Security and Privacy Are NOT Mutually Incompatible

Joe St Sauver, Ph.D.
(joe@uoregon.edu or joe@internet2.edu)
Internet2 Security Programs Manager
Internet2 and the University of Oregon

Joint Techs, Lincoln Nebraska
July 21st-23rd, 2008

http://www.uoregon.edu/~joe/security-and-privacy

Disclaimer: All opinions expressed are solely those of the author and do not necessarily represent the opinions of any other entity.

1. Introduction

Why Talk About Security and Privacy at JT?

- There's a temptation to think about **privacy** as being strictly a **policy** sort of topic. If that were true, Joint Techs would not be the right place for this talk, since Joint Techs is a technical conference, not a policy one.
- However, by the time we're done talking, I hope you'll also agree that significant **technical** issues run inextricably through the topic of privacy, and thus privacy **is** something that we should -- and must -- be thinking and talking about in technical fora, including this one, although we're not going to be able to cover all relevant topics at even a superficial level in just twenty minutes!
- The other question that may be rumbling around in the back of your mind may be, 'Why is a **security** guy talking about **privacy**? I thought the privacy and security guys were always "at war" with each other?' Not so!

Confidentiality *Is* An Integral Part of Security

- Information security is usually described as having three overarching goals (forming the mnemonic "CIA"):
  -- **C**onfidentiality,
  -- **I**ntegrity, and
  -- **A**vailability.
- Many of us might be tempted to think that "confidentiality" is synonymous with "privacy," but in the security community, the two terms are customarily differentiated. **Privacy relates to people, confidentiality relates to data.** (see, for example, "Privacy vs.Confidentiality:What's the Difference?," at slide 6, http://www.mcg.edu/audits/documents/PrivacyvsConfidentiality-March2008forHACfinalversion.ppt)
- But when **data contains information about people**, at that point privacy and confidentiality become inextricably intertwined, and that brings the privacy topic squarely within the scope of an information security.

Is Now The Right Time To Talk About Privacy? Why Not Talk About It Next Time?

- Online privacy seems to be popping up everywhere right now, and even Google has (finally!) added a "Privacy" link to their notoriously high speed/low drag minimalist homepage!
- Or check the news. It seems as if every time you look at the news, there is some new news story describing how someone's privacy has been breached, or all of our privacy is about to be breached due to some new online phenomena.
- The Hill has also been extremely busy in privacy-related areas. For example, Congress has been holding many hearings concerning Internet privacy, while also passing legislation which potentially affects privacy, including 43 pages worth of amendments to FISA, the statute governing the United States' foreign intelligence surveillance programs.

"Whoa! I *Don't* Want To Help The Badguys!"

- **Trust me, none of us do!** But privacy isn't just about terrorists or drug smugglers who may criminally exploit the freedoms that we all enjoy (and I've tried to be very careful to keep anything that even *might* help them out of this talk)
- Privacy is about protection **from** the criminals who want to steal our financial information or our identities. Privacy is also about securing the medical and other data that must be kept confidential as a **matter of law**. And privacy is about taking technical steps to keep plain text from being **sniffed** on the wire, or diverted and **man-in-the-middle**'d.
- Privacy is also about resisting the unbounded accumulation of data about who we are, where we live, what we read, how much we have in the bank, and how we handle our medical conditions, our sexual preferences, our political leanings, and our religious inclinations (or lack thereof).

And Make No Bones About It, Our Privacy IS Under Concerted Attack

- **Miscreants** now target data, rather than systems per se, and phishing, carding and identity theft are the all-too-common result.

- Since the terrible tragedy of 9/11, **some in our government** have questioned whether we can even have **privacy *AND* security** at the same time.

- Many **Internet advertising companies** are embarking on increasingly intrusive online data collection programs -- but in doing so, their actions raise grave privacy concerns.

- Or how about maintaining your privacy while **traveling?** it seems as if our privacy is under attack **everywhere we may go, and maybe even when we're on our way home…**

2a. Attacks on Our Privacy: Criminal…

Identity Theft

- *"Ten million Americans a year fall victim to **Identity Theft, the fastest growing white collar crime in the country**. Operating across state and national borders, identity thieves cost U.S. business and finance at least $50 billion a year in fraudulent transactions."* [May 26, 2004, www.ustreas.gov/press/releases/js1690.htm]

- *The Federal Trade Commission today issued its annual report, "Consumer Fraud and Identity Theft Complaint Data" on fraud complaints consumers have filed with the agency. **For the seventh year in a row, identity theft tops the list,** accounting for 36 percent of the 674,354 complaints received between January 1 and December 31, 2006.* [www.ftc.gov/opa/2007/02/topcomplaints.shtm]

"Banks Claim Credit Card Breach Affected 94 Million Accounts"

- **"**More than **94 million accounts** were affected in the theft of personal data from TJX, a banking group has alleged in court filings, more than twice as many accounts as the retailer had said were affected in what was already the **largest data breach in history**.

  "The data breach affected about 65 million Visa account numbers and about 29 million MasterCard numbers, according to the court filing, which was made late Tuesday by a group of banks suing TJX over the costs associated with the breach."

  www.iht.com/articles/2007/10/24/business/hack.php
  October 24th, 2007

2b. Attacks on Our Privacy: Governmental…

The DNI on Security vs. Privacy

- *In order for cyberspace to be policed, Internet activity will have to be **closely monitored.** Ed Giorgio, who is working with [Director of National Intelligence] McConnell on the plan, said **that would mean giving government the authority to examine the content of any e-mail, file transfer, or Web search.** "Google has records that could help in a cyber-investigation," he said. Giorgio warned me, "We have a saying in this business: 'Privacy and security are a zero-sum game.' "*

  "The Spymaster," *New Yorker Magazine*, http://www.newyorker.com/reporting/2008/01/21/080121fa_fact_wright?currentPage=all

Schneier's Take On Giving The Government The Authority To Examine Any Email, Etc.

- 'If there's a debate that sums up post-9/11 politics, it's security versus privacy. Which is more important? How much privacy are you willing to give up for security? Can we even afford privacy in this age of insecurity? **Security versus privacy: It's the battle of the century, or at least its first decade.** [* * *] **There is no security without privacy.** And liberty requires both security and privacy. The famous quote attributed to Benjamin Franklin reads: "Those who would give up essential liberty to purchase a little temporary safety, deserve neither liberty nor safety." It's also true that **those who would give up privacy for security are likely to end up with neither.**' Bruce Schneier, "What Our Top Spy Doesn't Get: Security and Privacy Aren't Opposites," 01/24/2008, www.wired.com/politics/security/commentary/securitymatters/2008/01/securitymatters_0124

2c. Attacks on Our Privacy: Commercial…

Privacy and Commercial Firms #1: NebuAd and Deep Packet Inspection (DPI)

Two watchdog groups accused Silicon Valley startup NebuAd June 18 of hijacking Web sites and intercepting users' browsers. NebuAd is an online advertising company that provides targeted advertising for ISPs.

According to a new technical report by Free Press and Public Knowledge, NebuAd uses special equipment that "monitors, intercepts and modifies the contents of Internet packets" as consumers go online. The report found that NebuAd inserts extra hidden code into users' Web browsers that was not sent by the Web site being visited.

In turn, the code directs the browser to another site not requested or even seen by the consumer, where more hidden code is downloaded and executed to add more tracking cookies. Using the secretly collected information, NebuAd serves up ads based on the user's browsing habits.

"Watchdogs Claim NebuAd Hijacking Sites," 2008-06-18, www.eweek.com/c/a/Legal/Watchdogs-Claim-NebuAd-Hijacking-Sites

#2: What You've Watched on YouTube

Not for the first time, a court ruling in a copyright-policy case has made privacy rights an afterthought. Last week, U.S. District Court Judge Louis L. Stanton ruled that Google had to hand over video-viewing records of its YouTube subsidiary to Viacom, which alleges that YouTube built a business on the unauthorized sharing of Viacom's copyrighted works and seeks at least $1 billion in damages.

*As my colleague Ellen Nakashima wrote in Friday's Post, the ruling will require Google to provide its viewing log --**12 terabytes' worth of data** containing **"the unique login ID of the viewer, the time he began watching, the Internet Protocol, or IP, address of the user's computer and the identification of the video."** [continues]*

"Court Invites Viacom to Violate YouTube Viewers' Privacy,"
7/7/2008, http://blog.washingtonpost.com/fasterforward/2008/07/court_invites_viacom_to_violat_1.html

[the parties subsequently agreed to 1:1 pseudonomyze the data]

2d. Attacks on Our Privacy: Abroad… and Coming Back Home?

U.S. Fears Threat of Cyberspying at Olympics

By SIOBHAN GORMAN
July 17, 2008; Page A6

WASHINGTON -- A debate is brewing in the U.S. government over whether to publicly warn businesspeople and other travelers heading to the Beijing Olympics about the dangers posed by Chinese computer hackers.

MORE

- The Department of Homeland Security last month warned of cyber threats facing overseas travelers but did not release the information to the public.
- The U.S. Cyber Consequences Unit assembled sets of guidelines for determining whether you are a likely target of cyber-espionage; how to deliver a presentation without a laptop; and securing your laptop when traveling abroad.

According to government officials and security consultants, U.S. intelligence agencies are worried about the potential threat to U.S. laptops and cellphones. But others, including the State and Commerce departments and some companies, are trying to quiet the issue for fear of offending the Chinese, these people say.

Barack Obama became the first major presidential candidate to propose new

http://online.wsj.com/article/SB121625646058760485.html

During a trip to Beijing in December 2007, spyware programs designed to clandestinely remove information from personal computers and other electronic equipment were discovered on devices used by Commerce Secretary Carlos Gutierrez and possibly other members of a U.S. trade delegation, according to a computer-security expert with firsthand knowledge of the spyware used. Gutierrez was in China with the Joint Commission on Commerce and Trade, a high-level delegation that includes the U.S. trade representative and that meets with Chinese officials to discuss such matters as intellectual-property rights, market access, and consumer product safety. According to the computer-security expert, the spyware programs were designed to open communications channels to an outside system, and to download the contents of the infected devices at regular intervals. The source said that the computer codes were identical to those found in the laptop computers and other devices of several senior executives of U.S. corporations who also had their electronics "slurped" while on business in China. The source said he believes, based on conversations with U.S. officials, that the Gutierrez compromise was a source of considerable concern in the Bush administration. Another source with knowledge of the incident corroborated the computer-security expert's account.

"China's Cyber-Militia," 05/29/08,
http://www.nextgov.com/nextgov/ng_20080529_5500.php

"US Defends Laptop Searches at the Border"

"*Is a laptop searchable in the same way as a piece of luggage? The Department of Homeland Security believes it is.*

For the past 18 months, immigration officials at border entries have been searching and seizing some citizens' laptops, cellphones, and BlackBerry devices when they return from international trips.

In some cases, the officers go through the files while the traveler is standing there. In others, they take the device for several hours and download the hard drive's content. After that, it's unclear what happens to the data.

The Department of Homeland Security contends these searches and seizures of electronic files are vital to detecting terrorists and child pornographers. It also says it has the constitutional authority to do them without a warrant or probable cause.

But many people in the business community disagree, saying DHS is overstepping the Fourth Amendment bounds of permissible routine searches. Some are fighting for Congress to put limits on what can be searched and seized and what happens to the information that's taken. The civil rights community says the laptop seizures are simply unconstitutional. They want DHS to stop the practice unless there's at least reasonable suspicion." [continues]

http://features.csmonitor.com/innovation/2008/07/10/
us-defends-laptop-searches-at-the-border/

A Couple of Notes About That…

- Information, particularly encrypted information, is routinely "imported" and "exported" across national borders without any sort of online "customs control." It seems inconsistent (in my opinion) to see information transferred encrypted over the Internet subject to one standard of inspection (e.g., none), while potentially identical information (albeit on a laptop) receives a completely different level of scrutiny.
- Even if you have no objection to US border agents inspecting your laptop (and I don't), beware! How will you feel if foreign legislatures reciprocally adopt the same laptop inspection standard for your entry into *their* countries, eh? Ugh! [This sort of reciprocity can be routinely seen in other immigration-related areas, such as visa waiver programs (e.g., if you make my citizens get a visa to enter your country, I'll make yours get a visa to enter my country, etc)]

3. What's Needed?

Let's Consider Just A Few Areas
Where You May Be Able to Readily
Improve Your Online Privacy

3a. Identifiers

Online Identifiers and You

- In some cases, **data may be inherently personally identifiable/associated with you**. For example, data may include your name, or SSN, or credit card number
- Other times, data (as in the case of some YouTube records as originally ordered to be released to Viacom), a record may be "just" associated with an **IP address**.
- You, as technical people, understand that an IP address may be statically mapped to one system or one user, and sometimes the rDNS associated with an IP can give a pretty good "hint" about who that person may be, even without any additional information (like DNS registration records). E.G., *4.3.2.1.in-addr.arpa. 86400 IN PTR johnsmith.example.com*
- Sometimes static address will not have rDNS, or the rDNS may be non-descript, or the rDNS may be out of date, or the IP may be used by a NAT box that is shared by many users, or the IP may be from a dynamic pool. In many of those cases, administrator help is need to map IP's to users.

Dynamic Addresses; NAT Gateway Addresses

- In the case of dynamic addresses (such as those handed out from a DHCP pool), in order to map an IP address to a user, you may need not just the IP address to ID a user, but also the timestamp (and time zone) when the IP was seen. Time stamps are necessary because Bill Jones may be using a dynamic IP at one time, while a few minutes later that same IP address may be in use by Sally Anderson. You need accurate time stamps (e.g., NTP sync'ed or better timestamps), with time zone, to map an IP to the right user.
- If an IP address is that of a NAT gateway, not only do you need the IP address and time of an incident, but you may also need additional details about the network traffic that was seen so the NAT gateway administrator can work to identify the correct network session in his or her logs.
- DHCP and NAT logs can grow rapidly, and may only be retained for a limited period of time due to finite disk capacity, so timeliness can also be key.

Usernames; Cookies; Web Bugs in Email

- Other times, a user may actually "log in" to a site, in which case the user (or at least someone with access to that user's credentials) and their activity on the site may be closely trackable, and mappable to an individual if the username used for that service maps to a real identity.
- Sometimes, while a user may not employ a username and password to login to a site, a persistent http cookie may serve to identify that unique user to a web site, and to enable tracking of their behavior. If you haven't looked at the cookies in your web browser's cookie store in some time, you may be surprised at what you find.
- You should also be alert to things like web bugs, or "tracking gifs" in HTML email. A unique customized URL, prerecorded as having been sent to a particular user, may become associated with your IP address when your mail client opens that message and renders that gif; the marketer then knows the email address that may be visiting pages from that IP

Shibboleth

- One of the most promising advances in delivering good quality authentication while simultaneously protecting privacy is associated with the Shibboleth Project.

- Shibboleth is based on federations, making it possible for a partner site to trust another another site to determine that someone is a member of a particular set (such as, “current student at WagonWheel University,”) without knowing WHICH student at WagonWheel University the person may actually be. This is perfect for controlling access to site licensed resources while simultaneously protecting user privacy.

- It is worth noting that even if your school hasn’t yet deployed Shib, ProtectNetwork (http://www.protectnetwork.org/) can serve as a third party identity provider for some scenarios

Simple Suggestions for Enhancing Your Privacy

- Do not read your email with an HTML-aware email client.
- When using a "portal" site such as Google, do not create a username. If you do create a username, minimize the period of time when you use it. When you ***are*** logged in, remember that your activity is easily tracked/trackable by username, rather than just by IP address. (Of course, even when you aren't logged in, your username may still be strongly correlated with your IP address, e.g., in cases where your PC has a static IP or a dynamic address with a long lease).
- Routinely refuse or promptly delete any/all cookies, and use an anti-advertising plugin (such as Adblock for Firefox).
- If you administer your own DNS, you may want to modify your /etc/host file to set known tracking-related domain names to 127.0.0.1

IPv6 and Privacy

- As all of you should now know, we're less than 1,000 days from running out of IPv4 addresses. When adding IPv6 support to your campus network, you should note that IPv6 has some built-in privacy enhancing DNS options, and those options may be on **by default** in some operating systems.

- At the same time privacy may be enhanced by those new IPv6 addressing options, privacy may be inadvertently be compromised if IPv6-enabled hosts end up tunneling IPv6 traffic to v4/v6 gateways of unknown provenance off-site.

- You may want to consider putting together a group of local technical staff just to look at IPv6 and its privacy implications (but don't let doing that slow you down from getting it actually deployed -- time's running out!)

And While We're Talking About DNS

- I hope by now that you're all ALSO aware of VU#800113 (Dan Kaminsky's DNS vulnerability). It is **very** important that you patch your recursive resolvers before August 7th of this year, when he'll be doing a talk about that vulnerability!
- If you're not sure whether you're vulnerable, you can check the status of your resolvers with Duane's cool test point:
  `% dig +short porttest.dns-oarc.net txt`
  (obviously you can also add `@something.whatever.edu` at the end of the dig command to check that additional server,assuming you can get to it from where you're testing). See also https://www.dns-oarc.net/oarc/services/dnsentropy for a pretty cool graphical version of the default tester :-)
- Patching may negatively impact performance for heavily loaded resolvers, and some patches may interact with some firewalls, so look things over carefully before just diving in.

3b. Encryption

Encryption and Content

- While message content is often what folks worry about most when it comes to privacy, ironically message content is perhaps the easiest thing to protect: encrypt it.

- Having encrypted private content, the risk to the confidentiality of that content is dramatically reduced, if not eliminated, although non-escrowed encryption can present its own risks, such as non-recoverable loss of access to data.

- The problem many folks run into is that good quality encryption isn't **routinely and consistently** used.

- You want to encrypt **EVERYTHING** by default.

Even Though We Know Encryption is "Key"

- If I could secretly poll you today (Joint Techs should have audience response clickers!) I bet that there are still many of you who…
  1) allow unencrypted password-based logins to at least one or more application services (such as FTP)
  2) have one or more web-based applications which delivers sensitive traffic over the network without using SSL
  3) have nil usage of PGP/GnuPrivacyGuard (or S/MIME) for email encryption and signing on your campus
  4) have "someone" using WEP as "encryption" on some link on campus (don't! it only conveys an illusion of protection!)
  5) haven't yet rolled out full disk encryption for all systems which touch administrative/sensitive PII information
  6) aren't offering VPN services to the campus community
  7) have campus VoIP traffic, but still aren't encrypting it
  8) have unencrypted SNMP traffic

But Wait, Bad As That May Be…

- There are some areas relevant to advanced applications where production encryption options may be **limited**, **non-existent, or uneconomical**, including:
  -- encryption for **very high bandwidth traffic flows**
  -- encrypted **DNS** (note, **not** talking about cryptographically signing DNS ala DNSSEC, **nor** using a VPN, I'm talking about **encrypting** native DNS query and response traffic)
  -- **encrypted IP multicast** (I'm aware of Cisco's secure IP multicast, see www.cisco.com/en/US/products/ps6552/products_white_paper0900aecd8047191e.shtml but I don't have a good sense of how widely that's employed)
  -- some **mobile devices** may also require optional or third party encryption solutions to handle local storage and/or secure connectivity, which seems crazy to me (hey, mobile devices are quite prone toward being lost, right? and wireless is a broadcast media, eh?), but I'm not a mobile device guy, so what do I know

One *Specific* Encryption Flaw I'll Flag

- Many of you may already know this, but on the off chance not, there was a subtle but **very** important flaw in some Debian and derivate OS version of OpenSSL which reduced the amount of entropy below safe levels. See http://www.metasploit.com/users/hdm/tools/debian-openssl/ for an excellent discussion of the problem and a couple of amusing cartoons.

- Note that if you've accepted OpenSSL keys generated on a Debian system (or an affected variant), regardless of what distro *you're* running, this vulnerability will also affect you.

- Of course, if this vulnerability (from May) did affect you, you're probably already compromised, but then again, maybe the bad guys just haven't found you yet, or maybe its time for a system audit, eh? :-)

3c. Traffic Analysis

Once Your Content Is Well Encrypted…

- Taking privacy to the next level (after you've got your ID managed and your content encrypted is a little harder), because it requires you to deal with network traffic analysis.

- If someone monitoring your traffic can't see the content of your traffic (remember, it is all encrypted now, right?) they **can** at least still see the source where the traffic is coming from and the destination where the traffic is going to, and that's often enough to convey "useful" (albeit potentially privacy defeating) information, even if they don't know anything about the content of the traffic.

- For example, a bank that observed repeated encrypted connections from a teller's work PC to an online gambling web site might conclude that they should check their PC and/or visit with that employee, even if they can't see the details of the encrypted network traffic streams to that site.

Anonymity Networks

- The most common solution to traffic analysis attacks is to introduce an “encrypted anonymity network” which will accept your traffic, route it through an encrypted network of intermediate nodes, perhaps interleaving your traffic with other users traffic, and then eventually dropping it out on the Internet via an exit node located somewhere innocuous (and typically far away from where it originated).
- Anyone monitoring that local user just sees encrypted traffic from the local user to an otherwise undistinguished address (actually the “on ramp” to the anonymity network).
- Tor is one example of a well-known anonymity network, see http://www.torproject.org/
- The problem with using anonymity networks is that from a traffic analytical point of view, simply identifying that an anonymity network may be in use may be enough to raise a “red flag,” and then there’s always the risk that the operator of one or more exit nodes may be untrustworthy.

“Tor Researcher Who Exposed Embassy E-mail Passwords Gets Raided by Swedish FBI and CIA”

“[Dan] Egerstad created a stir three months ago when he posted on his web site the log-in information and passwords for 100 of the 1,000 e-mail accounts for which he obtained log-ins and passwords. (His site is no longer online). He posted the information, he said, because he felt it would be the most effective way to make the account owners aware that their communication had been compromised.

“Initially, Egerstad refused to disclose how he obtained the log-ins and passwords. But then in September he revealed that he'd intercepted the information through five exit nodes that he'd set up on the Tor network in Asia, the US and Europe.

“Tor is used by people who want to maintain privacy and don't want anyone to know where they go on the web or with whom they communicate. Tor traffic is encrypted while it's enroute, but is decrypted as it leaves the exit node and goes to its final destination. Egerstad simply sniffed the plaintext traffic that passed through his five exit nodes to obtain the user names and passwords of e-mail accounts.”

blog.wired.com/27bstroke6/2007/11/swedish-researc.html

A Second Example: UltraReach

"Our five existing tools – UltraSurf, DynaWeb FreeGate, Garden, GPass, and FirePhoenix — currently accommodate an estimated **95% of the total anti-censorship traffic** in closed societies around the world, and are used DAILY by millions of users. These tools have been of benefit to US-based organizations such as Human Rights In China, the Chinese Democracy Party, Voice of America, and Radio Free Asia -- and even companies like Google and Yahoo since we bring the uncensored version of their services into closed societies like China.

"As of January 2008, the Top Five censoring countries with the most average daily hits to our anti-censorship systems are (hits per day): (a) China: 194.4 million, (b) Iran: 74.8 million, (c) Saudi Arabia: 8.4 million, (d) UAE: 8 million, (e) Syria: 2.8 million."

judiciary.senate.gov/testimony.cfm?id=3369&wit_id=7187
May 20th, 2008

4. Conclusion

Is That It?

- That's NOT it. There are still many more privacy things we could talk about, but that's about all the time we have today.
- What IS important is that you realize that privacy is a very hot topic right now, and why.
- Please also remember that you can protect your privacy while not impacting your security, and that there are specific technical areas you should be looking at as part of that work
- Once you've gotten through the three areas I've already called out (identifiers, encryption, and traffic analysis), there are many additional areas we could also talk about, but if you begin to pay attention to even just those three areas, your site will still be far "more private" than average
- And if there ***are*** any policy type folks lurking in the audience, an obvious bit of low hanging privacy-related fruit might be a review of your campus privacy policy, if any.
- Thanks for the chance to talk! Are there any questions?