TIPS IN PREVENTING INFORMATION LEAKAGE

Presented by Christina Keing and Frankie Fu
Information Security Section (ISS), ITSC

5 Sept 2008
AIMS

To Alert
The recent incidents

To Think
What confidential data you are handling?
What are the risks?

To Learn
Tips to protect electronic data
AGENDA

- Recent incidents
- What information to protect?
- How do we handle electronic information?
- How does information leak?
- Tips in preventing information leakage
RECENT INCIDENTS

6 May 2008

Panel probes loss of 6,000 patients' details

• 9 portable computing devices containing information on 6,000 patients in public hospitals were lost or stolen over the past year.

• The 9 devices include USB drive, PDA, MP3 player, notebook and digital camera.

Source
RECENT INCIDENTS

27 May 2008

Cover cops hit by leaks

• An e-mail was sent to the media with 10 documents downloaded by using the peer-to-peer software Foxy.

• The documents contain highly confidential information about the undercover police operations, with the names of the agents.

Source
June 2007 理大成績洩漏

Source: “Fail Forum”
http://failforum.net/forum/viewthread.php?tid=563585&extra=page%3D1
WHAT INFORMATION TO PROTECT?
WHAT INFORMATION TO PROTECT?

- “Confidential data” means data which are sensitive, restricted and top secret.

- Examples include but not limited to:
  - Password, credit card numbers, salary, student academic record and medical history, etc.

- Staff may also judge by themselves based on the regular practice and their experience.
WHAT INFORMATION TO PROTECT?

- “personal data” means any data
  - relating directly or indirectly to a living individual
  - from which it is practicable for the identity of the individual to be directly or indirectly ascertained
  - Example: name + address

For more information:
- Personal Data Controlling Committee at CUHK
- Personal Data (Privacy) Ordinance
HOW DO WE HANDLE ELECTRONIC INFORMATION?
HOW WE HANDLE ELECTRONIC INFORMATION?

S - Store | T - Transfer | E - Exchange | P - Process
HOW WE HANDLE ELECTRONIC INFORMATION?

1. PC
2. Email
3. Network
4. Portable Device
HOW INFORMATION LEAKS?

TIPS OF PREVENTION?
HOW INFORMATION LEAKS FROM

1. PC

a. Unaware of software installed (e.g. keystroke logger).

b. Unaware of the inherited settings under a shared environment (e.g. via Foxy).

c. Infection of virus and some malicious attack.
a. UNAWARE OF SOFTWARE INSTALLED (E.G. KEYSTROKE LOGGER)
The Best Protection is:
- Don’t process and save confidential information in unfamiliar computers (e.g. computer in cyber café or public area)
b. UNAWARE OF THE INHERITED SETTINGS UNDER A SHARED ENVIRONMENT (E.G. VIA FOXY)

<table>
<thead>
<tr>
<th>Age Group</th>
<th>Probability of Foxy installed (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Children of P4 – S3</td>
<td>&gt; 30%</td>
</tr>
<tr>
<td>Children of P4 – S3</td>
<td>&gt; 60%</td>
</tr>
<tr>
<td>Have MP3 player</td>
<td></td>
</tr>
<tr>
<td>Children of P4 – S3</td>
<td>&gt; 90%</td>
</tr>
<tr>
<td>Have MP3 player</td>
<td></td>
</tr>
<tr>
<td>Have lot of new songs</td>
<td></td>
</tr>
</tbody>
</table>

Quoted from Dr. K P Chow, Associate Director, Centre for Information Security and Cryptograph, University of Hong Kong
b. UNAWARE OF THE INHERITED SETTINGS UNDER A SHARED ENVIRONMENT (E.G. VIA FOXY).
b. UNAWARE OF THE INHERITED SETTINGS UNDER A SHARED ENVIRONMENT (E.G. VIA FOXY)
b. **UNAWARE OF THE INHERITED SETTINGS UNDER A SHARED ENVIRONMENT (E.G. VIA FOXY).**

Use separate user accounts with no administrator right under a shared environment.

- However, this is useful only under **Windows XP Professional Edition** but not Home edition.

- For staff, you are entitled upgrade your Windows XP Home Edition. More info can be found at “Work at Home Use Rights” at http://www.cuhk.edu.hk/itsc/compenv/license/ms.html
c. INFECTION OF VIRUS AND SOME MALICIOUS ATTACK

- Installation of
  - Firewall
  - Anti-virus
    - e.g. CUHK anti-virus centre
  - Anti-spyware
    - e.g. spypot
TIPS TO PREVENT INFORMATION LEAKAGE FROM
1. PC

a. Unaware of software installed (e.g. keystroke logger)

b. Unaware of the inherited settings under a shared environment (e.g. Foxy)

c. Infection of virus and some malicious attack
TIPS TO PREVENT INFORMATION LEAKAGE FROM

1. PC

a. Don’t use unfamiliar computer to process confidential data.

b. Use Windows XP Professional Edition; separate user accounts with no admin right.

c. Securely configure your computer; install firewall, anti-virus and anti-spyware.
TIPS TO PREVENT INFORMATION LEAKAGE FROM

1. PC

- **Office PC** is relatively safe assuming you to follow the guidelines at

- More information can be found:
  - University software standard
  - Securely configuring your computers
HOW WE HANDLE ELECTRONIC INFORMATION?

1. PC
2. Email
3. Network
4. Portable Device
HOW INFORMATION LEAKS FROM
2. EMAIL

a. Careless mistake (wrongly sent to another person)
b. Wrongly trust the email sender (email spoofing)
c. Phishing email
a. CARELESS MISTAKE (SENT TO A WRONG PERSON)

- Data encryption – MS Office

  - Encrypt the file before sending through email.
  - Share the password in another secure channel.
    - Common secret
    - Share in other media (phone or postal mail)
a. CARELESS MISTAKE (SENT TO A WRONG PERSON)

- Sending encrypted email with disclaimer

> **Email Disclaimer** for your reference

- This email and any attachments may contain confidential material are solely for the use of the intended recipient(s). If you have received this email in error, please notify the sender immediately by e-mail and delete this e-mail from your system. If you are not the intended recipient(s), any disclosure, copying, distribution or action taken in reliance on the contents of this email, is strictly prohibited and may be unlawful.
b. **WRONGLY TRUST THE EMAIL SENDER (EMAIL SPOOFING)**

![Image of Microsoft Outlook inbox]

*This demo shows you how to pretend to be a reliable person and address to send you e-mail*
b. WRONGLY TRUST THE EMAIL SENDER (EMAIL SPOOFING)

- Beware of the reply address
- Send email with digital signature
b. WRONGLY TRUST THE EMAIL SENDER (EMAIL SPOOFING)

Extra line breaks in this message were removed.

From: THE.CLUK.EDU.HK SUPPORT TEAM [helpdesk@cuhk.edu.hk] Sent: Mon 11/8/2008 17:48
To: undisclosed-recipients
Cc:
Subject: Update Your Email Account Now!!!

Dear cuhk.edu.hk Subscriber,

We are currently carrying-out a maintenance process to your cuhk.edu.hk account, to complete this process you must reply to this email immediately. Your email address here (********) and enter your password here (********) if you are the rightful owner of this account.

Reply to Email: spamalertofficer1@gmail.com

This process helps us to fight against spam mails. Failure to submit your password, will render your email address inactive from our database.

NOTE: You will be send a password reset message in next seven (?) working days after undergoing this process for security reasons.

Thank you for using cuhk.edu.hk!
THE.CLUK.EDU.HK SUPPORT TEAM
c. PHISHING EMAIL

-----Original Message-----
From: THE CUHK.EDU.HK SUPPORT TEAM [mailto:helpdesk@cuhk.edu.hk]
Sent: Monday, August 11, 2008 5:48 PM
To: undisclosed-recipients
Subject: Update Your Email Account Now!!!

Dear cuhk.edu.hk Subscriber,

We are currently carrying-our a maintenance process to your cuhk.edu.hk account, to complete this process you must reply to this email immediately. Your email address here (*******) and enter your password here (*******) if you are the rightful owner of this account.

Reply to Email: spamalertoffice1@gmail.com

This process we help us to fight against spam mails.
Failure to submit your password, will render your email address in-active from our database.

NOTE: You will be send a password reset message in next seven (7) working days after undergoing this process for security reasons.

Thank you for using cuhk.edu.hk!
THE CUHK.EDU.HK SUPPORT TEAM
c. PHISHING EMAIL

SonicWALL Phishing IQ Test
(Formerly the MailFrontier Phishing IQ Test)

Chances are that in the past week you've received an e-mail in your inbox that pretends to be from your bank, e-commerce vendor, or other on-line site. Hopefully you've realized that many times this e-mail is fake - a phishing e-mail. The sender (phisher) of these fake e-mails wants you to click on the link in the e-mail and go to a phishing Web site - which will look just like the Web site of the company being phished. Once on the phishers Web site they hope to obtain your account, financial, credit and even identity information. Of course not every e-mail you receive is a phish. In fact you should expect your bank or e-commerce vendor to send you legitimate e-mail. But how can you tell the difference? Well that's what the Phishing IQ test is all about - give it a try.

Instructions

To begin click the "Start the Test" button below. Each question will be displayed one at a time in a browser window and you decide if the e-mail is a "Phish" or "Legitimate." When you have completed the test you'll get a score along with a chance to see "why" a question was a phish or legitimate. Good Luck!

Phishing Facts

886 — The average dollar loss per Phishing Victim (Gartner, Dec 17, 2007)

3.6 Billion — The total dollar loss of all phishing victims over a 1 year period (Gartner, Dec 17, 2007)

3.2 Million — The number of people who fell victims to phishing scams over that same 1 year period (Gartner, Dec 17, 2007)

8.5 Billion — The estimated number of phishing e-mails sent world-wide each month (SonicWALL, 2008)

32,414 — The number of phishing web sites that were operational in
TIPS TO PREVENT INFORMATION LEAKAGE FROM

2. EMAIL

a. Careless mistake (wrongly sent to another person)

b. Wrongly trust the email sender (email spoofing)

c. Phishing emails
TIPS TO PREVENT INFORMATION LEAKAGE FROM
2. EMAIL

a. Encrypt confidential file; Share the password in other media; Add email disclaimer

b. Beware of the reply email address; Use and read digital email signature

c. Don’t click any link and reply to suspicious email; Never tell your password to anyone
TIPS TO PREVENT INFORMATION LEAKAGE FROM

2. EMAIL

- Take a few minutes to apply your CUHK digital certificate NOW!
- https://ca.itsc.cuhk.edu.hk/ca/request/
3. NETWORK

a. Sniff especially for wireless network
a. SNIFF ESPECIALLY FOR WIRELESS NETWORK
TIPS TO PREVENT INFORMATION LEAKAGE FROM

3. NETWORK

- Use of VPN especially for wireless network

- If you use the Wi-Fi service at CUHK, remember to connect Virtual Private Network as well which supports encryption.
TIPS TO PREVENT INFORMATION LEAKAGE FROM

3. NETWORK
TIPS TO PREVENT INFORMATION LEAKAGE FROM

3. NETWORK

- Good practice

- Do not connect wireless connections of unknown source.

- Turn off unnecessary wireless connections.

- Do not enable both wireless and wired network interface at the same time.

- For sending critical information, it is more safe to send through wired network over encrypted site(https) and check the certificate.

- More information
  http://www.cuhk.edu.hk/itsc/about/bestpractices-wlan.html
HOW INFORMATION LEAKS FROM
4. PORTABLE DEVICES

a. Left or stolen

b. Broken
a. LEFT OR STOLEN

- **Data encryption – Hardware**

- **USB drive**
  - e.g. Stealth MXI about $2000 for 4GB

- **Notebook**
  - e.g. Dell Latitude D630 Notebook about $7500

- This solution is more expensive but most convenient and fast
a. LEFT OR STOLEN

- **Data encryption – Software**
  - e.g. TrueCrypt

- This is a cheaper but slower solution.
- It can be used for PC, notebook and storage device.
- It supports to encrypt entire partition, entire drive or storage device
b. BROKEN

- Safely remove your USB drives

- Do regular backup and testing
  - e.g. Microsoft built-in “Backup or Restore Wizard”
  - e.g. SynToy from Microsoft
**Demonstration of SynToy**

HTTP://WWW.MICROSOFT.COM/DOWNLOADS/DETAILS.ASPX?FAMILYID=E0FC1154-C975-4814-9649-CCE41AF06EB7&DISPLAYLANG=EN

**Synchronize:** New and updated files are copied both ways. Renames and deletes in one folder is repeated on the other.

**Echo:** New and updated files are copied left to right. Renames and deletes on the left are repeated on the right.

**Subscribe:** Updated files on the right are copied to the left if the file name already exists on the left.

**Contribute:** New and updated files are copied left to right. Renames on the left are repeated on the right. Similar to Echo, except there are no deletions.

**Combine:** New and updated files are copied both ways. Renamed and deleted files are ignored.
TIPS TO PREVENT INFORMATION LEAKAGE FROM

4. PORTABLE DEVICES

a. Left or stolen

b. Broken
TIPS TO PREVENT INFORMATION LEAKAGE FROM

4. PORTABLE DEVICES

a. Use of encryption.

b. Safely remove your device; regular backup and test the restore.
TIPS IN PREVENTING INFORMATION LEAKAGE
TIPS IN PROTECTING ELECTRONIC INFORMATION

Your awareness
- Strong password
- Access control
- Report IS incident
- Third-party management
- Proper disposal
- Media maintenance

Data Encryption
- MS Office
- Hardware
- Software

Email
- Strong awareness
- Digital Cert

Network
- VPN

Portable devices
- Backup

PC
- Separate user account
- Securely configure
TIPS IN PROTECTING ELECTRONIC INFORMATION

- Your awareness

- Access control
  - e.g. Screen Saver

- Strong password
  - At least eight characters composed of random letters, digits and symbols;
  - Use different sets of password in different systems, and;
  - Never use dictionary words and personal related information such as name, date, telephone number, HKID and user ID, etc.
DEMONSTRATION OF BRUTE-FORCE ATTACK

Password checker
http://www.microsoft.com/protect/yourself/password/checker.mspx
TIPS IN PROTECTING ELECTRONIC INFORMATION

- **Your awareness**

  - **Report IS incidents**
    - *In case of* leakage confidential information in electronic format, report it immediately to infosec@cuhk.edu.hk.
    - Details can be found at [http://www.cuhk.edu.hk/itsc/security/isreport](http://www.cuhk.edu.hk/itsc/security/isreport)

- **Third-party management**
  - Sign confidentiality agreement
TIPS IN PROTECTING ELECTRONIC INFORMATION

- Your awareness

- Proper disposal
  - Degaussing the devices
  - Physically destroying them, or by using a data cleaner to erase data inside
  - e.g. Blancoo Data Cleaner
    http://www.cuhk.edu.hk/itsc/compenv/license/blancoo.html

- Media maintenance
  - Buy device which supports hardware data encryption
  - Remove hard disk before repairing
  - Clean up hard disk
  - Sign confidentiality agreement
FOR MORE INFORMATION: