



Digital Forensics Solutions

Electronic Pickpockets Are Right Behind You

Andrew Case – Senior Security Analyst



Who Am I?

- Senior Security Analyst at Digital Forensics Solutions
 - Also perform wide ranging forensics investigations
- Volatility Developer
- Former Blackhat, SOURCE, and DFRWS speaker
- Computer Science degree from UNO
- GIAC Certified Forensics Analyst (GCFA)

Agenda for Today's Talk

1. Secure Web Browsing / Web Usage
2. Social Engineering
3. Computer Security Awareness



Secure Web Browsing



Rule #1

- Do not use Internet Explorer (ever)
- “The number one browser for downloading another browser”
- Has limited built-in security features
 - No plug-in system to let users create their own security protections (more on that later)

Set HTTPS as Default

- For Firefox:
 - <http://www.eff.org/https-everywhere>
 - Rewrites HTTP requests to force loading of all contents through HTTPS
- For Chrome:
 - There are plugins, but they are fairly useless
 - Plugins cannot rewrite requests
 - Chrome greatly restricts what plugins can do (this will keep being an issue as we go on)



Understand SSL Certificates

- SSL Certificates are signed by the website which wants to offer you a secure connection
- Unsigned certificates or improperly created ones will cause your browser to warn you
- Ignoring these warnings can lead to compromise of account information / data entered into forms



Firefox Example Warning



Secure Connection Failed

www.vedetta.com uses an invalid security certificate.

The certificate is not trusted because it is self signed.

(Error code: sec_error_ca_cert_invalid)

- This could be a problem with the server's configuration, or it could be someone trying to impersonate the server.
- If you have connected to this server successfully in the past, the error may be temporary, and you can try again later.

[Or you can add an exception...](#)



Webmail

- Webmail is (obviously) done through the web browser and is subject to the related security concerns
- Each webmail service needs to be configured for optimal security
- All services SSL the initial login, but further actions are sometimes done insecurely



Gmail

- SSL is not enabled by default when using web mail
 - “Settings -> General -> Browser Connection” then set to “Always use https”
- If POP/IMAP are not needed:
 - “Settings -> Forwarding and POP/IMAP” and choose “Disable POP” and “Disable IMAP”



Yahoo Mail

- SSL is used for login, but not for viewing messages
 - Means anyone reading your network traffic can see your emails
 - Not recommended for accounts with any sensitive data (migrate to Gmail)
- Attempts to manually force SSL for viewing, worked, but with issues
 - Invalid certificate and pages loaded slowly
 - Does not seem to be officially supported

Hotmail

- Uses SSL for login
- (Maybe?) has a “Connect with HTTPS” option for viewing messages and other info over SSL
 - Means all interactions with service will be secure
 - Some guides said it was only for the paid version, if true, migrate to Gmail



Managing Email Accounts

- Use multiple E-mail accounts
 - One for personal information
 - One for friends/family
 - One for unknown/un-trusted websites (forums, games, etc)
- Use “throw away” email accounts
 - 10minutemail.com
 - Firefox users can use the *Spamavert* plug-in



Securing Your Browser



Whitelist Javascript/Java/Flash

- No reason for random websites to be able to load arbitrary code/apps on a webpage
 - Security hazard
- Firefox users, use NoScript:
 - <http://noscript.net/>
- Firefox users, use NotScripts:
 - Not as powerful as NoScript due to lack of Chrome plugins capabilities



“Web Developer” Plugin

- The purpose of the plugin is to help web developers debug their pages / code
- Also contains a number of other features that can be used for security
 - Disables caching of files
 - Disables sending of referrers



Protecting Proxy Settings

- Web proxies forward HTTP/HTTPS requests for clients
 - Can monitor and edit all traffic
 - Very useful for performance boosts and security restrictions
- Malware/Ad-ware often attempt to change browser proxy settings to their own malicious proxy server
- Firefox – BrowserProtect



Ad Blocking

- The large majority of web-based malware is served through advertisements
- Advertising companies have more data on you than you want to think about
 - Their “opt outs” are generally useless
 - Deleting opt-out cookies re-enables you in their tracking systems



Ad Blocking Cont.

- Blocking advertisements is the best way to avoid these problems
 - Plugins allow for selective enabling in order to help support websites you trust
- Adblock Plus is most useful plugin in this arena
 - Originally for Firefox, supports Chrome with caveats



Secure Facebook Usage



Privacy Settings

- Facebook has terrible track record with privacy
- Don't put anything on Facebook that you don't want public
- No need to list your phone, address, etc on there
- Do not add friends that you do not know!



Controlling Private Settings

- Account -> Privacy Settings
- Choose the “Friends Only” option



More Privacy Settings

- “Connecting on Facebook” -> View Settings
- Set these to friends only:
 - See your friend list
 - See your education and work
 - See your current city and hometown
 - See your likes, activities and other connections

Privacy from Applications

- Account -> Privacy Settings -> “Apps and Websites”
- Click “Edit Settings” next to “Info accessible through your friends” and uncheck all boxes
- Click “Edit Settings” next to “Instant personalization” and ensure it is unchecked
- Set “Game and app activity” to friends only
- Uncheck “Public Search”



Photo Album Privacy

- Photo privacy is the most important setting on Facebook
- When creating an album, you are given the initial choice
 - Set to “Friends Only”
- Once created, view the album and click “Edit Album”, the same privacy choice will appear
- Can also hide entire albums from certain people (blacklist)

More Photo Privacy

- Unfortunately, lax privacy by your friends can lead to exposure of your tagged pictures
- Tell your friends to secure their account or untag yourself from their albums



Turn on SSL

- Account -> Account Settings -> Account Security -> Secure Browsing
- Will make all HTTPS communication encrypted
- This make break some applications and games that have not upgraded
 - Don't use them

Risks from Applications

- Facebook applications (can) have complete actions over a user's profile and its data
- Only install applications that you trust!
- Periodically review your installed application and remove unused ones
 - Account -> Account Settings -> Apps, Games, and Websites -> Apps you use



Facebook “Viruses”

- Many fake applications (viruses) go viral on Facebook due to people installing them
 - Incentive for malware writers is \$ through advertising campaigns
- Risks to end-users (besides embarrassment)
 - Applications can access profile data/pictures/etc
 - Sites that the applications redirect to likely are hosting malware
 - One virus installation will be used as a catalyst to attack friends’ accounts



Facial Recognition

- Facebook has a new feature that will scan uploaded pictures and attempt to locate your friends in them
- Can then be used to automatically tag them
- All users are included in this system by default
- Opt-out using these instructions:
 - <http://bit.ly/FBoptout>



Secure Twitter Usage



Shortened Links

- Twitter has a 140 character limit on messages
- Led to an explosion in the use of shortened URLs
 - Turn long URLs into 9-15 characters
 - Shortening service handles redirection
 - Security hazard because, by default, there is no way to know where the redirect leads
- Extensions for Chrome and Firefox to preview links before clicking them
 - NoRedirect

OAuth Authentication for Apps

- Applications should never ask you for your password
- OAuth provides the ability to give temporary access to your portions of your account, without giving credentials
- Only authorize applications that use OAuth to access your account

Enable HTTPS

- Sound familiar?
- Go to: Settings -> HTTPS Only



Why HTTPS Matters

- The issue with websites logging you in with SSL but then not encrypting the rest is that your session can be hijacked
 - People sniffing the network can steal your authentication tokens and data
- See:
 - <http://codebutler.com/firesheep>
 - <http://erratasec.blogspot.com/2010/10/re-firesheep.html>



Social Engineering



Basics

- Social Engineering attacks target humans instead of networked resources
- Highly successful due to people's general willingness to be over helpful, combined with lack of security awareness
- Real world breaches have occurred for years with little impact on the general population's resiliency



Main Attack Types

- Email (Phishing)
- Phone Calls
- In-Person
- Postal Mail



Email (Phishing)

- Normal Phishing:
 - A generic email is sent to a large group of people in hopes of enticing them to click a link, fill out form information, reply with sensitive data, etc
- Spear Phishing:
 - Information is gathered on a specific person or people
 - Emails sent contain very targeted information



Email Attack Vectors

- Malicious websites
 - Compromise a user's browser upon clicking
 - Fake/mirrored web pages that harvest credentials
- Attachments
 - Executables (yes this still works)
 - Malicious documents that can exploit vulnerabilities in Office, Adobe, etc

Phone Calls

- Simply calling people can reveal a lot of information
- Targeted calls inside an organization can lead to people that do not normally interface with clients
 - Their guard is down
 - Do not receive as much training on what information is not to be revealed



Phone Attack Example

- Find the internal phone number/extension of an IT employee
- Spoof a phone call (a number of cell phone apps will do this) as the IT employee to target employee
- Tell them their computer has been compromised and you need to access it
- Eventually receive username and password



In-Person

- A number of attack vectors are available when physical contact can be made
- Combines computer security attacks with security awareness of employees



Example In-Person Attack

- Walk into lobby, tell receptionist you want to apply for a job, but your resume is on a thumb drive
- Your thumb drive is configured to auto run executable when plugged in
- Receptionist's computer now compromised



Postal Mail

- A great method to get unfiltered access to a target employee
- People who mail electronic data are generally considered less technical
 - Target's guard goes down



Postal Mail Attack

- Create a “resume” that is actually an executable file
- Hide file details:
 - Make the filename really long so that the “exe” extension won’t show in Explorer
 - John-Smiths-resume-for-manager-position-June-21-2011.exe
 - Edit the icon to be that of PDF or DOC
- Mail resume on a CD with printed cover letter
- Computer compromised once the “resume” is opened



Real World Consequences

- The ease of social engineering combined with the value of the information / access gathered makes it a highly prized attack vector



RSA

- RSA is a large company that provides hardware and software for two factor authentication
 - Clients include hundreds of government agencies and large/medium sized businesses
- Their network was recently breached and information related to authentication stolen
- A number of large defense contractors compromised as a result

Epsilon

- Is the largest online direct marketing provider
 - Handles online advertising services (through email) for numerous large companies
- Information related to Epsilon's clients and the email addresses of previous advertisement receivers was compromised through spear phishing
- How many email notifications did you get after this attack?



US Government Officials / Military

- In June, Gmail disclosed spear-phishing attacks against a number of US officials and military officers
- Compromised files included joint statements between countries and private correspondence



Oak Ridge

- In April, Oak Ridge was compromised through phishing
- Led to shutdown of entire network
- Lots of interesting information to steal from there...

Security Awareness



Password Security

- **Establish and Maintain Secure Passwords!!!!**

Create your passwords using these tips

- 1) Use at least 10 characters
- 2) Use a mix of upper and lower case letters, numbers, and special characters
- 3) Do not base it on words in the dictionary
- 4) Do not repeat words
- 5) Do not use info like your birthday, child's name, middle name, or any other personal information

Password Security Cont.

- Do NOT re-use the same password everywhere
 - At least use different ones for every email, online banking, etc account
- If you have a security breach (virus, malware) then change your passwords
 - Boring malware can quickly harvest all your stored passwords
 - Advanced malware can pull passwords still resident in-memory after you leave a website



Personal Wireless Security

- Set an encryption key on your router!
- Do not use WEP
 - Might as well make it unsecured
- Do use WPA2
 - Assuming a strong passphrase, is currently ‘uncrackable’ outside of bruteforcing
- Do use MAC address filtering
 - Easy to maintain if number of devices in household are static



Public Wireless Security

- Do not use un-encrypted wireless connections for private communications, unless you:
 - Best - Use a (forced-tunnel) VPN
 - Better - Force SSL on all web pages
 - Remember web mail caveats!
 - Triple check certificates!
- Make sure firewall is set to block 'local' traffic
- Turn off file sharing



Public Terminal Security

- Many libraries, hotels, and other public buildings have public computers
 - Only use them as a last resort
 - If you have no choice but to access email or other accounts on them, you **MUST** change your password ASAP after



Protecting Sensitive Data-at-Rest

- If data is sensitive, it needs to be encrypted
- Whole-disk encryption is obviously most inclusive
 - Also most difficult to setup and maintain
- Truecrypt provides the ability to create an encrypted “filesystem” within a normal file
 - Upon successful password enter, the file is mapped to a drive letter



Disposing of Hardware / PC Repair

- Do NOT just recycle or give away your computers or other electronic media (cell phones, cameras, etc)
- Forensics analysis can recover (almost) all of your data!
- On an individual level this can lead to identity theft, stolen accounts, loss of private info, etc
- On a business level can lead to loss of IP, client info, and serious fines from regulations



Proper Disposal

- There are ways to securely erase data while keep the hard drive and the rest of the computer usable
- Can be done through either software or specialized hardware
- Many products on the market that claim secure deletion are bogus
- Make sure your secure deletion is done through a reputable/proven company



Questions/Comments?

- Contact:
 - andrew@digdeeply.com
 - @attrc
- Company:
 - <http://www.digitalforensicssolutions.com>
 - <http://dfsforensics.blogspot.com>
 - @dfsforensics

