy Ward, VITA |
| IX. | Upcoming Events | Peggy Ward, VITA |
| X. | Other Business | Peggy Ward, VITA |



Internet Safety Month: September

HOUSE JOINT RESOLUTION NO. 587

Designates September 2007 & each subsequent September as Internet Safety Month!



Cyber Security Awareness Month: OCTOBER

Governor Kaine has proclaimed October to be Cyber Security Awareness Month!

This is for all of the Commonwealth!

**Celebrate! Have an event! Give tips!
Hand out reminders!**



Security Operations Center

Don Kendrick

Senior Manager, Security Operations, Service Management Organization

August 8, 2007



NORTHROP GRUMMAN

Agenda

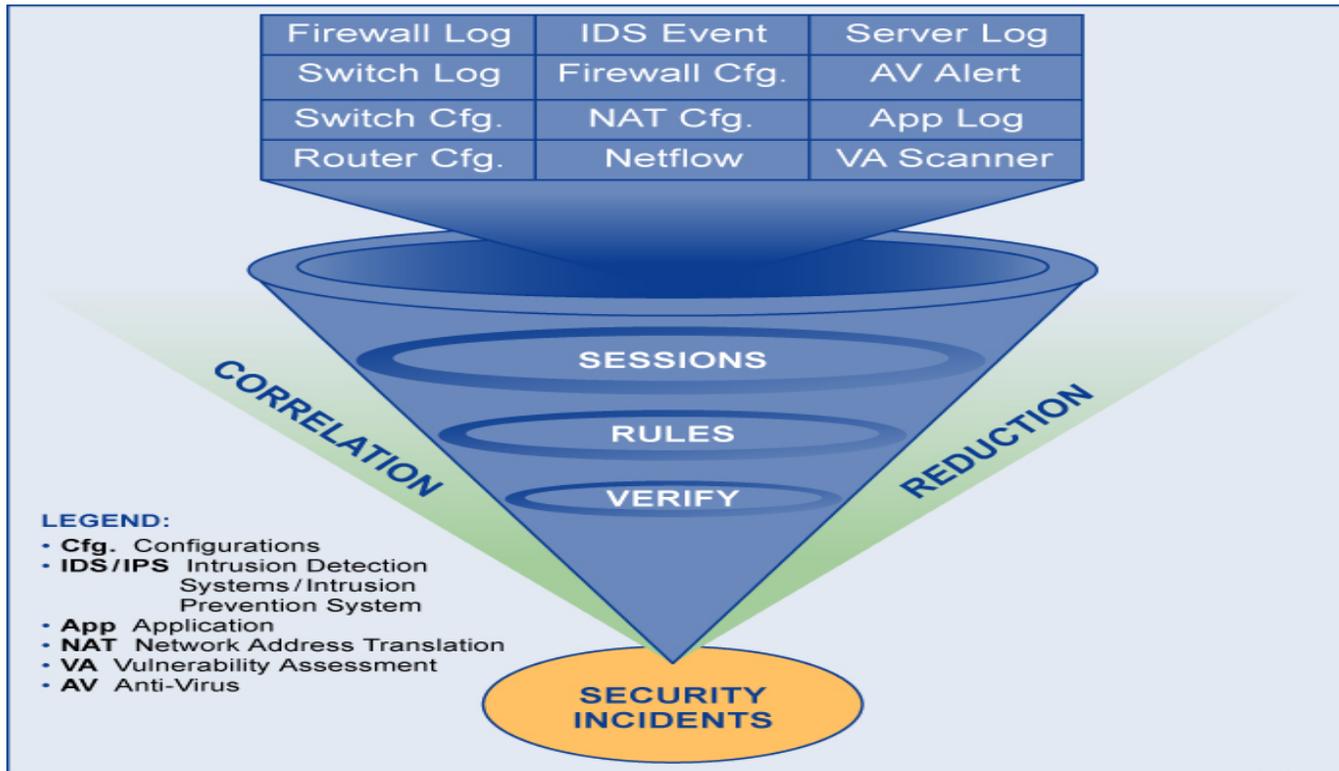
Centralized Logging

- Intellitactics

Coming Soon

- CSRIC
- Dashboard

Providing 24x7 Centralized Management and Monitoring Standardized Enterprise Security Protection (ESOC and TESOC)





Logging information flow in the overall security architecture

Intentionally left blank



After the transformation of forensic capabilities, CSIRC steps into action

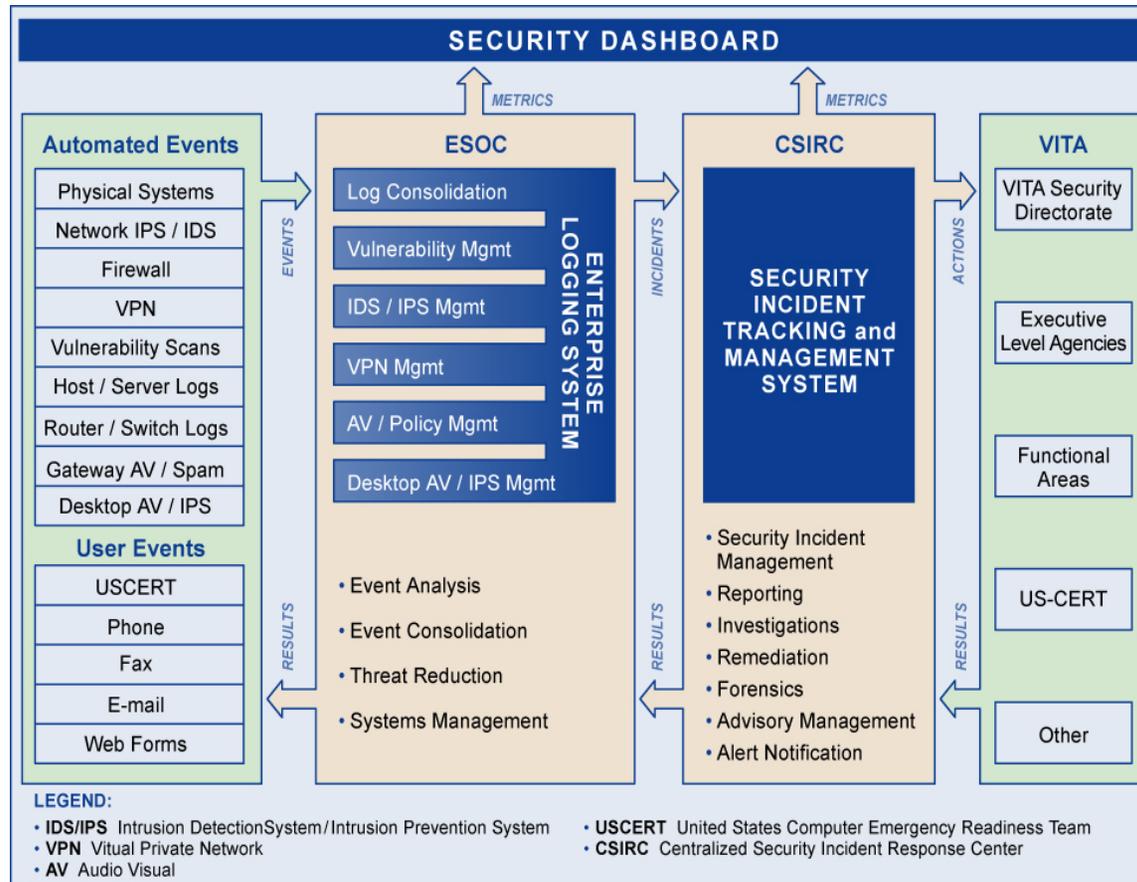
- **CSIRC handles all Agency and Enterprise forensics, including servers, laptops and desktops:**
 - Operations staff will secure evidence using newly developed procedures until CSIRC can assume control
- **CSIRC reports any results of an investigation to the following parties:**
 - Agency Information Security Officer
 - VITA Service Management Organization
 - VITA Security
- **Incident Monitoring and Tracking includes:**
 - The (T)ESOC monitors devices including server and firewall logs, Intrusion Prevention devices and host based IDS/IPS
 - Alert correlation and reviews occur 7x24x365 by Security personnel in (T)ESOC
- **Escalation:**
 - Suspected incidents identified by the SOC will escalate to CSIRC
 - CSIRC will validate incidents and assume control of management



A centralized and highly trained Incident Response Team provides immediate support and analysis

- Collocates with the Richmond Enterprise Solutions Center; responsible for all security incidents 24x7
- Helps VITA and executive branch agencies to comply with **Code of Virginia § 2.2-603.G**
- CSIRC staff responsibility includes keeping abreast of all advisories from industry, such as US-CERT, as well as investigating security incidents, focusing on sequence, the source and the time of events
- Reviews audit logs and reports and conducts forensic operations when necessary
- CSIRC staffing by dual-trained personnel with capabilities of operating both CSIRC and ESOC systems

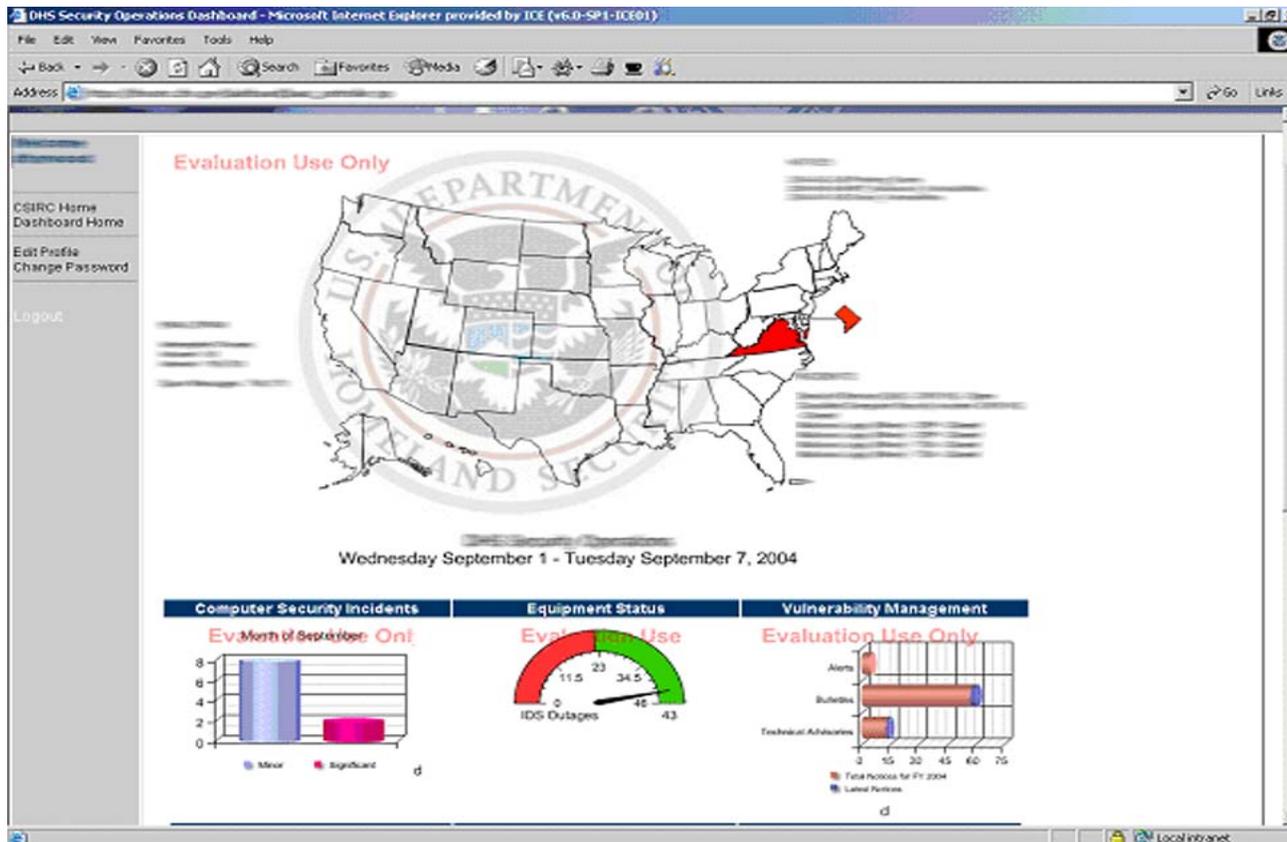
The Enterprise Security Dashboard Governance and Operational Control



VITA 026_r4

Sample
view

The Enterprise Security Dashboard Governance and Operational Control



Sample view

Questions?

Information Security Officers Meeting

Virginia State Police

Introduction



Mr. Richard Seweryniak
Digital Forensic Examiner

(804) 674-2593

richard.seweryniak@vsp.virginia.gov

Master of Science,
Information Technology
specializing in Information Assurance
University of Maryland

Introduction



Bureau of Criminal Investigation
Criminal Intelligence Division
Computer Evidence Recovery Unit

State Police Headquarters
7700 Midlothian Turnpike
Richmond VA, 23235

CERU

Computer Evidence Recovery Unit of the Virginia State Police provides assistance to local, state and federal law enforcement agencies with on-scene execution of search warrants for computer-related evidence, evidence recovery through forensic examination, and quarterly training classes in computer search and seizure.

CERU

- Investigate the crime or incident, not the technology
 - Network intrusion
 - Peer-to-peer networks
 - Concealed digital cameras
- Not a replacement for internal security
- CERU is “evidence recovery”

Other, national level

- Many agencies have their own digital forensics and incident response units
 - FBI field offices
 - Homeland Security
 - Department of Defense
 - Secret Service
 - National Ground Intelligence Center
 - ... and many others

HTCU, seven statewide

- High Tech Crime Units are located in each of 7 divisions with at least one high tech agent
- Considered “first responders”
- Investigators
- May assist local law enforcement

CERT, national level

Computer Emergency Response Team
Based at Carnegie Mellon University,
CERT is a federally funded research
and development center created in
response to an Internet worm that
spread in November 1988, crippling
about 10% of the existing Internet at
that time

Types of media examined



- Computers
 - hard drive
 - cd-rom media
 - dvd media
 - other storage media
- Servers (file, web, e-mail)
- Digital cameras
- Cell phones
- Blackberry and pda devices
- *USB drives*

Types not examined

- Items with no storage media
- Items that have been tampered which jeopardize the evidence – maintain proper chain of custody and forensic procedures!



When in doubt...

- Contact your nearest Virginia State Police High Tech Crime Unit for assistance from an experienced and trained special agent



Digital Artifacts

"Digital Artifacts" refer to evidence generated by computer and other electronic devices on storage media and can be retrieved for forensic examination

Digital Forensics

- Digital forensics differs greatly from biological or chemical forensic analysis
- Tests for DNA or drugs result in a yes or no response.
- Digital forensics involves much more data that includes, dates, times, locations, users, access permissions, physical data and logical data

Physical vs. Logical Data

- What's the difference?
- Physical data refers to the bits and bytes of the storage media, containing fragments of other data overwritten
- Logical data is the interpretation into usable format, such as an e-mail or document

Logical Data

- Logical data can be viewed by just about any computer user by opening an application such as Outlook or Word
- Copying logical files from one storage media to another will lose "RAM slack" and "file slack"

Physical Data

- Physical data contains much more information and is essential to investigations
- Who has permissions for files, when was it modified, trace evidence of a crime in files not completely overwritten
- Also traces of data not intended to be written to permanent files such as temporary files, "swap files", and "slack"

CERU stats, 2004

- In 2004, the CERU assisted with 89 investigations involving 3,946 gigabytes of data on 134 computers and 2,145 digital equipment items
- 54 of those investigations were conducted for federal, state and local law enforcement agencies in support of ongoing criminal investigations

CERU stats, 2006

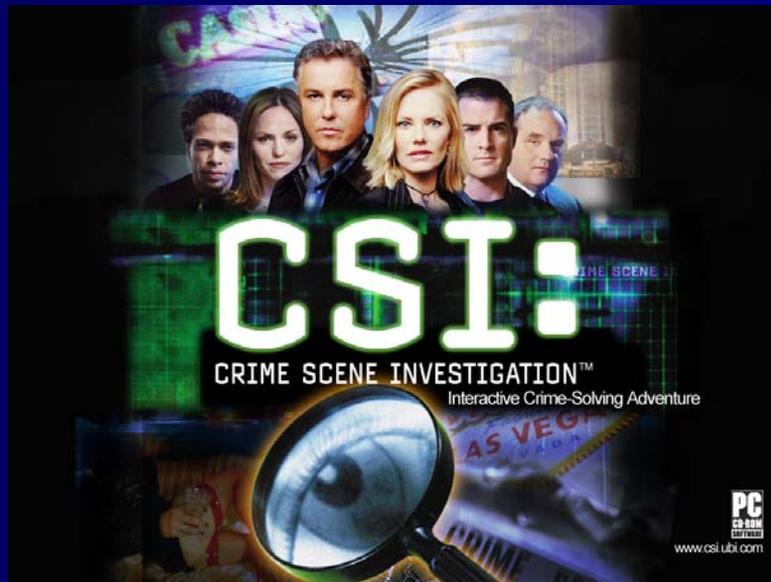
- In 2006, that number increased to 92 investigations involving 14,406 gigabytes of data on 130 computers and 1,224 digital equipment items
- This represents a shift from removable media such as cd-rom and floppy disks to larger capacity hard drives

Lots of ones and zeros!

- The number of examinations completed and the number of computers involved does not account for the complexity of each case
- Seven GB of data equals one 48' tractor trailer completely full of printed documents
- Last year alone, CERU processed the equivalent of more than 2000 tractor trailer loads full of data !



After these messages...



- CSI might be able to crack a case before the next commercial
- Real life takes an average of just over two weeks each and varies due to type of investigation and amount of data to examine
- Backlog is currently about 4-5 months for lower priority cases

Why so long?

- Digital evidence is examined thoroughly and acquired in a forensic manner which takes a very long time
- Must ensure that no data is overwritten or modified, booting Windows XP modifies literally hundreds of files just by "rebooting"
- Care must be taken to preserve the integrity of the data and all physical data is examined, not just the logical files, for the "needle in a haystack"

Preserving the data

- Take pictures, especially if the computer is on and applications are running
- Laptop computers: *remove battery*
- Desktop computers: *pull power plug*
- Servers: *do not shut down*
- Cellular devices: *protect from electronic signals*



Acquiring the data

- Bitwise copy, not a logical file copy
- Logical file copy would miss items in slack, files marked as deleted by operating system
- Bitwise grabs every one and zero
- Maintain a forensic environment to preserve integrity of the evidence
- Verify with MD5 hash calculations

MD5 uniqueness



- MD5 hash calculates a unique number for the media and will change if any one or zero is altered
- MD5 hash has a uniqueness value of 2^{128}
- That's 340 billion billion billion billion
- Many times more accurate than DNA analysis

Warrants

- Traditional item seizure of physical records took only documents mentioned
- Modern seizure of electronic records acquires all data on the storage media then limits the examination to items listed in the search warrant

Other Topics

- Legal considerations
- Protecting your data

Thank You!

Mr. Richard Seweryniak
Digital Forensic Examiner

(804) 674-2593

richard.seweryniak@vsp.virginia.gov

Bureau of Criminal Investigation
Criminal Intelligence Division
Computer Evidence Recovery Unit

State Police Headquarters
7700 Midlothian Turnpike
Richmond VA, 23235



Virginia Information Technologies Agency

IT Security Threat Management Guideline

James Philput

August 8, 2007





Introduction

- What is the IT Security Threat Management Guideline?
 - Existing Standards
 - IT Security Policy (ITRM Policy SEC500-02)
 - IT Security Standard (ITRM Standard SEC501-01)
 - IT Security Audit Standard (ITRM Standard SEC502-00)
 - Industry best practices
 - The SANS Institute
 - Security Mailing Lists
 - The Center for Internet Security
- Reduces impact of risks to an organization's IT systems and data

What Does the Guideline Cover?

- IT Security Threat Detection
 - Agency Responsibilities
 - Service Provider Responsibilities
- IT Security Incident Management
 - Risk categorization
 - Resource allocation
 - Response
- IT Security Logging and Monitoring
 - Log system design
 - Monitoring system design



IT Threat Detection

- Responsibilities for Oversight of Threat Management Program
 - Each Agency must designate an individual responsible for the agency's threat detection plan
 - May be agency staff or service provider
 - Responsibilities include:
 - Planning
 - Development
 - Implementation
 - Training
 - Maintenance

IT Threat Detection (Continued)

- Intrusion Detection Systems
 - Signature Based
 - Flexible and Easy to Update
 - If there is no signature there is no alert
 - Anomaly Based
 - Easy to keep up to date
 - Little flexibility in user defined settings
- Intrusion Prevention Systems
 - In-Line
 - Monitors single machine or ingress/egress point
 - Tap or Span
 - Monitors an entire switch or VLAN



IT Security Incident Management

- Define Roles and Responsibilities
 - CIRT Team Composition
 - Technical and Non-Technical
 - Incident Handling Training
- Set Priorities
 - Customer Data vs. Office Supply Ordering Data
- Categorize Incidents
 - Low to High
 - Virus Alert to Unauthorized Network Access
- Determine Appropriate Response
 - Virus Cleaning Tools
 - Contact Law Enforcement



IT Security Incident Management (Con't)

- Establish a Reporting Process
 - Internal
 - External
- Determine Reporting Requirements
 - Incidents must be reported to VITA within 24 hours (<http://www.vita.virginia.gov/security/default.aspx?id=317>)
 - Does Law Enforcement Need to be Involved?
 - Do Customers need to be Notified?
- Establish Evidence Collection and Examination Procedures
 - Maintain Evidence Integrity
 - Chain of Custody



Incident Management - Examples

- Virus Attacks (unable to clean, rename or delete)
 - remove affected machines from the network and restage
- Denial of Service Attack (DOS) – implement router or firewall changes to mitigate, require assistance from upstream network provider
- Internal threats (espionage) – contact HR and Legal, begin monitoring of user's traffic



IT Security Logging and Monitoring

- Log Monitor Design
 - Determine What to Collect
 - Determine Where it Should be Stored
- Event Correlation
 - Analysis Tools
 - Alert Systems



Useful Forms - Appendix

- Recording and Reporting Procedure
- Internal Incident Handling Procedure
- Computer Incident Reporting Form
- Chain of Custody Form



Questions?

Questions?



Virginia Information Technologies Agency

Information Security Infrastructure Assurance Plan

Benny Ambler, VITA
Rodney Chisolm, NG

August 8, 2007



Assurance of Infrastructure Security

- VITA is Responsible for IT Infrastructure supporting customer agency business
- Goals:
 - Keep as secure as when “inherited”
 - Improve where possible
- Customer agencies need assurance regarding the information security controls over this Infrastructure



Assurance of Infrastructure Security

- Data collected and analyzed included:
 - VITA IT Partnership SEC501-01 “Self Assessment” and the accompanying matrix provided late June for ISO information only, no action required!
 - Commonwealth Security’s Assessment of IT Infrastructure reported practices, policies and procedures
 - APA recent reports



Assurance of Infrastructure Security

- Future data sources for annual assessments:
 - SAS 70 Type II
 - IT Security Audits
 - Vulnerability scans
- Not included in current assessment due to timing



Assurance of Infrastructure Security

- IT Security domains assessed:
 - IT Contingency Planning
 - IT System Security
 - Logical Access Controls
 - Data Protection
 - Facilities Security
 - Personnel Security
 - IT Threat Management
 - IT Asset Management



1st Assurance of IT Infrastructure Security

- High Level Summary “Report Card” for agency heads based on the number of negative attributes relative to total attributes in the security domain:
 - None – 0
 - Few – >0% - 33%
 - Some – >33% - 66%
 - Many – >66%



Assurance of Infrastructure Security

- Letter of Assurance for each agency
 - will explain the assurance process
 - will provide rating per security domain
 - will be sent to the Agency Head
 - ISO and AITR will be copied
- Notice in the Leadership Communiqué



Assurance of Infrastructure Security

- Remediation of Vulnerabilities:
 - IT Partnership working on a remediation plan with specific vulnerabilities
 - Some remediation actions:
 - may be quick and easy
 - may take longer - pending transformation
 - may necessitate an agency requested IT Security Exception

SEC 501.01 Risk Remediation

Rodney Chisolm, NG

SEC 501.01 Risk Remediation

Purpose:

COV ITRM Standard SEC501-01; required all COV Agencies and their respective service provider (Northrop Grumman) to document current security practices no later than July 1, 2007.

Self assessments were completed by partnership staff at the agencies to determine whether or not they were compliant with the documented security practices.

Developing remediation plans relative to risks identified with Agencies Non-Compliant with SEC501.01 Security Practices and VITA technical compliance survey.

SEC 501.01 Risk Remediation

- Partnership Plan & Status:
 - √ Complete a Risk-Ranking of each SEC501.01 and VITA technical compliance survey requirement
 - Identify Remediation plans for each SEC501.01 and VITA requirement (in-progress)
 - Review Agency Self Assessments & create Draft Agency Remediation Plans for each individual Agency (next step)

SEC 501.01 Risk Remediation

- Partnership Plan & Status (cont):
 - Deliver and review your Agency Draft Remediation Plans with your Agency
 - Finalize your Agency Remediation Plan with your Agency
 - Partnership Staff begins work on agreed to Agency Remediation Plan
 - Some Remediation efforts will be completed NLT 28 Sept 2007
 - Additional Remediation efforts (such as those addressed via Transformation) may require the Agency to file an Exception with Commonwealth Security NLT 28 Sept 2007



NORTHROP GRUMMAN

Sample Agency Remediation Plan

(A) COV ITRM Standard SEC501- 01 Requirements	(B) NG Enterprise Security Practice(s)	(C) Practices Compliant (yes/ no)	(D) Document Different Practices	(E) Remediation Plan	(F) Time Frame
<p>Requirement 5.3.2.2: Documented Agency password management practices shall define requirements for password length and complexity based on sensitivity and risk.</p>	<p>VITA/NG EISP 3.2.2.3 (d)</p>	<p>No</p>	<p>N/A</p>	<p>The partnership has documented password management procedures to ensure compliance with SEC 501.01. Partnership personnel will be implementing these new procedures before the 28 Sept 2007 deadline.</p>	<p>Immediate</p>
<p>Requirement 9.2.2.3: Documented Agency threat detection practices should address log reviews of Intrusion Detection Systems (IDS) and Intrusion Prevention System (IPS) to detect new attack patterns as quickly as practicable.</p>	<p>VITA/NG EISP 8.2.3 (a), (b)</p>	<p>No</p>	<p>N/A</p>	<p>Partnership personnel have indicated that an IDS is not currently in place for your network infrastructure. However the Partnership does currently provide an enterprise security protection system, called the Internet Security Internet Tracking and Monitoring System (ISITMS), to track, alert and prevent malicious traffic from coming across Partnership networks. In addition, once your infrastructure assets are consolidated into the Chesterfield Data Center, all your assets will be provided with IDS protection and 24x7 incident monitoring.</p> <p>Therefore, you will need to evaluate the risks of not having an IDS in place, and if you should decide that you require an IDS then an RFS must be submitted. Also, since an IDS can't be implemented by the 28 Sept 07 deadline, an exception to SEC501.01 requirement 9.2.2.3 must also be requested from VITA Security.</p>	<p>Transformation and/or TBD</p>

Sample Agency Remediation Plan

(A) COV ITRM Standard SEC501-01 Requirements	(B) NG Enterprise Security Practice(s)	(C) Practices Compliant (yes/ no)	(D) Document Different Practices	(E) Remediation Plan	(F) Time Frame
Requirement 6.3.2.1: Commensurate with sensitivity and risk, each Agency shall define and document Agency practices for selecting and deploying encryption technologies and for the encryption of data.	VITA/NG EISP 7.2.2.2 (a-i)	No	N/A	Implementing an encryption solution is the responsibility of the Agency and not the Partnership. However, Partnership will implement and utilize the encryption solution adopted by the Agency.	TBD
Requirement 7.2.3: Documented Agency facilities security practices shall require appropriate environmental controls such as electric power, heating, fire suppression, ventilation, air-conditioning and air purification, as required by the IT systems and data.	VITA/NG EISP 13.2 (and sub-sections)	No	N/A	The partnership has documented facility security procedures to ensure compliance with SEC 501.01 and Partnership personnel will be working with you in order to implement these new procedures.	TBD

SEC 501.01 Risk Remediation

- Questions?



Virginia Information Technologies Agency

The Current State of Malware

• Botnets •

Tripp Sims

Commonwealth of Virginia Security Architect

August 8, 2007

Questions & Comments: tripp.sims@vita.virginia.gov



Content

- Common Infection Methods
 - Browsers, Network Services, and Users
- Botnet Threats
- Defenses
 - Desktop & Patch Management, AntiVirus, Firewall/IDS/IPS, Behavior Based HIDS, and Education and Solutions
- Questions and Answers



Common Attack Methods

Methods of Infection

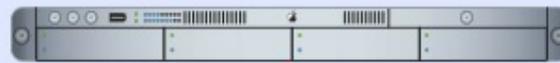
The Browser
Network Services
The User

How the "Drive-by" Works

Real World Example of How the Asus.com Hacker Infected Victims



• Legitimate Asus Website Hacked •
No Defacement
Located at a data center in the UK.



• Elicit Web Server •
Hosting Exploit and Malware
Located at a data center in the China.



What happened to my bank account?

Hacker gains ability to edit asus.com html

•
Hacker doesn't "tag" the site.

•
Hacker edits the homepage to include an invisible reference to his exploit hosted in China

•
Upon successful browser exploitation password stealing malware is installed on the users computer

Mpack - A Browser Exploitation Kit

Mpack Features

Included with kit is a free malware downloader executable for Windows that is guaranteed undetectable to AV at time of sale.

Version 0.93 supports 12 browser exploits.

Encrypted (trivial) Javascript for exploit delivery to browser.

Browser identification routines ensure exploits are only delivered to browsers deemed vulnerable.

Mpack currently sells on underground forums for between \$150 and \$1000 depending on the version and extra features requested.

Referer	Count
http://81.95.148.162/e1/check.php	2967
No referer	282

Country	Traff	Loads	Efficiency
DE - Germany	2829	43	1.52
RU - Russian federation	124	6	4.84
US - United states	38	18	47.37
UA - Ukraine	28	2	7.14
GR - Greece	22	0	0
GB - United kingdom	16	6	37.5
PS - Palestinian territory, occupied	16	2	12.5
EG - Egypt	15	2	13.33
QA - Qatar	15	8	53.33
CA - Canada	14	7	50
BY - Belarus	10	0	0
AT - Austria	10	0	0
MA - Morocco	7	0	0
SA - Saudi arabia	7	0	0
FR - France	6	5	83.33
KW - Kuwait	6	0	0
IL - Israel	5	1	20
TR - Turkey	5	0	0
LT - Lithuania	4	0	0
BG - Bulgaria	4	0	0
BH - Bahrain	4	0	0
ES - Spain	4	2	50

Mpack v0.86 stat

Attacked hosts: (total/uniq)

IE XP ALL	2913 - 2896
QuickTime	265 - 253
Win2000	89 - 89
Firefox	105 - 105
Opera7	21 - 21

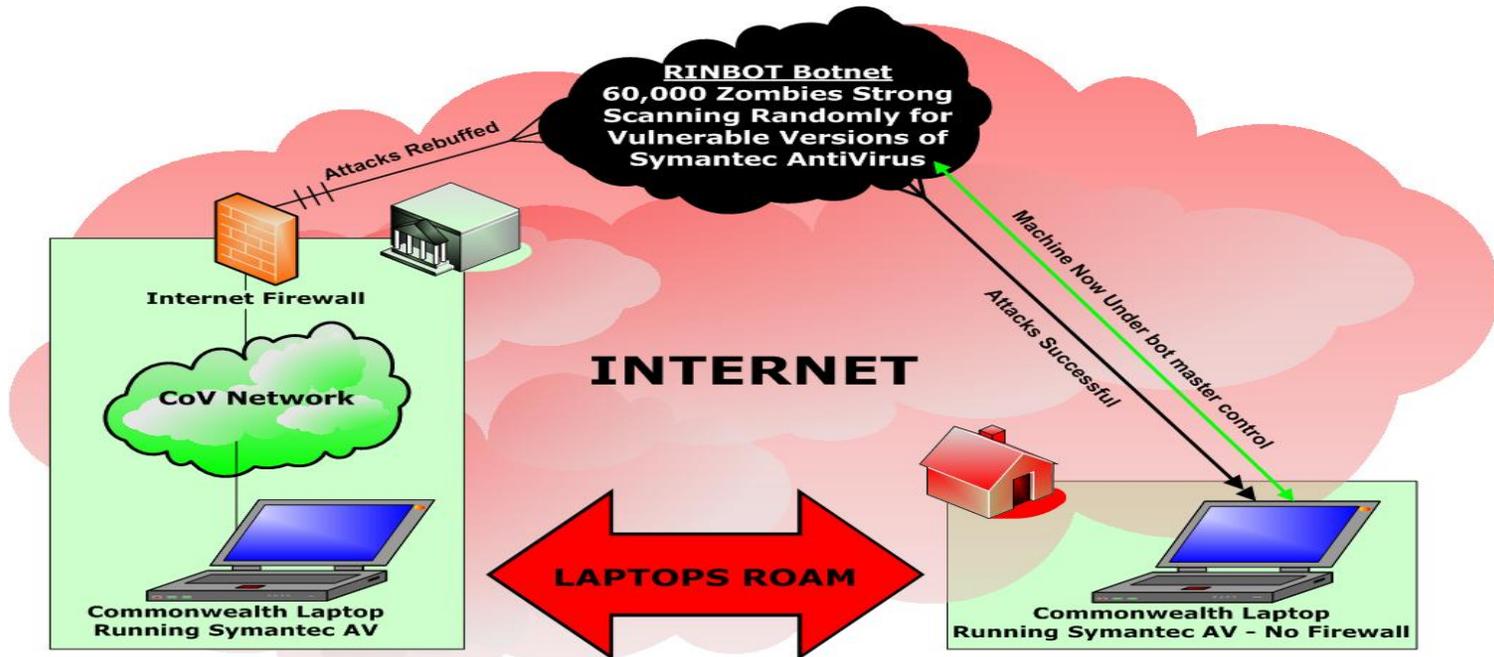
Traffic: (total/uniq)

Total traff:	3255 - 3223
Exploited:	436 - 136
Loads count:	111 - 89
ider's response:	25.46% - 65.44%
lser blocking:	ON
untry blocking:	OFF

Efficiency: 3.41% - 2.76%

Network Services Attack Example

If your assets aren't firewalled at all times, eventually they will be exposed to a network services attack.



Real World 0-Day Example – “RINBOT”

“...the average time-to-exploitation on some networks for an unprotected computer is measured in minutes.” -USCERT

Using Users to Exploit Systems

- Malicious e-mail attachments
 - Still a highly utilized methodology
 - Vulnerable application formats are still highly variable
 - .doc; .zip; .rar; .ppt; .xls; .jpg; .msi; etc...
- Peer-to-Peer File sharing
 - P2P propagation is still highly viable
- Pirated Software and “Cracks”
 - Bittorrent, Newsgroups, and other forms of pirated software distribution are still shown to contain a high quantity of malicious code.
 - Most pirated software cannot be updated for security vulnerabilities.
- Instant Messenger Mal-Links
 - “Did you see this picture of you on MySpace?”



Botnets

Botnet is a jargon term for a collection of software robots, or zombies, which run both as autonomous units and as collective units.

While the term "botnet" can be used to refer to any group of bots, such as IRC bots, the word is generally used to refer to a collection of compromised computers (called zombie computers) running malware which operates under a common command and control infrastructure.

A botnet's creator (aka "herder") can control the zombies remotely, usually through a means such as HTTP, Peer-to-Peer, and most commonly IRC.

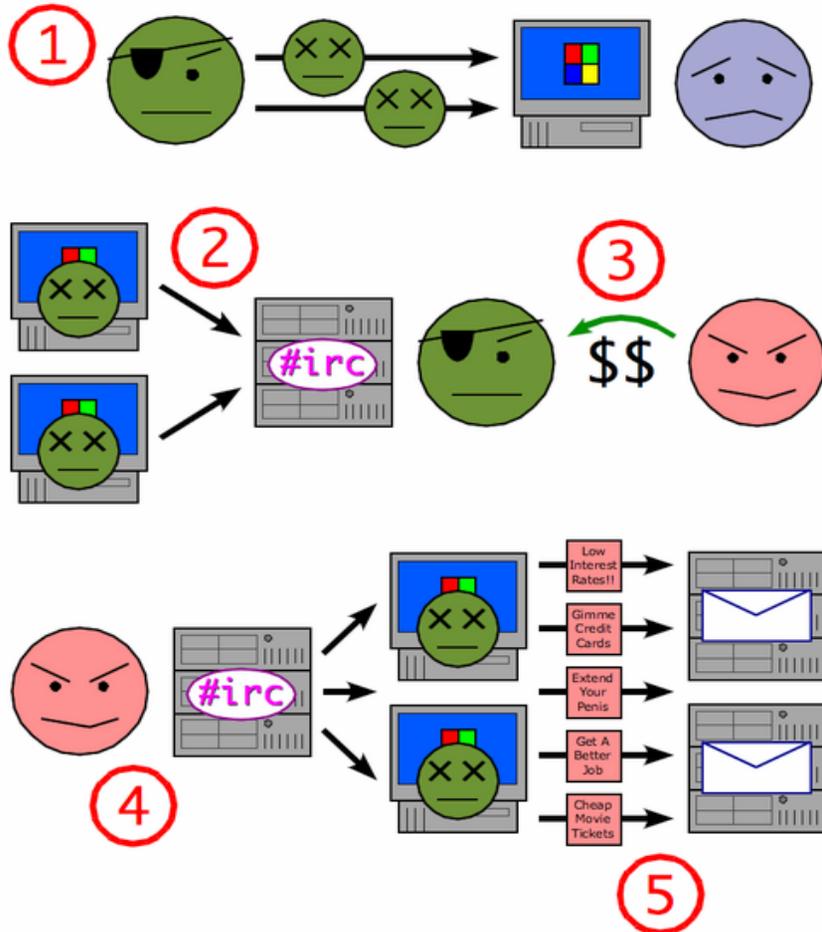
The largest botnets typically spread themselves. This is done by scanning and exploiting remote vulnerabilities, IM spamming malicious links, and email spamming malicious links.



Botnets – Some Facts

- Can be self-propagating with no need to communicate to Command & Control server
- Features that have been found in bot code include: spam engines (both SMTP and IM), firewall bypass, AV killer, keylogger, password stealer, DDoS, vulnerability scanning, CD Key Thief, web server, Socks server, click fraud, remote installation of ad-ware, rogue bot “killer” code, and backdoors.
- Botnets have been found that are 1 million+ computers strong. No internet infrastructure could withstand a Distributed Denial of Service attack from such a network.
- Botnets have been used to attack key pieces of Internet infrastructure, including: Root DNS servers, DNS Registrars, small countries, and online commerce companies.

Botnets – The SPAM Example



From Botnet to SPAM

1. Herder seeds his initial botnet through by-hand-hacking.
2. Machines infected with the herder's bot code connect to an IRC Command & Control server and begin to self-replicate by scanning other machines for vulnerabilities.
3. When the network reaches a sufficient size a spammer pays the herder for use of his network to send out spam email.
4. Spammer feeds the botnet his code to send out millions of spam emails.
5. Spam from zombies begins to hit Inbox's around the world.



Malware Defense

- Layered approach to Security (Defense in Depth)
 - In situations where it's not cost effective to support the best possible security posture, keep in mind that every layer of protection utilized is another security hurdle for the "bad guys" to circumvent.
 - As security representatives of the citizens of Virginia's data we are not only required to keep our own resources secure, but we are also bound to educate and offer solutions to the citizens to better protect their own data.



Desktop and Patch Management

A strong desktop policy and patch management can be one of the easiest and most effective layers of security

- Apply Principle of Least Authority (POLA) to users' workstations.
 - Can your users install software themselves?
 - Do you use separate user accounts on your home computers? And does your primary account have Administrator privileges?
- Keep up with OS & application patching.
 - Managed enterprise infrastructure has documented plans for testing and deploying security patches.
 - Home users should be advised to turn on automated updates and respect the importance of these updates to their computers.

IT Security Standard, Section 5.2.2 – “Requires that local administrator rights, or the equivalent on non-Microsoft Windows-based IT systems, be granted only to authorized IT staff.”



Anti-Virus

- Anti-Virus is an essential first line of defense
- Use solutions from well known vendors
- Be aware of malicious offerings that distribute malware posing as Anti-Virus

For enterprise workers consider using the standard Anti-Virus used in the enterprise for your home computer.

AntiVirus

As the chart to the right illustrates, the overall effectiveness of AntiVirus is a tricky beast to evaluate. But, as a rule, any AntiVirus is better than no AntiVirus.

You are however encouraged to work with well known names. There are numerous companies that distribute their malware posing as AntiVirus.

For enterprise workers we recommend the standard AV from your enterprise be extended to your home computer.

vendor	detected	total	percent
NOD32	15451	15682	98.53%
DrWeb	15322	15682	97.70%
AntiVir	15302	15682	97.58%
Norman	15209	15682	96.98%
Kaspersky	7812	15682	49.82%
QuickHeal	7746	15682	49.39%
Vexira	7449	15682	47.50%
F-Prot	7125	15682	45.43%
AVG7	6768	15682	43.16%
McAfee	6767	15682	43.15%
Avast	0	15682	0.00%
BitDefender	0	15682	0.00%
Clam	0	15682	0.00%
Panda	0	15682	0.00%
VBA32	0	15682	0.00%
VirusBuster	0	15682	0.00%

Zero day binaries collected and scanned by Shadowserver on 7/7/2007



Firewalls/IDS/IPS

- Network Firewalls are another layer of defense
- Firewalls features can include Intrusion Detection/Prevention features
- Recommend a 'default deny' policy for outbound traffic, then selectively open for user traffic as needed



Firewalls/IDS/IPS

- Network Intrusion Detection & Prevention Systems as an additional layer of defense
- Most IDS/IPS solutions are signature based and must be updated and current (same as Anti-Virus)
- There are 'security center' solutions for home users that include host-based personal firewalls with IDS/IPS features built in.



Customer Education

- Customer Education is the most important line of defense!
- The citizen's computer is much more likely to be the source of leaking personal information than legitimate websites
- What can you do to help keep citizens' data secure?
 - Banner type notification when citizens visit your site to do business
 - Offer security resource pages that can help a customer understand what they can do to increase their own security.



Draft – Banner Security Template

Protecting against viruses and spyware

There are several easy ways to protect your computer against viruses and spyware:

- **Anti-spyware protection:** Make sure your computer has an anti-spyware protection program that detects and removes all forms of spyware, which can steal vital information. Use this program to scan your computer frequently. Many software companies offer software that will protect you from a wide variety of spyware threats, and also will provide customer service in case you have questions. To keep up with any new threats, be sure to keep your anti-spyware program updated.
- **Anti-virus protection:** Make sure your computer has an anti-virus protection program that detects and removes viruses. Software from major providers will protect you from a wide variety of threats, and also will provide customer service in case you have questions. Be sure to always keep your anti-virus program updated.
- **Automatic upgrades.** Buy a protection program that automatically upgrades your spyware or virus protection on a recurring basis. If you don't have this automatic upgrade feature, make sure you update your spyware and virus detection programs daily, as well as whenever you hear of a new computer threat.
- **Attachments.** Don't open attachments or diskettes unless you're sure that you can trust the source. Learn how to manually screen diskettes and attachments if your anti-virus software doesn't automatically do so.
- **Contact your ISP.** Your Internet service provider (ISP) may have more recommendations and technical support for protecting yourself. Contact your ISP for recommendations specific to your computer and network.



Customer Education

Customer Solutions

There are practices you can consider for inclusion on your customer facing applications. There are also a number of free resources online that can help a customer understand the security posture of their computer.

- Many AntiVirus vendors offer free web based AntiVirus and security scans which run through the web browser. Point your customers to them as a resource for their personal data security
- There is also a free browser security testing site available @ <http://www.scanit.be/browser-security-test.html>
- Consider maintaining a black-list of known insecure browser user-agents. Browsers which identify themselves as known insecure to your applications could be warned before gaining entry to your applications.



The Current State of Malware

Questions



Virginia Information Technologies Agency

ISO Orientation

Peggy Ward





ISO Orientation

What is it? – Small group overview of the IT Security Program in the Commonwealth focusing on the COV IT Security Policy and Standards!

Who can attend? All ISO's for any Commonwealth State Government entity should attend! Localities welcome if they have an interest!



ISO Orientation

When is it? – As needed but generally monthly for 1.5 – 2 hours!

How can attend? Send an email expressing interest to:

VITASecurityServices@VITA.Virginia.Gov

We will contact you for next available date, time and place!



Virginia Information Technologies Agency

Upcoming Events

Peggy Ward





UPCOMING EVENTS!

Wednesday August 22, 2007, 2:00 p.m. – 3:00 p.m.

FREE national webcast "Keeping Your Broadband Internet Connection Secure"

Sponsored by the Department of Homeland Security's National Cyber Security Division & the Multi-State Information Sharing and Analysis Center

More information and registration is available at:

- http://www.msisac.org/webcast/08_07/



UPCOMING EVENTS!

FREE seminars on Soft Target Awareness for Large Buildings

Jointly sponsored by The U. S. Department of Homeland Security, Virginia Department of Transportation, & the Governor's Office of Commonwealth Preparedness

- Location: VDOT Central Office Auditorium; 1221 E. Broad St., Richmond, VA
 - August 29, 2007 - 1:00 pm to 5:00 pm or
 - August 30, 2007 – 8:30 am to 12:30 pm
- Location: Greenfield Educational Center; 57 South Center Drive, Daleville, VA
 - September 12-14, 2007 8:30 am to 5:00 pm; 8:30 am – 12:00 pm

Pre-Registration Required. To Register, contact:

Lisa Cline

Operations & Security Division

Virginia Department of Transportation

1221 E. Broad St.

Richmond, Va. 23219

Lisa.cline@vdot.virginia.gov

Fax: (804) 692-0810



UPCOMING EVENTS!

ISOAG -Thursday, September 13, 9:00 a.m. - noon
@ the **Library of Virginia**

Draft Agenda:

- Document Management - DEQ
- Electronic Records - Library of Virginia
- COV IS Council Update
- New IT Security Guidelines
- Honeypots - VITA



UPCOMING EVENTS!

COVITS – September 16 -18

Chantilly, Va

<http://www.covits.org/>

NSAA IT Conference & Workshop

September 26 – 28, 2007

Richmond, Virginia

http://www.nasact.org/conferences/conferenceinfo/IT_07_geninfo.htm



Virginia Information Technologies Agency

Any Other Business ?





ADJOURN

THANK YOU FOR YOUR
TIME AND THOUGHTS

Stay COOL

!!!

