Cybersecurity

- What are some great Anti-Spyware Tools?
- Detecting Mac OS X Trojan "Flashback"
- SQL Injection (Application Vulnerability)
- Cloning systems with Sophos and Sysprep
- Useful OSS Security Tools
- What is the function of www.AppliedSecurity.ucla.edu site?
- Is the cost of licenses to protect sensitive data by encrypting the disk paid by the campus?
- How to Prevent Unauthorized Users From Accessing Your Computer if you Step Away From Your Desk
- What to do if your e-mail is hacked
- Verizon's Annual Data Breach Investigations Report (DBIR)
- Reducing Laptop Theft
- Sophos Security News & Blogs
- Symantec's Annual Internet Security Threat Report
- Sophos Security Threat Report
- Mobile Device Management Now Available With Sophos
- Explaining to your mother how to safely surf the web at Starbucks
- Heartbleed Remediation
- Windows Bitlocker Strength
- Tips for creating a secure password
- Intrusion Detection Systems Information
- Where can I go to find out more information on viruses, worms, trojans, spyware, hoaxes, etc...
- Phishing protection
- Why shouldn't I email or post Microsoft Word documents?
- How can I make more secure passwords that I can still remember?
- What is PGP? Where can I get more info?
- Are there any security requirements for connecting a device to the UCLA network?

- What is UCLA ASTF and who are its members?
- Kerberos
- Anti-virus, firewall and Internet security software
- Where can I download Sophos Anti-virus and how do I install it?
- National Vulnerability Database
- Norton Antivirus causes email sending problems
- New UC guidelines on Encryption
- Preventing SSH Dictionary Attacks With DenyHosts
- Security Engineering - free e-book
- How do I obtain Sophos Anti-Virus Software at UCLA
- Uninstalling Norton Antivirus
- I need a free file encryption software
- Is there a free Anti-Virus software for Windows XP 64-bit?
- UCLA Multi-Factor Authentication

What are some great Anti-Spyware Tools?

Ad-Aware SE Personal Edition – http://www.download.com

Spybot Search and Destroy – http://www.download.com

Hi-Jack This – http://www.download.com

Detecting Mac OS X Trojan "Flashback"

Background

As of October 2011, a Trojan named Flashback has been targeting Mac OS X users by masquerading as a legitimate version of the Adobe Flash Player installer. Its visual elements and user interface are is quite similar, if not identical in certain cases, to the official Adobe Flash Player installer. Upon installation, it checks for the built-in Mac OS X firewall and if it is not found, the malware may request payloads from remote hosts. (1)

According to F-Secure researchers:

“There are three variants of Flashback. According to F-Secure, two of them cannot connect to their remote hosts, as they are offline. The third can connect to the remote host for additional payloads, but the host isn’t serving anything. Also, unlike the first version, the other variants are requiring an administrator password before proceeding with installation.” (2)

Mitigation Recommendations

1. It is recommended that Adobe Flash player installations only come from the official Adobe Flash website (http://www.adobe.com/products/flashplayer.html)

2. Flashback installs to “~/Library/Preferences/Preferences.dylib” so a user could check for the presence of that file to gauge whether Flashback is running on their Mac.

3. Sophos also detects the file as “OSX/FlshPlyr-A” so those with the campus-provided anti-virus software should be notified so long as their anti-virus definitions are updated. Sophos is a free anti-virus software that UCLA provides to the campus community. It can be downloaded from the UCLA

Bruin OnLine Sophos website. (http://www.bol.ucla.edu/software/sophos/)

References

(1) http://www.securityweek.com/mac-os-x-trojan-targeting-apple%E2%80%99s-anti-malware-system

(2) Ibid.

SQL Injection (Application Vulnerability)

Summary

SQL Injection is a type of security vulnerability that occurs when application does not properly sanitize user inputs. The vulnerability potentially allows attacker to arbitrarily manipulate queries sent to the database layer. This type of vulnerability is usually considered medium/high severity since private data can be leaked or integrity of data can be affected.

Types

- Unsanitized or improper sanitized escape characters
- Weak-typed user input handling
- Blind SQL injection

Cloning systems with Sophos and Sysprep

During deployments of multiple systems with the exact same hardware configuration, Sysprep is the most common tool to assist this along with Ghost.

If you have Sophos on your original deployment image, you may find that you cannot access the Sophos console on cloned systems with Sysprep (or other tools that change the computer SID).

To repair this:

http://www.sophos.com/support/knowledgebase/article/12561.html

---

If you have already deployed cloned systems and need to repair your Sophos installation follow the instructions at the bottom of the article, “Changed SID values and Sophos Anti-Virus”:

On a computer where the SID value has been changed, open a command prompt and type the following command:

- MsiExec.exe /i “c:\Program Files\Sophos\AutoUpdate\cache\savxp\Sophos Anti-Virus.msi” REINSTALL=ALL REINSTALLMODE=voums UPDATEDRIVERS=0 /l*v c:\msi.log /qb

On Windows Vista the command is:

- MsiExec.exe /i “c:\ProgramData\Sophos\AutoUpdate\cache\savxp\Sophos Anti-Virus.msi” REINSTALL=ALL REINSTALLMODE=voums UPDATEDRIVERS=0 /l*v c:\msi.log /qb

-

If you are doing this on the master image *before* you have deployed it or after you have deployed cloned systems, follow the link above.

1. On the template computer, stop the following services (if they are present):

- Sophos Message Router
- Sophos Agent
- Sophos AutoUpdate Service

1. Read the Microsoft warning about editing the registry.
2. On the template computer, in turn, open each of the following registry keys (if they are present):

- [HKEY_LOCAL_MACHINE\Software\Sophos\ALC Agent\Private]
- [HKEY_LOCAL_MACHINE\Software\Sophos\Messaging System\Router\Private]
- [HKEY_LOCAL_MACHINE\Software\Sophos\Remote Management System\ManagementAgent\Private]

and, in each key, delete the following two entries

- pkc
- pkp

Note: These keys must not be removed from a server running Enterprise Console.

1. Delete the following files from the template computer:
   C:\Program Files\Sophos\AutoUpdate\Data\Status\status.xml
   C:\Documents and Settings\All Users\Application Data\Sophos\Sophos Anti-Virus\Config\Machine.xml

Useful OSS Security Tools

1 – Alienvault – Open Source Security Information Management system – *good review in the latest (March 2010) Linux journal*

From the web site: The OSSIM platform consists of a Management Server, and Sensor or “Probe”. A professional version that includes SEM functionality is also available (please see below). The solution may be implemented as a single monolithic appliance or a set of appliances in which probes are separated from the management server, and distributed throughout the enterprise.

Probes capture network and system information in real time, and send it to the central Management Server where the data is analyzed to assess immediate threats and risk, filter out false positives, and locate false negatives that other security devices and software on the network cannot detect.

Probes not only capture data, but can be tasked as sophisticated attack detection components. They come with several attack detection systems, audit systems, and context learning systems (network profiles, inventory, availability), all of which are seamlessly integrated. When deployed in this fashion probes provide a very quick and safe way of continuously and transparently monitoring local and remote networks, providing provide full visibility of all security related aspects of the enterprise.

The information from the organization’s security systems, such as the firewall, antivirus, IPS, HIDS, etc, are all collected through these probes, and then analyzed through sophisticated intelligence technology. This technology correlates data from many sources to detect blended threats otherwise undetectable by individual systems; prioritize these threats; and make automated decisions with regard to the risk implied in each one.

2 -DEFT Linux – live Linux Distro for Forensics / Network Security / Analysis

DEFT Linux v5 is based on the new Xubuntu Kernel 2.6.31 (Linux side) and the DEFT Extra 2.0 (Computer Forensic GUI) with the best freeware Windows Computer Forensic tools ; it isn’t a customization of Xubuntu like the old version, it is a new concept of Computer Forensic live system that use LXDE as desktop environment and thunar file manager, mount manager as tool for device

management, dhash2, guymager, dcfldd, ddrescue and linen as forensic imager tools, sleuthkit 3.01 andvautopsy 2.21 as landmark for the disk forensic, nessus 4 as security scanner and much more like:

an advanced file and directory researcher
foremost, scalpel and photorec carving tools
a complete support for the most used file systems
a complete support for logical volume manager
a complate support for afflib and ewflib support
a very powerful tools for network forensic as Xplico, wireshark,
kismet, ettercap and nmap
a very powerful tool for identify file type from their binary
signatures (TrID)
the last version of ophcrack, the password cracker based on rainbow
tables and john the ripper password cracker
chkrootkit, rkhunter and exploit scanner
clam 4.15 virus scanner
steganography detection software as outgess
tool for screenshot as take screen shot and video screen capture as
record my desktop
deft-mount script for mount device in read only

Can be booted from a thumbdrive or CD.

3 – Eraser for Windows Eraser is an advanced security tool for Windows which allows you to completely remove sensitive data from your hard drive by overwriting it several times with carefully selected patterns. Works with Windows 98, ME, NT, 2000, XP, Vista, Windows Server 2003 and Server 2008.

Sort of like a Windows-native Darik's Boot And Nuke

Taken from email to UC-CSC list by UCI colleague Harry Mangalam

What is the function of www.AppliedSecurity.ucla.edu site?

This site is dedicated to posting practical solutions to current data security issues facing the community. The current topics include listing of IT policies, Peer-to-Peer, and Encryption of sensitive data and related tools on campus.

The site is accessible only from UCLA IP addresses. The site address is:

- http://www.itsecurity.ucla.edu/

Is the cost of licenses to protect sensitive data by encrypting the disk paid by the campus?

Yes. The campus IT security group has chosen PGP full disk encryption and related tools for this purpose. All campus entities with a need to protect their sensitive data and data coverd in campus Policy 404 (Data including Personal Information) are entitled to use the available tools at no cost to the department or the individual.

Contact your IT department or your IT Compliance Coordinator on how to start protecting your data. For more information visit: www.appliedsecurity.ucla.edu.

How to Prevent Unauthorized Users From Accessing Your Computer if you Step Away From Your Desk

It takes only a few seconds to secure your computer and discourage malicious individuals. Lock down (or log out of) your computer every time you leave your desk.

To log back in, you'll need to put in the username/password for your computer, which may be one you choose, or it may be your departmental login information. Be sure to shut down your computer completely when you leave for the day.

To Lock Down Your Computer

- Mac
- Windows 7
- Windows XP

To Log out of a Mac

- From the Apple pull-down menu, select "Log Out"
- Mac shortcut: Shift-Command-Q

To Lock Down Windows 7

1. Go to the Start menu

2. Select the right pointing arrow from Shutdown category from the bottom right
3. Select Lock

To Lock Down Windows XP

1. Click Ctrl+Alt+Delete
2. Select “Lock Workstation”
3. This will bring up your login screen and lock your computer down.

Windows XP shortcut: Click the Windows key (the flying window key at the bottom of the key board) and the L key. This will bring up your login screen and lock your computer down.

How do I set a password-protected screen saver?
If you forget to log out of your computer when you walk away, for your protection, you should set up a screen-saver that will lock your computer after a pre-set amount of time and require a password to log back in.

To Set a Password-Protected Screen Saver

- Windows 7
- Windows XP
- Macintosh OS 10.0 – 10.5
- To Set a Password-Protected Screensaver for Windows 7

- Right click on your desktop and select “Personalize” from the menu.
- Then click the “Screen Saver” link from the Personize window.
- Under the Screen Saver section, check the box for “On resume, display logon screen.”

To Set a Password-Protected Screensaver for XP
Right click on your desktop. A drop down menu box will appear. Select “Properties.” See Insert Fig. 1

Insert Figure 1

The display properties for the desktop will appear. Click on the “Screen Saver” tab.

See Fig. 2

Insert Figure 2

- Click the arrow on the drop down list for “Screen Saver.” Select the screen saver you would like.
- Click the up/down arrows on the “Wait” box to set the time lapse before your screen saver starts. Five minutes is a good choice.
- Check the box in front of “On resume, password protect.” If you have Windows 2000, it may just say “Password Protect.”
- Click “OK” or “Apply” and close out of the Display Properties Box.
- To login when your screen saver is running, you can: move your mouse; hit the enter key; or click Ctrl+Alt+Delete. Any of these will bring up your login screen. Type in your Novell or Windows password, click “OK” or hit the enter key and you will be logged in to your computer.
  Alternative Method: You can also reach the “Display Properties” box by:

Clicking “Start” in the taskbar at the bottom of the desktop screen and click on “Control Panel.” See Fig. 3

insert Figure 3

A window will appear that will have many icons or a list of items. Click on the “Display” icon or the “Display” in the list. See Fig. 4.

Insert Figure 4

To Set a Password-Protected Screen Saver for Mac OS 10.0 – 10.5

1. Open “System Preferences”
2. Click on the “Security” icon
3. Check the “Require password to wake this computer from sleep or screen saver” field.
4. Return to the “System Preferences” and choose the “Desktop and Screen Saver” icon
5. Select the “Screen Saver” tab
6. Set the amount of time you want to pass before the screen saver starts (5 minutes is a good limit)
7. When the screen saver activates after the required time period has lapsed and/or you want to unlock your computer move the mouse, click on a key to logon to your computer.

What to do if your e-mail is hacked

Standard steps to do if you believe your e-mail has been hacked:

http://blogs.msdn.com/b/securitytipstalk/archive/2010/07/07/hotmail-hacked-take-these-steps.aspx

While Hotmail is the most common target for hacking in the media, the instructions and general advice are good:

Courtesy of MSDN:

1. Change your password. (On the Windows Live Hotmail Web site sign-in page, click Forgot your password?)
2. Update and change the secret question and answer used to recover your password.
3. Update and change the alternative email address that you use on your account.

If you no longer have access to your account, please contact the appropriate administrator to restore access to your account.

- For Hotmail, try: https://windowslivehelp.com/PasswordReset.aspx
- For SSC e-mail, contact: http://computing.sscnet.ucla.edu/public/contact/
- For UCLA e-mail, contact: http://www.bol.ucla.edu/
- For Gmail (google mail), try: https://www.google.com/accounts/recovery?continue=http%3A%2F%2Fmail.google.com%2Fmail

Additionally, we strongly recommend that you consider whether or not personally identifiable information has been compromised and contact your banks/credit cards/etc. for fraud alerts if they are at risk.

Courtesy of MSDN:

- Your credit card company, if you have given your credit card information. The sooner an

organization knows your account may have been compromised, the easier it will be for them to help protect you.

- The Federal Trade Commission (In the United States). Report the circumstances to the FTC: National Resource for Identity Theft. http://www.consumer.gov/idtheft/
- The Anti-Phishing Working Group at spam@uce.gov.

Verizon's Annual Data Breach Investigations Report (DBIR)

A dramatic increase in attacks by outside parties. Breaches fueled by monetary gain. Hacking and malware threats on the rise.

Data breaches continue to plague organizations worldwide, and we continue to analyze them ? so you can learn how to avoid becoming a victim. The DBIR series now spans eight years, more than 2,000 breaches, and over 1 billion compromised records. Our goal is to distinguish who the attackers are, how they're getting in, and the assets they're targeting.

The more you know, the better you can prepare ? and our reports provide insight and clear recommendations for you to follow to face security threats head-on.

- **http://www.verizonenterprise.com/DBIR/**

Also:

- https://kb.ucla.edu/link/1607
- **2017**, https://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/
- **2016**, http://news.verizonenterprise.com/2016/04/2016-data-breach-report-info/
- **2015**, http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf
- **2014**, http://www.verizonenterprise.com/resources/reports/rp_Verizon-DBIR-2014_en_xg.pdf
- **2013**, http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf
- **2012**, http://securityblog.verizonbusiness.com/2012/03/22/2012-data-breach-investigations-report-released/, and http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

- **2011**, http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf
- **2010**, http://www.verizonenterprise.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf
- **2009**, http://www.verizonenterprise.com/resources/security/reports/2009_databreach_rp.pdf
- **2008**, http://securityblog.verizonbusiness.com/2008/08/20/do-the-findings-of-the-2008-data-breach-investigations-report-differ-among-industries/ (covers 2004 to 2007), and http://securityblog.verizonbusiness.com/2008/10/02/2008-data-breach-investigations-supplemental-report/

Reducing Laptop Theft

To assist in reducing laptop theft UCPD participates in part of a nationwide security tracing program. The STOP system is applicable to computer laptops, digital projectors, and other portable devices.

For $20 UCPD will affix a permanent tag which ‘tattoos’ the device. The process takes five to ten minutes.

Contact UCPD CSO at 310/82*5-4774*, or email at **cso@ucpd.ucla.edu**.

STOP homepage

Sophos Security News & Blogs

Sophos has a number of security news feeds and blogs at:

- http://www.sophos.com/en-us/why-sophos/our-people.aspx
- http://www.sophos.com/en-us/why-sophos/our-people/technical-papers.aspx
- http://www.sophos.com/en-us/why-sophos/our-people/inside-sophoslabs.aspx
- http://nakedsecurity.sophos.com/category/sophoslabs/
- http://www.darkreading.com/blog/archives/sophoslabs-insights/index.html

Sophos Support on Twitter:

- **https://twitter.com/SophosSupport**

Symantec's Annual Internet Security Threat Report

The Internet Security Threat Report (ISTR) provides an overview and analysis of the year in global threat activity. The report is based on data from the Symantec Global Intelligence Network, which Symantec’s analysts use to identify, analyze, and provide commentary on emerging trends in the dynamic threat landscape.

- **http://www.symantec.com/business/threatreport/**

see also:

- **Archived reports**, http://www.symantec.com/security_response/publications/archives.jsp
- Symantec **YouTube** channel, http://www.youtube.com/user/symantec

Sophos Security Threat Report

See the threats through the hype, with the latest research and commentary from SophosLabs.

- http://www.sophos.com/ThreatReport

See also,

- **2013**, http://www.sophos.com/en-us/security-news-trends/reports/security-threat-report.aspx
- **2012**, http://www.sophos.com/threatreport2012
- **2011**, http://www.sophos.com/threatreport2011
- **Archive**, http://www.sophos.com/en-us/security-news-trends/whitepapers.aspx

Mobile Device Management Now Available With Sophos

The current UCLA-wide agreement for Sophos anti-virus software has been renewed through October 2018.

The decision to renew was based upon input from numerous key stakeholder groups UCLA-wide. Input identified that Sophos effectively fulfills UCLA's anti-virus needs, and that the cost to change to an alternative solution would outweigh any potential benefits.

Renewal negotiations resulted in favorable terms, including:
—Unlimited coverage for UCLA owned or leased devices
--Unlimited coverage for personally owned devices of faculty, staff and full-time students
—Upgrade to Endpoint Protection-Advanced
--Addition of Sophos Mobile Control

Sophos remains AVAILABLE AT NO COST to UCLA departments, faculty, staff and students for work and home use.

For Department IT Administrator access to the products available under this agreement, please go to http://www.bol.ucla.edu/software/sophos/admin/.

Explaining to your mother how to safely surf the web at Starbucks

The title is mostly for fun, but I’m curious if anyone has found fairly simple guides to safely browsing at public internet cafes or open wireless like UCLA_WIFI.

Not simple enough for some mothers, I did like this guide.
(9 Tips to stay safe on public wifi)

Heartbleed Remediation

For up to date status of Dell products in relation to Heartbleed visit —

- http://www.dell.com/learn/us/en/04/campaigns/heartbleed-remediation

Mashable's List of sites to watch for Heartbleed—

- **The Heartbleed Hit List: The Passwords You Need to Change Right Now**, http://mashable.com/2014/04/09/heartbleed-bug-websites-affected/

Lynda.com has a couple of short videos to explain the situation—

- **Protecting Yourself from the Heartbleed Bug** (6 min)
- **Heartbleed Tactics for Small IT Shops** (16min)

Please feel free to add links to other articles about Heartbleed that others may find useful or interesting. Thanks!

Windows Bitlocker Strength

By default Windows 7/8 Bitlocker uses 128-bit encryption. Each version has an option for 256-bit AES encryption. The change to 256-bit requires a Windows policy modification.

See also—

- Bitlocker Step-by-Step Guide, http://go.microsoft.com/fwlink/?LinkId=53779
- Note for Vista and 7, http://windows.microsoft.com/en-US/windows-vista/What-is-the-difference-between-BitLocker-Drive-Encryption-128-bit-and-256-bit-encryption
- Bitlocker strength and unlock methods, https://technet.microsoft.com/en-us/library/ee706531(v=ws.10).aspx

Tips for creating a secure password

How can I create a secure password?

Update: Read this first: Choosing a Secure Password by Bruce Schneier, Feb. 25, 2014

Your password is your key to access important personal information both on your computer and online. Should criminals or other perpetrators discover your password, a wide variety of consequences ranging from loss of privacy to identity and credit theft can ensue. Fortunately, creating an effective and memorable password is fast and easy, and these tips will help your ensure your information remains protected.

What makes a strong password

Make it lengthy. Your passwords should be 8 or more characters in length; 14 characters or longer is ideal.

Combine letters, numbers, and symbols. The greater variety of characters that you have in your password, the harder it is to guess. Other important specifics include:

- **The fewer types of characters in your password, the longer it must be.** A 15-character password composed only of random letters and numbers is about 33,000 times stronger than an 8-character password composed of characters from the entire keyboard.
- **Use the entire keyboard, not just the most common characters.** Symbols typed by

holding down the “Shift” key and typing a number are very common in passwords.

Use words and phrases that are easy for you to remember, but difficult for others to guess. The easiest way to remember your passwords and pass phrases is to write them down. Contrary to popular belief, there is nothing wrong with writing passwords down, but they need to be adequately protected in order to remain secure and effective.

Use these steps to develop a strong password:

1. Think of a sentence that you can remember. This will be the basis of your strongpassword or pass phrase. Use a memorable sentence, such as “My son Aiden is threeyears old.”
2. Check if the computer or online system supports the pass phrase directly. If you can usea pass phrase (with spaces between characters) on your computer or online system, doso.
3. If the computer or online system does not support pass phrases, convert it to a password. Take the first letter of each word of the sentence that you’ve created to create a new, nonsensical word. Using the example above, you’d get: “msaityo”.
4. Add complexity by mixing uppercase and lowercase letters and numbers. It is valuable to use some letter swapping or misspellings as well. For instance, in the pass phrase above, consider misspelling Aiden’s name, or substituting the word “three” for the number 3. There are many possible substitutions, and the longer the sentence, the more complex your password can be. Your pass phrase might become “My SoN Ayd3N is 3 yeeRs old.” If the computer or online system will not support a pass phrase, use the same technique on the shorter password. This might yield a password like “MsAy3yo”.
5. Finally, substitute some special characters. You can use symbols that look like letters, combine words (remove spaces) and other ways to make the password more complex. Using these tricks, we create a pass phrase of “MySoN 8N i$ 3 yeeR$ old” or a password (using the first letter of each word) “M$8ni3y0”.
6. Test your new password with Password Checker. Password Checker is a non-recording feature on this Web site that helps determine your password’s strength as you type.

For more information on password security, make sure to check out these sites:

- http://www.microsoft.com/protect/yourself/password/create.mspx
- http://netsecurity.about.com/cs/generalsecurity/a/aa112103b.htm
- https://kb.ucla.edu/link/145

Reference:

http://www.microsoft.com/protect/yourself/password/create.mspx

Intrusion Detection Systems Information

Intrusion Detection Systems (IDS) have many approaches. This page is intended to document the different approaches and reference places where more information can be obtained.

Intrusion Detection Systems — http://en.wikipedia.org/wiki/Intrusion_detection_system
Intrusion Prevention Systems — http://en.wikipedia.org/wiki/Intrusion-prevention_system
Host-based IDS — http://en.wikipedia.org/wiki/Host-based_intrusion_detection_system
Application Protocol-based IDS — http://en.wikipedia.org/wiki/Application_Protocol-based_Intrusion_Detection_System
Network IDS — http://en.wikipedia.org/wiki/Nids

Where can I go to find out more information on viruses, worms, trojans, spyware, hoaxes, etc...

I like going to these sites:

- Sophos
- Symantec
- McAfee
- Cert

BruinTech http://www.bruintech.ucla.edu/security_virus.htm provides a number of links to further information and products.

Phishing protection

Applications that offer phishing protection:

Standalone

- Thunderbird (1.5+) – warns you if a e-mail looks like a phishing e-mail

---

Web-based

- (Add stuff here)

Why shouldn't I email or post Microsoft Word documents?

Many people send Microsoft Word documents as email attachments without realizing that there are several security risks.

- some viruses specifically target Microsoft Word files
  - Microsoft Word vulnerability gives hackers a backdoor May 24, 2006
- earlier versions and edits of your document are often contained in documents. See this article by security expert Bruce Schneier for more details. http://www.schneier.com/crypto-gram-0308.html#8
- using .PDF instead provides a smaller, and usually non-editable file, preventing hijacking of ‘official’ document templates
- if you must use MS Word, download and use the Remove Hidden Data tool from Microsoft
- if you need an editable version save it as RTF (Rich Text Format), which can be imported into almost every word processing program and won’t contain scripts or macros.

How can I make more secure passwords that I can still remember?

This link below leads to a few simple systems described in a paper titled “Simple Formula for Strong Passwords: Dramatically Increase Information Security with Minimal Training, and Without Costly Infrastructure Changes.” (It’s a 42 page PDF.)

- http://www.sans.org/rr/whitepapers/authentication/1636.php

Slightly off topic, but if you must write a password down, see if you can write only part of it, just enough to help you remember the rest.

Related Reading

- http://xkcd.com/936/ – in comic form
- Lock IT Down: Creating passwords that are secure and easy to remember
- Creating Secure Passwords
- A Future-Adaptable Password Scheme
- http://www.lightbluetouchpaper.org/2011/11/08/want-to-create-a-really-strong-password-dont-ask-google/

If anyone has other suggestions, please add them.

See https://kb.ucla.edu/link/1037

What is PGP? Where can I get more info?

What is PGP?

PGP (“Pretty Good Privacy”) is a powerful, free crypto package. PGP lets people exchange files in a private, encrypted format, and also provides message authentication (to an extent).

If you have an encryption key for sending and receiving email, you can publish the public key for it in the UCLA key directory at:
http://keys.ucla.edu/vkd/GetUploadKeyScreen.event

For discussion of PGP, see the newsgroup alt.security.pgp. A FAQ is also available for this newsgroup at:
http://www.faqs.org/faqs/pgp-faq/

The Electronic Privacy Information Center is a good resource on privacy issues. Visit the EPIC Online Guide to Privacy Resources web site at:
http://www.epic.org/privacy/privacy_resources_faq.html

The PGP commercial product is available at:
http://www.pgp.com/

The open source equivalent of PGP, GnuPG, is available at:
http://www.gnupg.org/

Are there any security requirements for connecting a device to the UCLA network?

Please see UCLA’s Minimum Security Standards for Network Devices UCLA Policy 401

From: Associate Vice Chancellor Jim Davis, Office of Information Technology

Sent: Monday, July 17, 2006 6:00 PM

Subject: Minimum Security Standards for Network Devices

UCLA Office of Information Technology

Deans, Directors, Department Chairs and Administrative Officers

A minimum security standards policy for all devices connecting to the UCLA network has gone into effect as part of an ongoing initiative to enhance the security and privacy of UCLA’s electronic data and resources. UCLA Policy 401 focuses on the security of individual devices connecting to the UCLA network â” including, but not limited to, laptop and desktop computers, printers, specialized medical and research instruments, and PDAs. Policy 401 articulates standards for software patch updates, anti-virus software, host-based firewall software, passwords, authentication, email relays, proxy services, and physical security. This policy is pursuant to the draft minimum standards policy that you were informed of in June 2005.

This policy has implications for faculty, non-IT staff, and students. Specifically, anyone who maintains a computer that connects into UCLA’s network is responsible for compliance with this policy in order to connect. For example, a student, faculty or staff member who uses a personal computer in his or her home for work would be responsible for ensuring that the system complies

with the minimum standards. A device that is not compliant or for which there is not a security plan may not be permitted to connect.

UCLA Computing Support Coordinators, Network Coordinators, Help Desk Consortium members, System Administrators and unit CIOs have a primary role and responsibility in the implementation, enforcement and ongoing support of this policy within their units. However, it must be understood there are many devices for which the user, not the support staff, will have the primary responsibility for compliance.

The new policy was emphasized to departmental technologists in May in order to give them an opportunity to ask questions and make suggestions about the policy and its implementation. Many of the campus technologists were already familiar with the policy through their participation in working drafts circulated during the policyâ™s development and are now working to bring their units into compliance.

UCLA Policy 401 can be found at:
http://www.adminpolicies.ucla.edu/app/Default.aspx?&id=401.

Sincerely,

Jim Davis
Associate Vice Chancellor
Office of Information Technology

What is UCLA ASTF and who are its members?

The Applied Security Task Force issues advisories on IT vulnerabilities, threats, patches and other security issues as information becomes available. The advisories are generally sent to Computing Support Coordinators and the Help Desk list. If you are not on either of these listserves, but would like to receive Security Advisories, contact the ASTF at: safecomputing@ucla.edu.

It also includes RSS feeds.

- http://www.appliedsecurity.ucla.edu/
- http://www.appliedsecurity.ucla.edu/taskforce.htm
- http://www.appliedsecurity.ucla.edu/members.htm

Kerberos

- **Kerberos**
  - http://web.mit.edu/kerberos/www/
  - Apple’s Introduction to Kerberos [Part 1 http://www.afp548.com/Articles/Panther/kerberos1.html] and [Part 2 http://www.afp548.com/Articles/Panther/kerberos2.html] – *very useful*

Anti-virus, firewall and Internet security software

- **AVG Anti-virus** – free; anti-virus
- **Microsoft Security Essentials** – Free anti-virus and anti-spyware from Microsoft. Supercedes Windows Defender (see below). Also, Security Essentials definitions
- **Microsoft Windows Defender** – Free anti-spyware from Microsoft. Best designated for Windows XP sp3 machines. Included in Windows Vista and Windows 7, and not compatible with Windows 2000. Also, Windows Defender definitions
- **Norton Internet Security** – non-free; anti-virus, firewall, spam/phishing protection, parental control
- **Sophos Anti-Virus** – shareware; anti-virus. Full version free to UCLA students, staff, and faculty for all Windows versions & Mac OS versions via BOL's software area.
- **ZoneAlarm** – free for non-commercial use; firewall

For general info on securing your PC/Mac you might want to check out:

- http://www.scribd.com/doc/48356630/MakeUseOf-com-HackerProof-Your-Guide-to-PC-Security

Where can I download Sophos Anti-virus and how do I install it?

Sophos Anti-virus is offered to all faculty, staff, and students at UCLA. Sophos is offered by BOL and can be downloaded at this link:

https://www.it.ucla.edu/bol/software-downloads/sophos-antivirus

National Vulnerability Database

National Vulnerability Database is a comprehensive cyber security vulnerability database that integrates all publicly available U.S. Government vulnerability resources and provides references to industry resources.

- “USERS POPULATE THE VULNERABILITY DATABASE
  A database of computer vulnerabilities created by the National Institute of Standards and Technology (NIST) has proven extremely popular, both for reporting new problems and for researching existing ones. Since its debut one year ago, the National Vulnerability Database receives hits at the rate of 25 million per year and has grown from 12,000 vulnerabilities to 20,000, with new ones being reported regularly. According to Peter Mell, senior computer scientist at NIST, who created the database, “I think 20,000 is just the tip of the iceberg.” The database categorizes vulnerabilities by product and version number, directing users to resources to fix the problems. The database uses the Common Vulnerability Scoring System to rate the severity of each vulnerability recorded. Alan Paller, director of research at the SANS Institute, noted that a significant portion of the most recently reported problems affect Web-based applications. Federal Computer Week, 31 October 2006" – source Educause Edupage Listserv

- Security database: The hits just keep on coming – Federal Computer Week – Oct. 31, 2006

Norton Antivirus causes email sending problems

The outgoing email scanning function in Norton Antivirus is usually turned on by default. Individuals who use NAV should be aware that the scan does not support SSL. Please do not be alarmed if the following message occurs:

Unable to establish a SSL connection with the server. Account: ‘SSCNET’, Server: ‘mail.ucla.edu’, Protocol: SMTP, Server Response: ‘454 TLS not available due to temporary reason’, Port: 25, Secure(SSL): Yes, Server Error: 454, Error Number: 0×800CCC7F.

Simply turn off the outbound scanning feature and the email client using SSL can send mail again. See NAV help files to disable scanning feature (instructions will vary based on different versions).

UCLA pays for Sophos, so that is what I use. However, Notre Dame uses Norton, so here are some instructions from its site:

Notre Dame Norton AV Instructions

New UC guidelines on Encryption

The best way to protect data is to not have it. However, restricted data should be retained only when it is necessary but if you must keep sensitive data, the University requires encrypting it. The purpose of encryption is to prevent unauthorized access to data while it is either in storage or being transmitted. For example, encryption can protect the privacy of restricted data that is stored on a laptop computer, even if that laptop computer is stolen. Similarly, it can protect data that is transmitted, for example, over a network, even if that network is tapped by an unauthorized third party.

In April, 2006, UCOP's Information Resources and Communications released guidelines for encryption and announced an agreement with Pointsec to provide the University with encryption tools for PCs, smartphones, PDAs, removable media such as CDs and flash drives, and management tools for those who have to look after all these various devices.

As the guideline states "Encryption is not, however, a panacea. It is not a substitute for other security measures, such as authentication, authorization, and access control, and must be used in conjunction with those other measures." The guidelines provide information on developing strategy at the local level to use encryption effectively.

Preventing SSH Dictionary Attacks With DenyHosts

From the tutorial:

“In this HowTo I will show how to install and configure DenyHosts. DenyHosts is a tool that observes login attempts to SSH, and if it finds failed login attempts again and again from the same IP address, DenyHosts blocks further login attempts from that IP address by putting it into /etc/hosts.deny. DenyHosts can be run by cron or as a daemon. In this tutorial I will run DenyHosts as a daemon.”

http://www.howtoforge.com/preventing_ssh_dictionary_attacks_with_denyhosts

Security Engineering - free e-book

Free online copy of a good and comprehensive computer security book: Security Engineering: A Guide to Building Dependable Distributed Systems.

“If you’re even thinking of doing any security engineering, you need to read this book”
Bruce Schneier

How do I obtain Sophos Anti-Virus Software at UCLA

UCLA has negotiated an agreement with Sophos for all of their anti-virus products for desktop and gateway servers. The software is available to all UCLA students and employees at no charge for home and work computers:

https://www.it.ucla.edu/bol/software-downloads/sophos-antivirus

Department IT Administrators (only) may request a username and password to download desktop and gateway anti-virus products directly from Sophos via this link:

https://www.it.ucla.edu/bol/software-downloads/sophos-antivirus-ucla-it-administrators

For questions on specific components of the license or availability of updates, please contact Bruin OnLine directly at consult@ucla.edu or (310) 267-4357.

Uninstalling Norton Antivirus

To install Sophos you must first remove your current anti-virus program. These instructions to uninstall Norton Antivirus for Windows.

- Go to Start>Settings>Control Panel
- Once in the Control Panel double-click on Add/Remove Programs
- Look for any items referencing either “Norton” or “Symantec” (example: “Norton Antivirus 2003” or “Symantec Script Blocker” or “Symantec Live Update”); click on the item and the select Change/Remove or Add/Remove. Follow the instructions for removing the software.
- After you finish check to make sure that there are no more any “Norton” or “Symantec” references.
- (Optional) Remove the directories used by Norton:
  for example: c:\Program Files\Norton Antivirus or c:\Program Files\Symantec etc.

If you still have trouble installing Sophos, check the Symantec website for more information on how to uninstall Norton Antivirus:
http://service1.symantec.com/SUPPORT/nav.nsf/docid/2001092114452606

I need a free file encryption software

TrueCrypt is a simple, easy-to-use, on-the-fly encryption program. It works on Windows 2000/XP/2003 and Linux.

Some features include:

1. Ability to encrypt entire hard disk partition or a storage device
2. Creation of a virtual encrypted disk within a file that mounts as a real disk.
3. Encryption using AES-256, Blowfish (448-bit key), CAST5, Serpeant, Triple DES, and Twofish.

For a more information, please visit:
TrueCrypt

_

UCLA offers PGP WDE (whole disk encryption) free to all departments. It is cross platform, has central key management (for recovery!), and there are staff to assist implementation:

- **http://itsecurity.ucla.edu/encryption_home.php**

Crashed PGP encrypted disks can be recovered by **DriveSavers**:

- **https://kb.ucla.edu/link/364**

Is there a free Anti-Virus software for Windows XP 64-bit?

Sophos 6.x supports 64-bit Windows XP, but according to Bruin Online, the earliest it will become available as a download/update is Spring 2007. Campus users still need to upgrade from Sophos 4.x to Sophos 5.x before UCLA releases Sophos 6.×.

During this transitional phase, 64-bit Windows users can try the personal version of AVAST Anti-Virus Software. Though I haven’t tried it, many of my colleagues really like this product.

Visit AVAST for more information.

Mikey

UCLA Multi-Factor Authentication

For Google Apps for Education (g.ucla.edu)

Since Google Apps authentication is done using UCLA Single Sign On (SSO), turning on 2-step verification through your Google Apps account settings won't have the intended behavior. If you'd like to add multi-factor authentication protection to your Google Apps account you'll want to turn on MFA for your UCLA Logon ID.

For UCLA Logon ID

All employees including student workers are required to enroll in MFA as of October 31, 2017 MFA is available as an option to all other UCLA Logon account holders (i.e. students, alumni, retirees, contractors, etc.) but is opt-in.

See https://www.it.ucla.edu/security/resources/mfa-at-ucla for more information.