Asia-Pacific
Economic Cooperation

2006/SOM1/ECSG/SYM/028
Agenda Item: 27

Privacy - Enhancing Tools List

Purpose: Information
Submitted by: Peru

APEC Symposium on Information Privacy Protection in E-Government and E-Commerce
Ha Noi, Viet Nam
20-22 February 2006

CPSR Perú

Ciudadanía y Derechos en la Sociedad de la Información

Information Privacy Tutorial

Katitza Rodríguez, Director of CPSR-Perú

APEC Symposium on Information Privacy Protection in E-Government and E-Commerce

Ha Noi, Vietnam, February 2006

Index

- About CPSR-Perú
- What is Data Protection?
- Identity Theft
- Financial Privacy
- Internet insecurities & Basic internet safety
- E-mail insecurities & Basic safe e-mail.
- Basic safe browsing tips.
- Basic computer and files securities.
- Online Privacy tools

About CPSR-Perú

CPSR-Perú is a public interest research centre of information and communications technology (ICT). Founded in Lima in October of 2002, its mission is to promote the socially responsible use and development of information and communications technologies, highlighting the social benefits that derive from their correct use and guarding against their use for detrimental, socially harmful purposes. CPSR-Peru attempts to influence government policy on ICT and carries out research into the regulation of ICT and their impact on society.

In addition, it provides legal representation for citizens and organizations whose rights to access to the Internet under threat. It is conformed by lawyers and technicians, with strong links with main local universities.

CPSR Perú

About CPSR-Perú

CPSR-Perú is working in privacy and data protection issues **http://www.cpsr-peru.org/privacidad/** from three different perspectives:

- **Academic:** Doing legal research in Peru and Latin America on legislation, regulations, public policies and private practices.

- **Advocacy and public policy at the local, regional and international level:** CPSR-Perú participated at the World Summit of Information Society, Asia Pacific Economic Cooperation Forum, the Ibero American Data Protection Network.

- **Practical:** Researching and organizing workshops on privacy enhancing technologies to protect our online privacy, secure communications and digital information. CPSR-Perú has trainned journalist and human right workers in tools and methods for secure communications and the protection of sensitive data in Latin America: Mexico, Perú, Colombia and Venezuela.

CPSR Perú

What is data protection?

- The fundamental right of the protection personal data recognizes all citizens the faculty to control its personal data and the capacity to arrange and to decide on the same ones. This means that all people have the right to know why and how their data are treated.

- Going online and taking advantage of the technology may require the disclosure and treatment of personal data. Nevertheless, most of the consumers are not aware about this issue.

Data Protection

- CPSR-Perú believed that to assure the privacy of our personal information, consumers must have the protection provided by basic law and law enforcement. However, protected by law or not, we thought consumers needs information to understand the risk associated when they use the technology.
- Consumers needs to be ever vigilant in terms of who gets our data. We need to learn to ask certain questions before giving out our data and to find out which information about us, they had.

Identity theft

- Criminals use personal data in order to theft the identity of another person. Criminal use your **existing credit information** or **open new accounts** in your name.

For example: Criminals use to steal

- ID cards
- Credit and debit card numbers,
- telephone calling cards,
- Find out the date of birth,
- Find out work and personal address.

Financial information

Your credit report is actually a credit history. It may contains information such us:

- Delay payments;
- Information of those to whom you owe money that may report this information to the credit bureau.
- If you do not make credit card, auto loans, or mortgage payments on time.

<u>Information in your report may contains</u>

- Name, address, telephone number, year and month of birth, employment information. Also includes matters of public record such as civil judgments, tax liens and bankruptcies.

CPSR Perú

Enforcing your data protection rights!

- In Perú, you have the right to free access to your credit report once a year or when your information is rectify.
- A creditor has the duty to report only legal, accurate, complete, and updated information to the CB.
- Look in depth your credit report. You have the right to access to your information, modify it or cancel it. An in case the CB gave this incomplete or inaccurate information to a third party, they had the obligation to rectify it.
- In Perú, the liability for the credit bureau is objective if they do not grant the right to access, modify, cancel or rectify the information.

Enforcing your data protection rights!

- Depends on your national law, after a period of time, 5 years in Peru, an in specific cases, negative information that was pay or extinguish, should be delete from your credit report. This is called the right of oblivion or right to be forgotten.

- Filing suit and complaining to government Agencies. If you win, you may be entitled to recover an amount of money for damages.

Internet insecurities & Basic internet safety

- The Internet connects computers to each other over a global network. The computer can be your laptop, your personal or family desktop or your computer at work. The software that your computer runs deliver, in some cases, information about their customers of their web sites.
- Browsers pass along information about the brand of the browser, the version and plug-ins that are available.
- The web server logs include the IP address that identifies “a computer” that visits that site.

Internet insecurities & Basic internet safety

- Cookies create an identity on the Internet but this identity is still tied to a computer, unless you disclose personal information. How? Filling out a form for subscription services, personalizing your site for example with My Yahoo account.
- Companies could triangulate information in order to identity you through the use of outside sources, not only the information you give through an online services.
- It isn't just the data that you give out today that may identify you, it's data that you have given out or that has been gathered about you your entire life.

Internet insecurities & Basic internet safety

- **Anti- Virus**: Install and keep up to date virus protection software to prevent causing problems to your computer or sending out files or another stored information.
- **Keylogger attack:** A “key logger” system can track every keystroke you make. These programs are spread either by someone putting it on your computer while you are away, or through a virus or Trojan you get over the Internet that attacks your system. Key loggers track your keystrokes and report back your activities, usually over the Internet.
- **Intrusions:** Install a firewall on your home computer to prevent crackers from enter to your computer.

E-mail insecurities & Basic e-mail practices

- Your email does not fly directly from your computer to the computer of the intended recipient. It goes through several nodes and leaves behind information as it passes. No matter if you are sending me an email from your computer in this room to my computer here in this room, email flies among several nodes.

Encrypt your email whenever possible

- It is always good to encrypt your email whenever possible. An unencrypted email is like a postcard that can be read by anyone who sees it or obtains access to it. An encrypted email is like a letter in an envelope inside is safe.
- When you are entering to your password of your email, someone can be looking over your shoulder as you type, in order to see your password.
- If your computer are connected to a network your email maybe accessible by everyone else in the office.
- The system administrator may have special administrative privileges to access all emails accounts.

Email insecurities & Basic email practice

- The Internet Service Provider has access to your e-mail. Anyone who has influence over your ISP may be able to pressure it to forward him or her copies of all your email or to stop certain email from getting through.
- As it passes through the Internet your email flows through hundreds of insecure third-parties: crackers can access email messages as they pass.
- The ISP of your intended recipient may also be vulnerable, along with the network and office of your intended recipient.

- **On line service:** Think twice, maybe three times, before signing up (filling a form with lot of personal information) for a web site's services. Be aware that by signing up you are creating an identity. Do you have reason to believe that you can trust the company with your information? Do you think it is necessarily to give to them all the information they are requesting to you?

- **Shopping online:** When shopping online, do business with companies that provide secure transaction platform and that have strong privacy policies. It could be good to do online shopping in countries that have strong data protections laws.

- **Going anonymous:** One of the best ways to protect your privacy is going anonymous. If you wish to maintain some anonymity, you can register for a free web-based e-mail account using fictitious information and then use that address for contact with potentially invasive services.

- If you feel strongly about controlling your identity on the Internet, there are services that can allow you to surf the web either anonymously or pseudonymously. Please see your materials for more information.

- **Passphrase protected:** To avoid someone accessing your computer while you are away, pass phrase protect your computer and always shut off your computer when you leave it. Create passwords that combine 8 numbers and letters, upper and lower case and or symbols.

- **Encrypted data/disk:** If they can get by your pass phrase protection, or if you have left your computer on, your files can still be secure if you encrypt your files. In your materials, you will find tools that help you encrypted your data.

- **Back up:** If your computer is stolen, you can get back your files if you have created a secure backup every day. Keep the encrypted backups away from your office in a safe place.

- **Wipe:** Do not rely on the "delete" function to remove files containing sensitive information. There are ways to recover that information. If you want that your delete files not be reconstructed, please wipe it. There are tools (see your materials) to wipe information. Use that tool instead of just throwing them into the Trash or Recycle Bin.

Privacy - Enhancing Tools List

Email encryption

- PGP
- GnuPG
- S-Mail
- Stealthmessage
- Hushmail
- CryptoHeaven
- MailVault

Disk encryption

- PGP Disk
- DriveCrypt
- BestCrypt

Anonymous Remailer and Surfing

- Anonymizer
- AnonymSurfen
- Anonymouse.com
- Anonymous Remailer
- Tor

Privacy - Enhancing Tools List

DATA STORAGE/Backup

- Martus
- CDRWs (CD read/write)
- Extra hard drive in computer

Backup software

- Retrospect.com
- DIY (Do It Yourself)
- USB, Compact Flash Memory or Memory Stick

Other

- PGP SDA (self decrypting archive)
- S-Mail S-Disk:
- Virtual shredder
- Keyboard popup
- Tempest

Asia-Pacific
Economic Cooperation

2006/SOM1/ECSG/SYM/029
Agenda Item: 27

Privacy - Enhancing Tools List

Purpose: Information
Submitted by: Peru

APEC Symposium on Information Privacy Protection in E-Government and E-Commerce
Ha Noi, Viet Nam
20-22 February 2006

CPSR Perú

Privacy - Enhancing Tools List

Email encryption

PGP – www.pgpi.org (free) or www.pgp.com (paid)

- Pros: trustworthy, free, relatively easy to use, cross-platform, can import and export files from the Web, standard encryption system used by most in the industry
- Cons: free version is not supported, installation not completely intuitive, Key system can be confusing. Key management can be difficult (policy level issues).

GnuPG, the free software version of PGP can be found at www.gnupg.org and is available in several different languages.

S-Mail – www.s-mail.com

- Pros: easy to use web-based email; supports Unicode, which has the capability of displaying characters of almost all languages on the world; integrates with MS Outlook with a plugin.
- Cons: not all features available in free version; developers are of unknown trustworthiness.

Stealthmessage – www.stealthmessage.com

- Pros: free, easy to use, Web-based secure messaging to email; can be used at Internet cafes; has "auto destruct" feature that erases very sensitive messages; 160-bit encryption within 128-bit SSL; can best be used to send a short message to yourself for later pickup, as there is no need to share your "secret code" with anyone else, which makes it a good way to send messages to yourself from the field at an internet café.
- Cons: can only type messages up to 20,000 characters; need to transmit shared password securely or at least separately; lower level of encryption than other systems based on PGP; developers are of unknown trustworthiness.

Hushmail – www.hushmail.com

- Pros: free lite version, supported, trustworthy (due to personal contact), easy to use, Web-based, can be used at Internet cafes, safe key generation; can use with other hushmail users and with "regular" PGP email users.
- Cons: lite/free version users must use every three weeks or account is deleted. Purchase without limitations is available for $30 per year. Does

not work on Macintosh computers. Some reported problems in loading makes it inconsistent.

CryptoHeaven – www.cryptoheaven.com

- Pros: Uses 256-bit encryption for secure email and secure file sharing; data never travels on public internet, which enormously cuts risks. Available for all major platforms: PC, Mac, Linux.
- Cons: Relatively new and untested by cryptocommunity; costs $30/year for advanced features like secure online file storage. Downloadable application – must be able to install new software on each computer using it.

MailVault – www.mailvault.com

- Pros. Supports 256-bit AES for SSL transmission security if your browser also supports it. Clients have the ability to send and receive encrypted e-mail from any location, not just from their own computers using Mailvault's secure web-based login. Non-encrypted e-mail messages can also be written and sent via MailVault. Encryption keys are created by the MailVault engine and stored on distributed offshore servers.
- Cons: Relatively new; You can not use your own domain name, just use the domain name mailvault.com.

Disk encryption

PGP Disk

Can be obtained on www.pgpi.com freeware version 6.0.1. New version 8.0 was released by PGP Corporation and is actively being supported by them.

- Pros: trustworthy; older version may be free. Paid version is a benchmark in the field.
- Cons: Not completely intuitive, and free versions do not work with modern/up to-date operating systems; older free versions may require a separate patch to be installed.

DriveCrypt – www.drivecrypt.com

- Pros: supported, trustworthy, has more features than PGP Disk
- Cons: $40

BestCrypt – www.bestcrypt.com

- Pros: works on Windows & Linux, supported, many features including Wipe, free trial version
- Cons: does not work on Macintosh, proprietary so not free

Anonymous Remailer and Surfing

Anonymizer – www.anonymizer.com

- Pros: Author is very credible within the security field.

- Cons: Proprietary, you must trust the author, no peer review.

AnonymSurfen - http://www.anonymsurfen.com/

- Surfing anonymous in the Net. Free web-based proxies that can be used directly from the website.

Anonymouse.com - http://nonymouse.com/

- Offers anonymous Web surfing and newsgroup posting. It is free.

FAQ Anonymous Remailer - http://www.andrebacard.com/remail.html
http://www.panta-rhei.eu.org/pantawiki

Tor – http://www.eff.org

- Anonymous web browsing, instant messaging, etc. Also allows users to offer "hidden" web servers and other services, even from behind firewalls.

DATA STORAGE/Backup

Martus – www.martus.org

- Pros: very easy to use; trusted source, will be open source; built in encryption; support and training readily available; based on basic database system; platform independent; can make parts of "bulletins" available to the public; can search and retrieve items easily.
- Cons: Should not be used as communication system, only as information storage and retrieval system; must rely on other organizations to host Martus servers (however, there are already several reputable ones in operation)

CDRWs (CD read/write)

- Pros: inexpensive and easy to use
- Cons: user-based so you must remember to perform the backup. Backup must be placed in secure, separate location.

Extra hard drive in computer

- Pros: easy to use and usually readily available, relatively inexpensive
- Cons: raid or surveillance/hacking could result in both original and backup destruction; can accidentally be overwritten – prone to user error.

Online backup company
(novastore.com, bitstore.com, virtualbackup.com and many more)

- Pros: easy to use
- Cons: cost, must send all documents encrypted as source is not necessarily trusted.

Backup software

Retrospect.com (NovaStore, Symantec Norton Ghost and more are similar)

- Pros: cross-platform, desktop and server versions, can be automated to save time, relatively easy to use, one time setup, then transparent to user, backs up to multiple media – disk, internet, etc.
- Cons: proprietary code, costs money

DIY (Do It Yourself)

- A knowledgeable computer systems administrator can set up a regular backup cycle, preferrably to an off-site location, sent in a secure manner so that your files can't be read in transit. Some of the utilities that will do this are "rsync" and "ssh". Please either contact us for assistance or make sure you have an experienced person helping you
- Pros: Cheap and fast to implement
- Cons: Can be complicated; must be an experienced computer user/technician

USB, Compact Flash Memory or Memory Stick

- Pros: extremely portable, can easily be hidden by casual inspection, can hold up to 1 GB (gigabyte), which is about a million one-page emails or 1000 1MB formatted documents
- Cons: must purchase hardware, user-based so you must remember to perform backup. Uses battery consumption so will wear laptop battery faster.

Examples of these can be found at:
http://www.rtsz.com/cryptostick.shtml - USB memory
http://www.memorysuppliers.com/memorystick.html - memory stick
http://www.memorysuppliers.com/compactflash.html - compact flash memory

Physical Security

Biometric (Fingerprint) Identification

- Siemens and other companies now make USB mice that have fingerprint recognition features built-in, preventing unauthorized users from using your computer.

Cameras

- Small, inexpensive cameras can be discreetly mounted to monitor who enters your doors and/or windows for when your computers are completely unattended.

Locks, etc

- Judicious use of locks, security personnel and placement of computers away from windows provides better protection.

Other

PGP SDA (self decrypting archive)

- Pros: Enables you to send a PGP-encrypted document to a user that doesn't have PGP installed on computer. Is bundled with PGP versions 6.5 and higher.
- Cons: Must get decrypting passphrase to end-user somehow in a secure manner.

S-Mail S-Disk:

- Pros: Allows you to share sensitive documents in an online encrypted space.

Virtual shredder

- Pros: Bundled with PGP, Diskwipe shreds files.
- Cons: Simply deleting a document does not wipe it from your system – you must remember to wipe it.

Keyboard popup

- "Type" your passphrase in a keyboard on your screen when you suspect that the emissions from your keyboard strokes are being logged. This is built into CryptoHeaven and Martus software, but we aren't aware of any others that have this feature built in.

Tempest

- Use of "tempest" shielded fonts in your email client (built in to PGP using "secure viewing") and others will protect you if you suspect eavesdropping on unintentional emissions produced by most electronic equipment. See www.tempest-inc.com/ for examples, additional information.

Acknowledgments: *This material was created for the workshop on privacy and secure communications for humans rights non-governmental organizations organized by Privaterra (http://www.privaterra.org), an on-going project of Computer Professionals For Social Responsibility (CPSR) with the cooperation of CPSR-Perú (http://www.cpsr-peru.org) in Lima, Peru 2003. It was prepared by the Privaterra team conformed by Robert Guerra (Managing Director), Caryn Mladen (formerly Privaterra), Jo Hasting (formerly Privaterra) and Katitza Rodríguez (formerly Privaterra and CPSR-Perú). A minor up date was done by Katitza Rodríguez, Director of CPSR-Perú, specially for this workshop.*

Disclaimer: *The speaker does not lobby for, consult, or advice companies, nor do we endorse specific products or services. This list merely serves as a sampling of available privacy-enhancing tools including our comments based in our own experience. If you have comments to share regarding one or more of the tools that are already listed, send an e-mail to katitza@cpsr-peru.org. If you have questions about a tool on this list, visit their own website directly for more information.*