Computers and Society

Computer Crimes, Information Security, and Privacy Issues

Overview

- Computer Crimes
- Information Security
- Privacy

Some Types of Crime

- Steal 偷 – information and money
- Cheat 呃 – false identity and transaction
- Abduct 拐 – hijacking web sites
- Fraud 騙 – various kind
- Rob 搶 – cyber asset
- Blackmail 勒索 – DDoS attack revenue model
- Libel 誹謗 – abuse of cyberspace “freedom of speech”
- Harassment 騷擾 – sexual or other means
- Online Gambling 網上賭博

Hacking

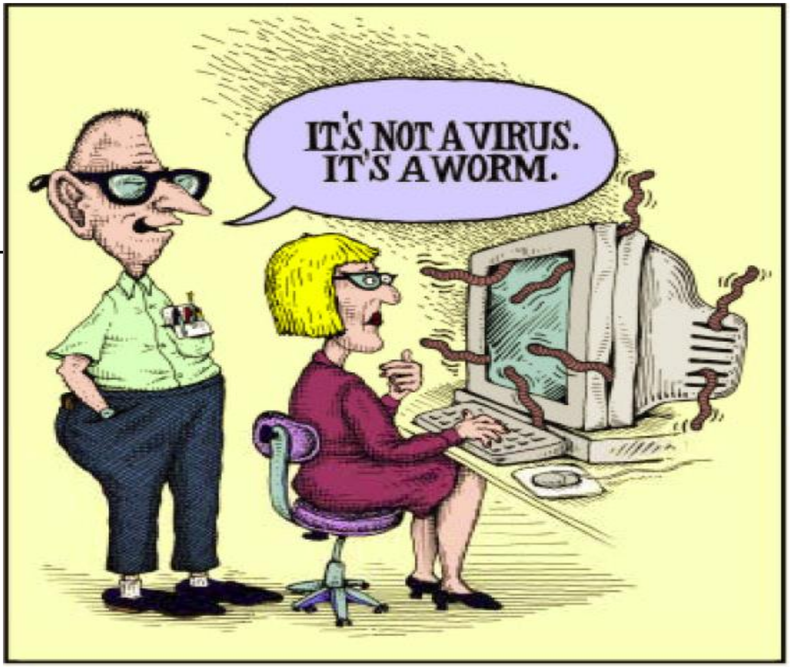
- Hacking – currently defined as to gain illegal or unauthorized access to a file, computer, or network

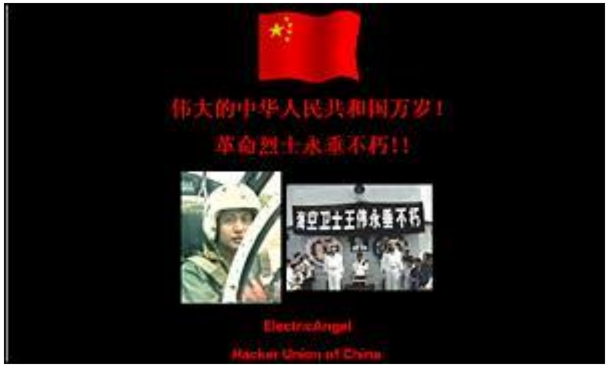
- The term has changed over time

- Originally,
  - It was a positive term
  - A "hacker" was a creative programmer who wrote elegant or clever code
  - A "hack" was an especially clever piece of code

Hacking (黑客)

- The growth of the Web changed hacking; viruses and worms could be spread rapidly
- Political hacking (Hacktivism) surfaced
- Distributed Denial-of-service (DDoS) attacks used to shut down Web sites
- Large scale theft of personal and financial information




伟大的中华人民共和国万岁！

革命烈士永垂不朽!!

ElectricAngel

Hacker Union of China

Defaced Whitehouse Web, some time ago

Common Web Application Vulnerabilities 易受傷／弱點

- Cross Site Scripting (XSS)
- Injection Flaws
- Malicious File Execution
- Insecure Direct Object Reference
- Buffer Overflow
- Information Leakage and Improper Error Handling
- Broken Authentication and Session Management
- Insecure Cryptographic Storage
- Insecure Communications
- Failure to Restrict URL Access

文字

http://newsletter.ascc.sinica.edu.tw/news/read_news.php?nid=1917

OS related
- Malicious File Execution
- Buffer Overflow

Database related
- Injection Flaws
- Info Leakage / Improper Error Handling

Browser related
- Failure to Restrict URL Access
- Cross Site Scripting
- Broken Authentication & Session Management

Insecure
- Direct Object Reference
- Cryptographic Storage
- Communication

Hacking: Law Enforcement

- Catching Hackers requires law enforcement and agencies to recognize and to respond to myriad hacking attacks.

- Computer forensics agencies and services include:
  - Computer Emergency Response Team (CERT)
    - http://www.cert.org/
  - HKCERT
    - http://www.hkcert.org/
  - US National Infrastructure Protection Center (NIPC)
  - China National Infrastructure Protection Center (国家计算机网络入侵防范中心)
    - http://www.nipc.org.cn/

Hacking: Law Enforcement (US)

In the US: Laws for Catching and Punishing Hackers:

- Computer Fraud and Abuse Act (CFAA, 1986)
  - Covers government computers, financial and medical systems, and activities that involve computers in more than one state, including computers connected to the Internet

- USA Patriot Act (USAPA, 2001)
  - Amends the CFAA.
  - Allows for recovery of losses due to responding to a hacker attack,
  - Higher penalties can be levied against anyone hacking into computers belonging to criminal justice system or the military.
  - *The government can monitor online activity without a court order.*

Hacking: Law Enforcement (HK)

- Computer Crimes Ordinance (電腦罪行條例, 1993)
  - Through amending the Telecommunications Ordinance (電訊條例), Crimes Ordinance (刑事罪行條例), and Theft Ordinance (盜竊罪條例)
  - Created new offences
  - Broadened the coverage of existing offences

Computer Crimes Ordinance (1993)

- New Offence:
  - Obtains unauthorised access to any computer by telecommunications
  - Obtains access to a computer with intent to commit an offence or with a dishonest intent
- Extending the meaning of …
  - Property → any program or data held in a computer or in computer storage medium
  - Criminal damage to property → misuse of a computer program or data
  - Burglary → unlawfully causing a computer to function other than established [and …]
  - False accounting → …, making false entry in bank book → …

Hacking: Law Enforcement

- Questions About Penalties:
  - Intent
    - Should hackers who did not intend to do damage or harm be punished differently than those with criminal intentions?
  - Age
    - Should underage/ juvenile hackers receive a different penalty than adult hackers?
  - Damage Done
    - Should the penalty correspond to the actual damage done or the potential for damage?

Hacking: Law Enforcement

- Penalties for young hackers
  - Some young hackers have matured and gone on to productive and responsible careers
    - E.g. Frank Abagnale now works for the FBI, see the movie <*Catch Me If You Can*>
  - Temptation to over or under punish
  - Sentencing depends on intent and damage done
  - Most young hackers receive probation, community service, and/or fines

Image source: http://en.wikipedia.org/wiki/File:Frank_Abagnale_(cropped).jpg by SOWHY

Hacking: Responsibilities

- Responsibility for Security
  - **Developers** have a responsibility to develop with security as a goal
  - **Businesses** have a responsibility to use security tools and monitor their systems to prevent attacks from succeeding
  - **Home users** have a responsibility to ask questions and educate themselves on the tools to maintain security (personal firewalls, anti-virus and anti-spyware)

Identity Theft and Credit Card Fraud

- Identity Theft – various crimes in which a criminal or large group uses the identity of an unknowing, innocent person
  - Targeted at credit card numbers, personal information, PIN, Social Security Numbers (SSN in the US), driving license numbers (US) or HKID Card Numbers
  - 18-29 year-olds are the most common victims because they use the web most and are unaware of risks
  - E-commerce has made it easier to steal card numbers and use without having the physical card

Identity Theft and Credit Card Fraud

- Techniques used to steal personal and financial information
  - Phishing - e-mail fishing for personal and financial information disguised as legitimate business e-mail
  - Pharming - false Web sites that fish for personal and financial information by planting false URLs in Domain Name Servers (DNS poisoning)
  - Online resume and job hunting sites may reveal identity numbers, work history, birth dates and other information that can be used in identity theft

Identity Theft and Credit Card Fraud

- Techniques used to protect personal and financial information
  - Activation for new credit cards
  - Retailers and ATMs do not print/show the full card number and expiration date on receipts
  - Software detects unusual spending activities and will prompt retailers to ask for identifying information
  - Services, like PayPal, act as third party allowing a customer to make a purchase without revealing their credit card information to a stranger
  - Credit card issuing agencies perform online verifications

Verified by VISA

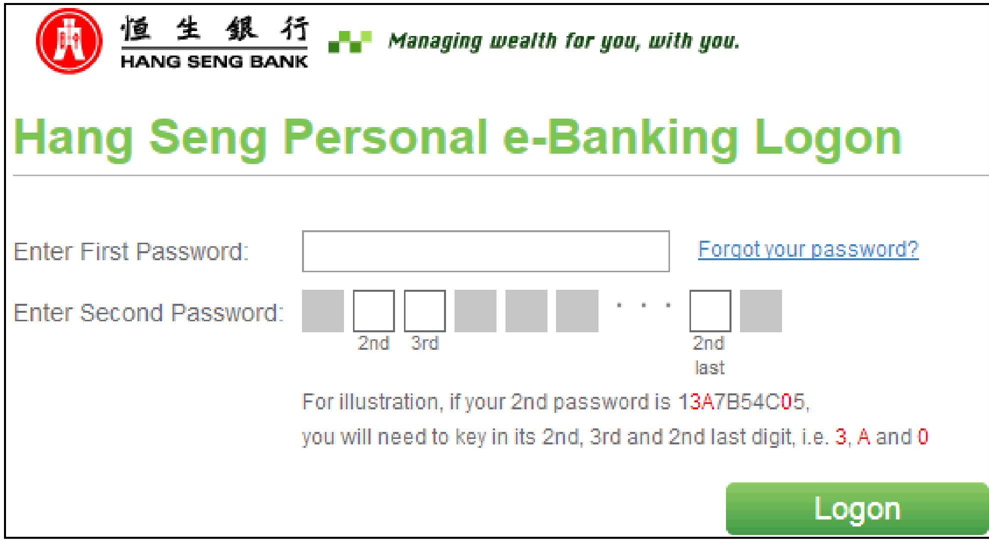
MasterCard SecureCode

look for this logo when shopping online

Identity Theft and Credit Card Fraud

Responses to Identity Theft:

- Authentication of e-mail and Web sites
- Use of encryption to securely store data, so it is useless if stolen
- Authenticating customers to prevent use of stolen numbers, may trade convenience for security
- In the event information is stolen, a fraud alert can flag your credit report; some businesses will cover the cost of a credit report if your information has been stolen

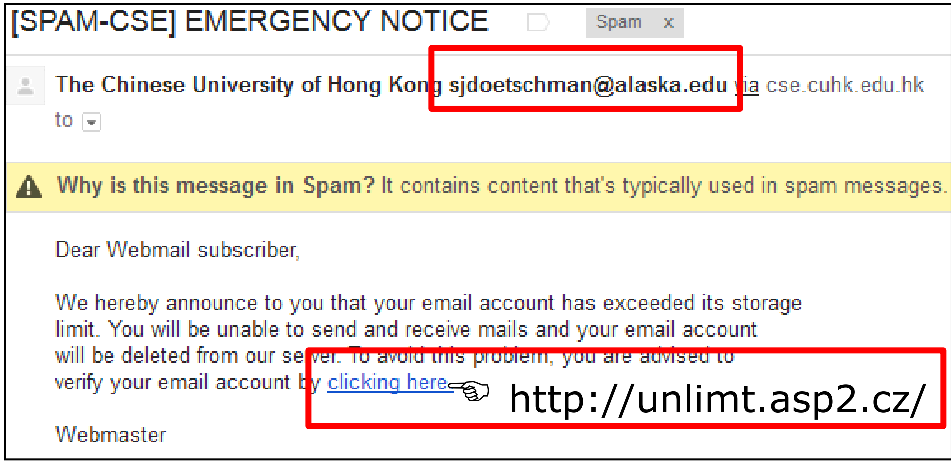

恒 生 銀 行
HANG SENG BANK
Managing wealth for you, with you.

Hang Seng Personal e-Banking Logon

Enter First Password:

Enter Second Password:

For illustration, if your 2nd password is 13A7B54C05,
you will need to key in its 2nd, 3rd and 2nd last digit, i.e. 3, A and 0


[SPAM-CSE] EMERGENCY NOTICE

The Chinese University of Hong Kong sjdoetschman@alaska.edu via cse.cuhk.edu.hk
to

Why is this message in Spam? It contains content that's typically used in spam messages.

Dear Webmail subscriber,

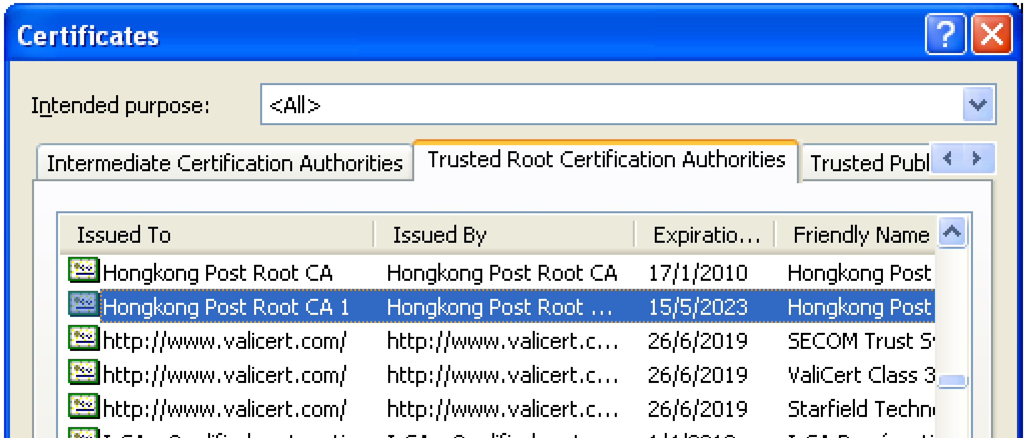
We hereby announce to you that your email account has exceeded its storage limit. You will be unable to send and receive mails and your email account will be deleted from our server. To avoid this problem, you are advised to verify your email account by clicking here

Webmaster

http://unlimt.asp2.cz/

https://...

- HyperText Transfer Protocol Secure
- By trust of
  - Good browser
  - Faithful Certificate Authority (CA)
  - Valid server certificate issued by CA
- To identify legitimate server



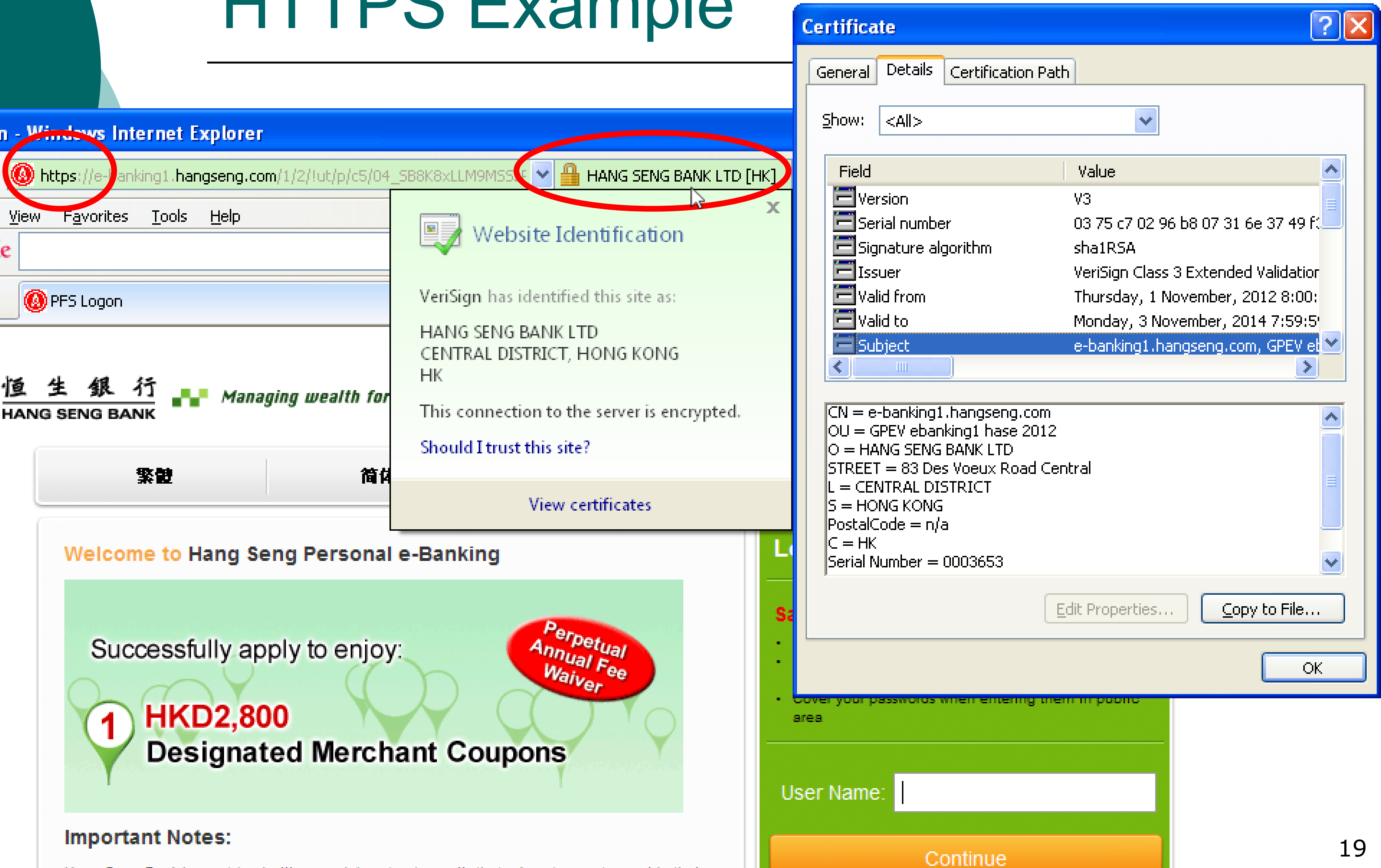
Certificates
?
Intermediate Certification Authorities
Trusted Root Certification Authorities
Trusted Publ

Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
Hongkong Post Root CA	Hongkong Post Root CA	17/1/2010	Hongkong Post
Hongkong Post Root CA 1	Hongkong Post Root ...	15/5/2023	Hongkong Post
http://www.valicert.com/	http://www.valicert.c...	26/6/2019	SECOM Trust S
http://www.valicert.com/	http://www.valicert.c...	26/6/2019	ValiCert Class 3
http://www.valicert.com/	http://www.valicert.c...	26/6/2019	Starfield Techn

Widely-Trusted Root CA's and their record on a browser

HTTPS Example



n - Windows Internet Explorer

https://e-banking1.hangseng.com/1/2/!ut/p/c5/04_SB8K8xLLM9MS5

HANG SENG BANK LTD [HK]

View Favorites Tools Help

PFS Logon

恒 生 銀 行 HANG SENG BANK Managing wealth for

繁體 简体

Welcome to Hang Seng Personal e-Banking

Successfully apply to enjoy:

Perpetual Annual Fee Waiver

1 HKD2,800 Designated Merchant Coupons

Important Notes:

User Name:

Continue

Website Identification

VeriSign has identified this site as:

HANG SENG BANK LTD
CENTRAL DISTRICT, HONG KONG
HK

This connection to the server is encrypted.

Should I trust this site?

View certificates

Certificate

General | Details | Certification Path

Show: <All>

Field	Value
Version	V3
Serial number	03 75 c7 02 96 b8 07 31 6e 37 49 f3
Signature algorithm	sha1RSA
Issuer	VeriSign Class 3 Extended Validation
Valid from	Thursday, 1 November, 2012 8:00:
Valid to	Monday, 3 November, 2014 7:59:5
Subject	e-banking1.hangseng.com, GPEV eb

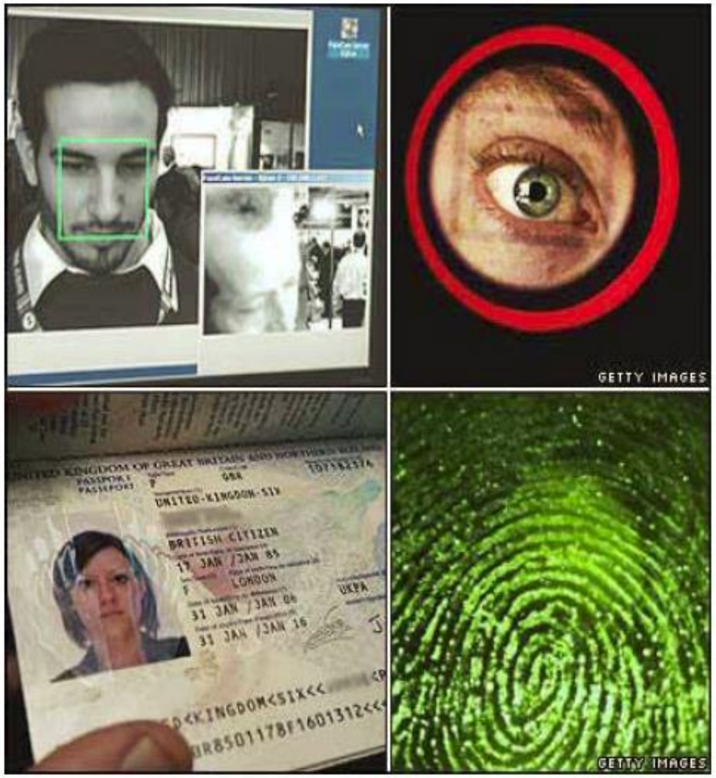
CN = e-banking1.hangseng.com
OU = GPEV ebanking1 hase 2012
O = HANG SENG BANK LTD
STREET = 83 Des Voeux Road Central
L = CENTRAL DISTRICT
S = HONG KONG
PostalCode = n/a
C = HK
Serial Number = 0003653

Edit Properties... Copy to File... OK

Identity Theft and Credit Card Fraud

Biometrics:

- Biological characteristics unique to an individual
- No external item (card, keys, etc.) to be stolen
- Used in areas where security needs to be high, such as identifying airport personnel
- Biometrics can be fooled, but more difficult to do so, especially as more sophisticated systems are developed



Identity Theft and Credit Card Fraud

- Terrible theft…

Image source: http://pixabay.com/en/hand-sky-fingers-hands-57312/

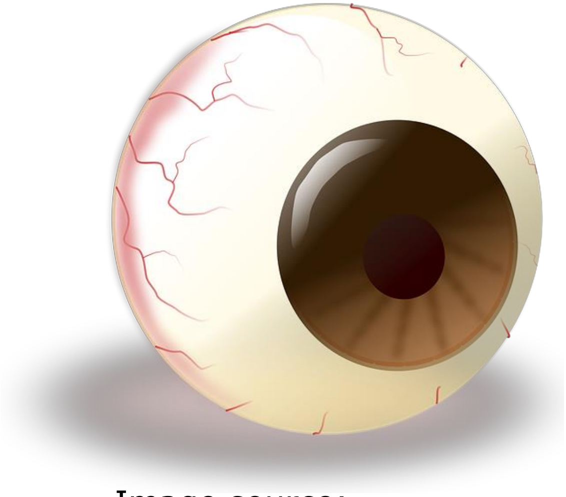


Image source: http://pixabay.com/en/eyes-eye-brown-cartoon-eyeball-32482/

Image source: http://www.flickr.com/photos/cahayadalamkegelapan/4624828088/
by Cahaya Dalam Kegelapan

Identity Theft and Credit Card Fraud Discussion Questions

- What steps can you take to protect yourself from identity theft and credit card fraud?

- How can you distinguish between an e-mail that is a phishing attempt and an e-mail from a legitimate business?

- What should you do to protect your users if you are a system administrator?

Overview

- Computer Crimes
- **Information Security**
- Privacy

What is Information Security?

- The goal of information security is to achieve ***C-I-A***:
  - ***C***onfidentiality (機密性)
  - ***I***ntegrity (完整性)
  - ***A***vailability (可用性)

Confidentiality

- Protecting information from being *disclosed to unauthorized parties*
  - When registering a user account on a website, who is eligible to use or access your personal data collected?
  - Who can access sensitive information (such as sales figures) in a company?

Integrity

- Protecting information from being *changed by unauthorized parties*
  - The bank alters the balance of your account.
  - An employee change sales figures in a company without authorization?

Availability

- Making information *available to authorized parties* only when requested
  - You should be able to check your bank account balance at any time
  - A CEO should be able to access sales figures when needed

Why does Information Security Concern me?

- Because we are exposed to information security ***risks*** whenever we are online
  - Do you scan your incoming e-mails?
  - Update your anti-virus software?
  - Regularly backup your files?
  - Forward e-mails/IMs that ask you to distribute a warning message to others?
  - Apply security patches to your PC?
  - Is your password strong/complicated enough?
  - …

Information Security Risks in Business

- Security doesn't generate revenue. Why should I invest on it?
- We don't have the expertise, so we have to drop it!
- Why should I buy a $100k firewall to protect a $5k PC?
- Everybody out there is the same. Why should I care?
- I have legal liability if I were hacked? Are you kidding?
- My PC was infected by virus before. What a big deal?

Virtual Private Network (VPN)

- To build a *Private* network on top of *Public* connections
- Concept of "tunneling"
- By means of mutual authentication and data encryption
- E.g., a student can connect back to CUHK VPN overseas or via ISP, thus be able to use most CUHK IT services as if in campus

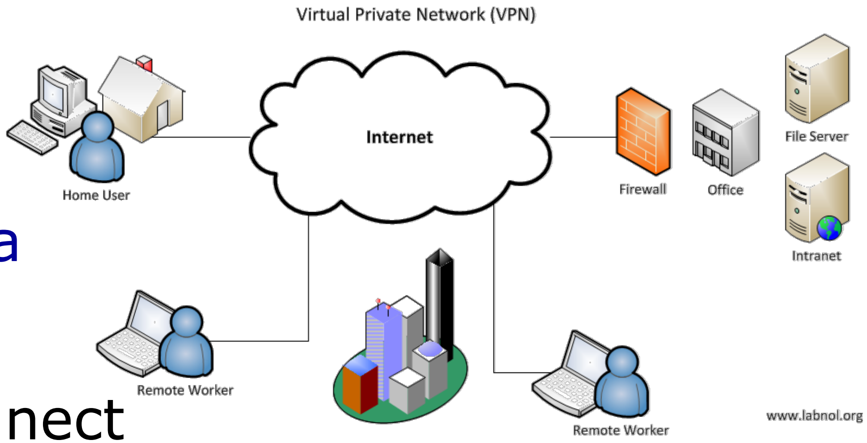


Image source: Digital Inspiration http://www.labnol.org/software/setup-virtual-private-network-vpn/12208/

Setting up and Using L2TP IPSEC VPN in CUHK: www.cuhk.edu.hk/itsc/network/vpn

Securing Wi-Fi Connections

- User’s perspective:
  - Only use registered and legitimate Wi-Fi services
    - Create/save profiles for trusted SSID
    - Do NOT use open/unsecured Wi-Fi AP
  - Prefer 802.1x or WPA2 to web portal login
  - Create a VPN connection on top of the Wi-Fi
  - Avoid doing confidential/sensitive transactions

- Service provider’s perspective:
  - Enable wireless security features such as WPA2
    - data encryption and user authentication
    - WPA or WEP were outdated and not recommended
  - Enable MAC address filtering and hardware firewall?

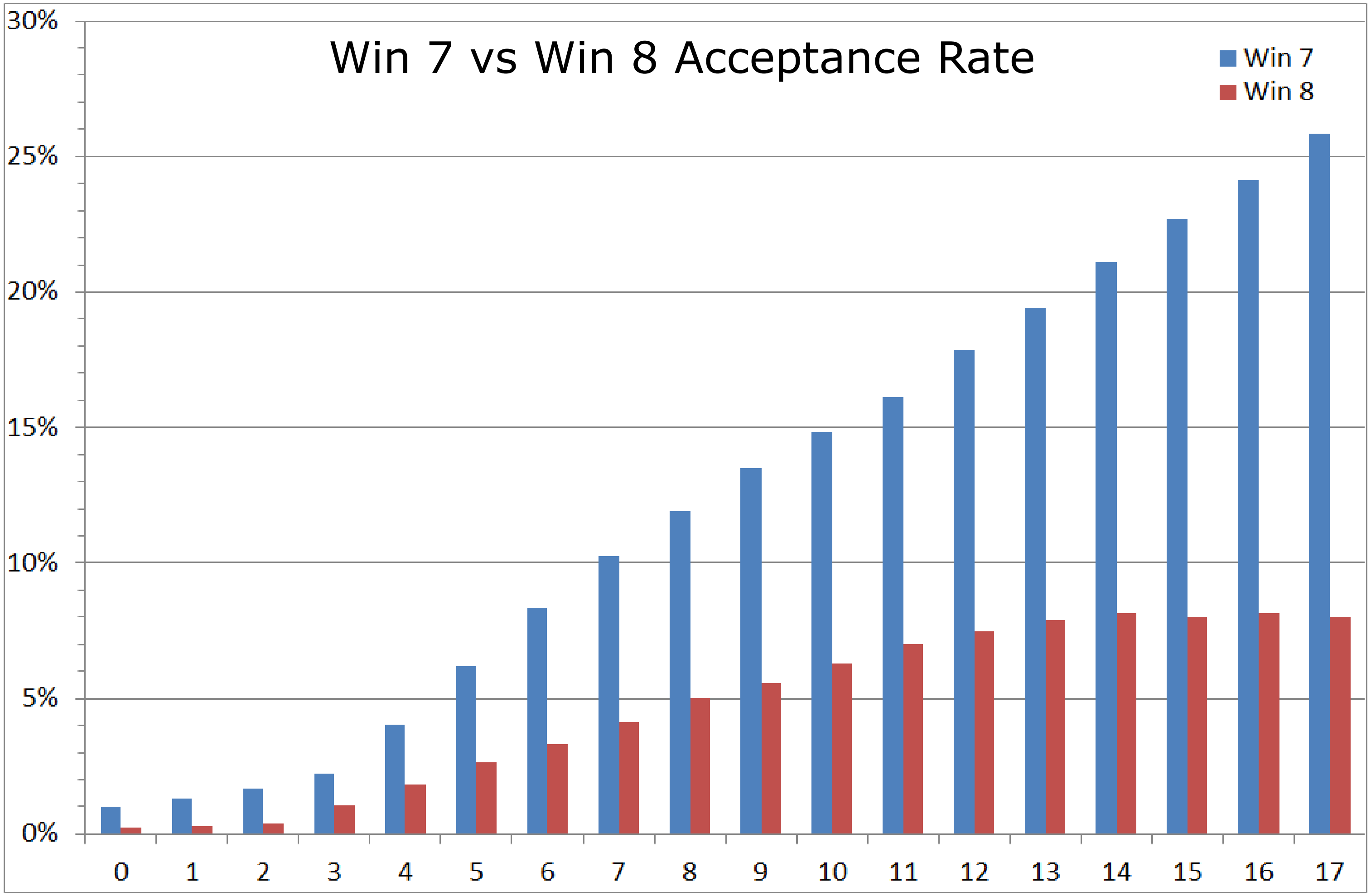
Attribute:
Celineyy

File Sharing with Public and Live Video Streaming

- Peer-to-Peer (P2P) file sharing softwares (BT, Foxy, …) or P2PTV (Sopcast, UUSee, …) have massive connectivity peer-wise
- Many such softwares embed adware/spyware within
- Some malwares target these softwares specifically
  - Copy itself into or adjusting shared folders
  - Dropping backdoors
- Foxy caused some well-known information leakage incidents in HK
- Monitor your configurations (of shared folders, etc.)

Source: http://gs.statcounter.com/

Newer OS, Better OS, Accepted OS?

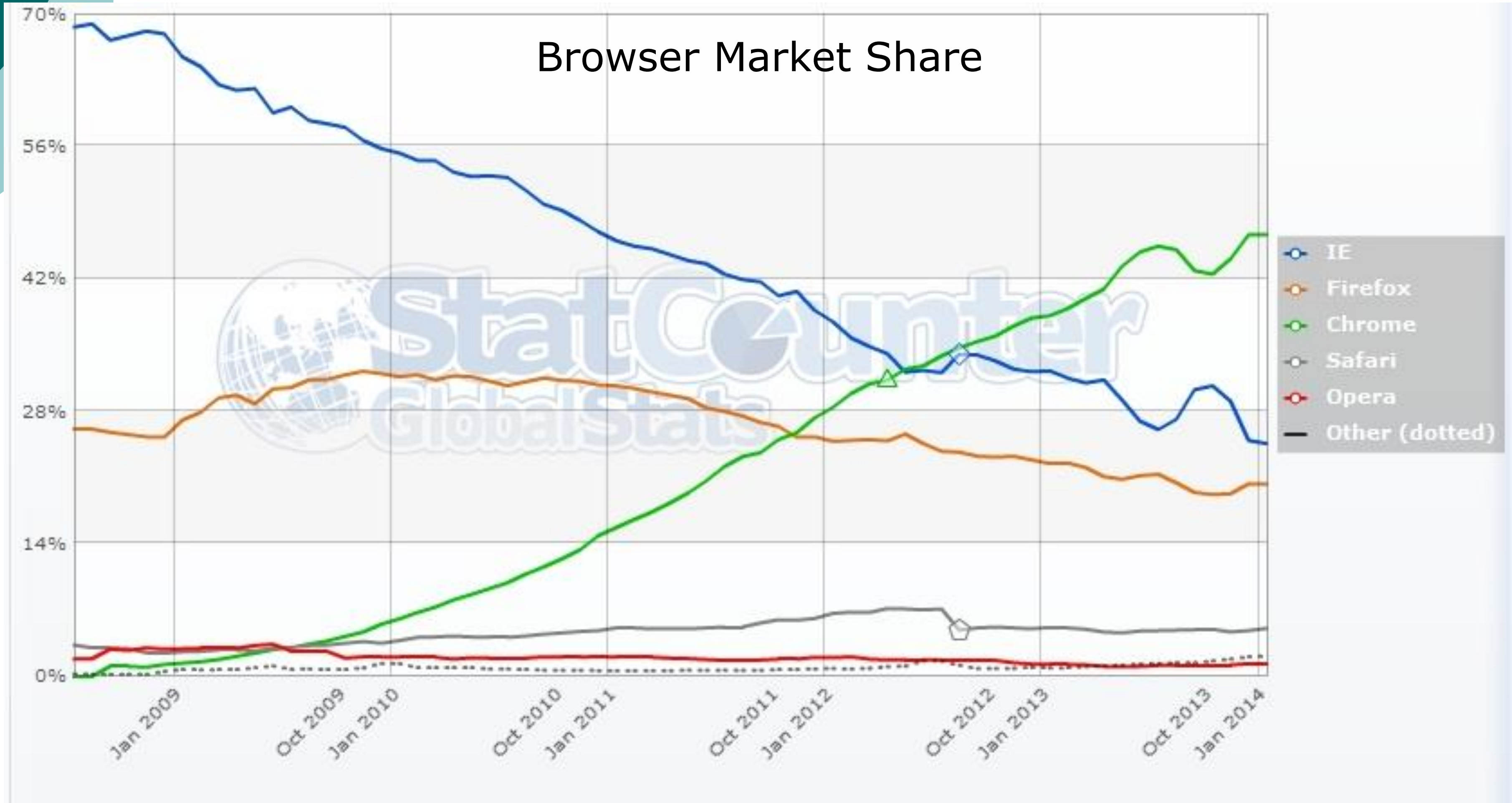


Months after General Availability

Source: http://gs.statcounter.com/

Web Browsing

- ○ Use “non-mainstream” browsers?



Using Email and Messaging Services

- Email, Private Messaging (PM), Instant Messaging (IM), SMS services and Apps-based Messaging (WhatsApp/ LINE)

- Related security issues:
  - Spamming: unsolicited messaging
  - Phishing: message leading to fake web sites
  - Cheat: ask for password or other personal privacy data
  - Eavesdropping: un-encrypted messages may be overheard
  - Spoofing: pretended message sender

- Be smart!
  - Use message filtering and sorting services
  - Do NOT click on links in a message
  - Verify the identity of the message sender

Image source: http://www.hksilicon.com/kb/articles/41471/IM
by Tech2IPO and《數字商業時代》

J*fg3#7Ke199qMn

- Each individual has tons of passwords and Personal Identity Numbers (PIN)
  - They should be composed of as many characters as possible from a large pool of symbols (letters, digits, etc.)
  - They should be unique
  - They should be hard to guess
  - They should be changed regularly
  - They should NOT be written down
  - They should be hard to remember?!

Why?

Any good strategy?

- For example, a single credit card account can bear ATM PIN, phone PIN, e-banking password, Verified-by-VISA password!!!

Facebook

Discuss

Door Lock

J*fg3#7Ke199qMn
QwertAsdf
9876543

Have It Your Own Way

- Prepare a few sets of difficult passwords which you can remember conveniently

- When registering a new service which requires a password, give it a “deserved security level”
  - E.g., GoldenForum may not deserve e-banking level of security
  - Assign password appropriately and cautiously

- Be aware that web administrators and hackers *may* capture your password and try to login other services on your behalf

→ do NOT use the same password for different services,
or at least, across services of different security levels

e-banking

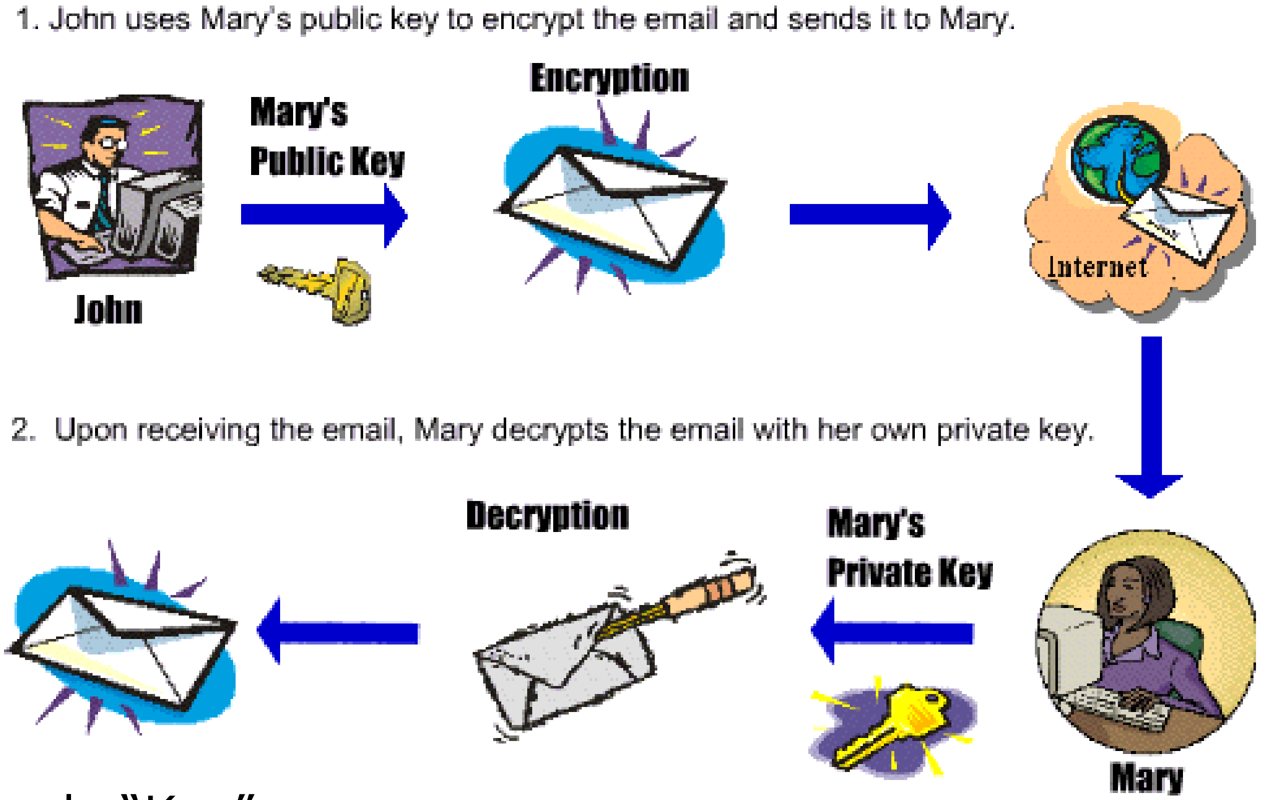
School

Forum

PayPal

Public Key Infrastructure (PKI)

- A framework for deploying public key cryptography



1. John uses Mary's public key to encrypt the email and sends it to Mary.

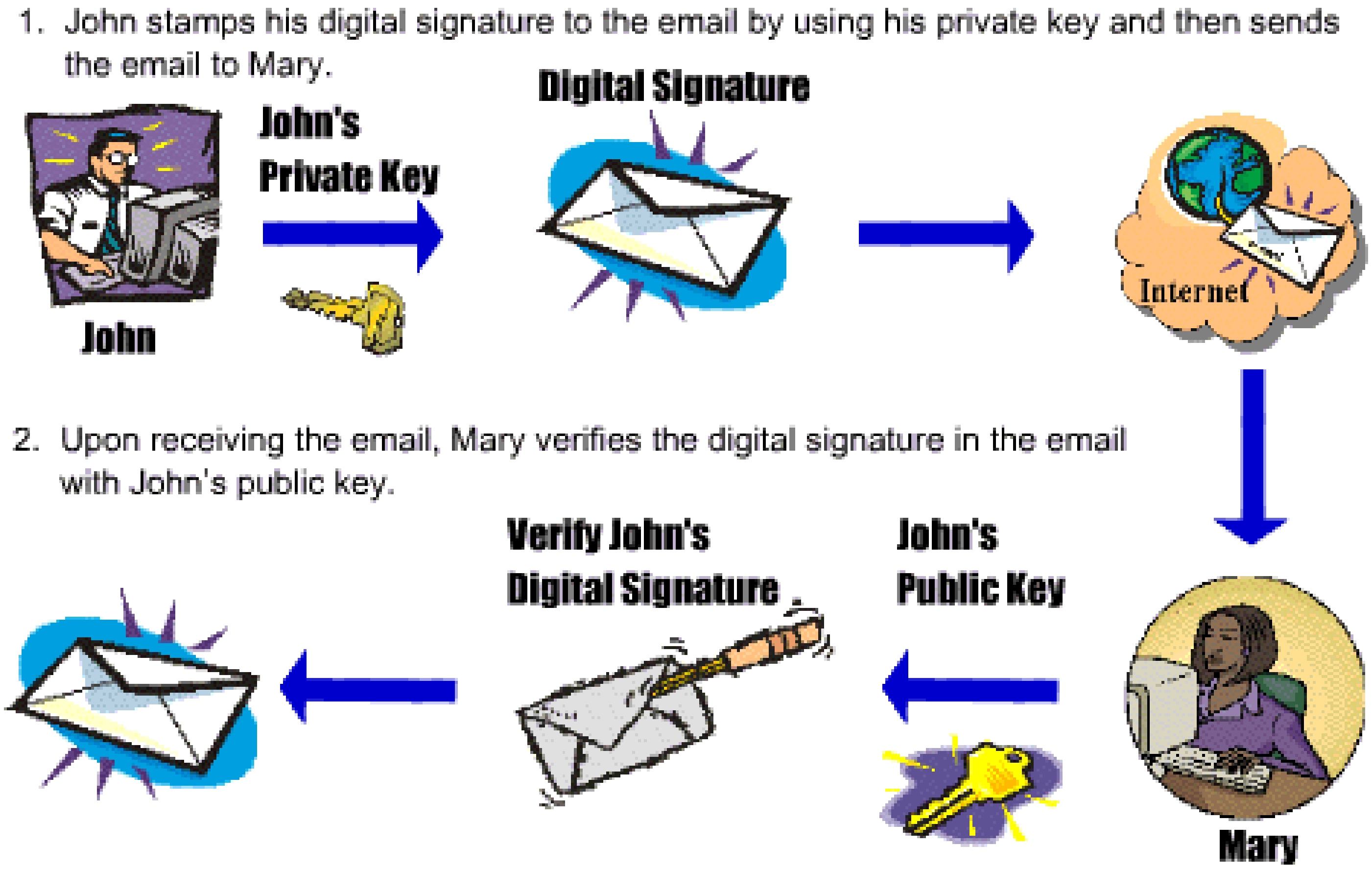
2. Upon receiving the email, Mary decrypts the email with her own private key.

Image source: http://www.infosec.gov.hk

An Example "Key": 3048 0241 00C9 18FA CF8D EB2D EFD5 FD37 89B9 E069 EA97 FC20 5E35 F577 EE31 C4FB C6E4 4811 7D86 BC8F BAFA 362F 922B F01B 2F40 C744 2654 C0DD 2881 D673 CA2B 4003 C266 E2CD CB02 0301 0001

Public Key Infrastructure (PKI)

- Digital Signature



1. John stamps his digital signature to the email by using his private key and then sends the email to Mary.

2. Upon receiving the email, Mary verifies the digital signature in the email with John's public key.

Image source: http://www.infosec.gov.hk

Public Key Infrastructure (PKI)

- **P**rivacy
  - **C**onfidentiality of communication
- **A**uthentication
  - **C**onfirm the identity of both parties
- **I**ntegrity
  - **C**omplete and accurate transmission
- **N**on-repudiation
  - **C**oncrete proof for resolving dispute

Public Key Infrastructure (PKI)

- Effective operation of PKI very much depends on the support of a ***Certification Authority*** (CA)
- A CA acts as a trusted third party to verify the identity of digital certificate subscribers
- Under the Electronic Transactions Ordinance (電子交易條例), Hongkong Post is the first publically recognized CA in HK
  - They issue different types of digital certificate such as e-Certs, Bank-Certs and Mobile e-Certs.

Good Practices for IT Professionals

- Lock the account for a certain time for continuous failed login
- Store password files separately from application system data
- Store and transmit passwords in protected (e.g. encrypted or hashed) form
- Setting session timeout for web applications
- Enable firewall logging and alerting
- …

Professional Certifications

- Certified Information Systems Auditor (CISA)
- Certified Information Systems Security Professional (CISSP)
- Certified Information Security Manager (CISM)

Information Security Standards

- ISO/IEC 27002:2005
  - Code of Practice for Information Security Management
- ISO/IEC 27001:2005
  - Information Security Management System - Requirements
- ISO/IEC 15408
  - Evaluation Criteria for IT Security
- ISO/IEC 13335
  - IT Security Management
- COBIT, ITIL, …

COBIT: Control Objectives for Information and related Technology
ITIL: Information Technology Infrastructure Library

Overview

- Computer Crimes
- Information Security
- **Privacy**

Importance of Personal Data Privacy

- One’s will and one’s freedom to protect, to use, to reveal data about oneself

- The level of protection and control affects one’s sense and feeling of security, or even actual physical security

- Personal Data can be considered as a kind of personal property/asset

Lawful/ Proper Privacy Data Usage

- Governments, corporations, institutions and even individuals sometimes need Personal Privacy Data for operation and activities
  - Census
  - Income data for taxation purpose
  - Personal identity and credit information for obtaining financial services
  - Health information for setting insurance policy
  - Home address for voting based on regional constituency
  - Phone number for dating!

- Data Privacy Laws and Agencies
- Privacy Policy Statement (PPS)
- Personal Information Collection Statement (PICS)

Protection of Privacy : Laws and Ethics
Data Privacy Laws and Agencies

Office of the Privacy Commissoner for Personal Data (PCPD, 個人資料私隱專員公署) in HK

Six Data Protection Principles (DPP) of the Personal Data (Privacy) Ordinance (個人資料(私隱)條例)

- **DPP 1** – Purpose and manner of collection
  - Personal data shall be collected for a purpose directly related to a function and activity of the data user; lawful and fair collection of adequate data; data subjects shall be informed of the purpose for which the data are collected and to be used.
- **DPP 2** – Accuracy and duration of retention
  - All practicable steps shall be taken to ensure the accuracy of personal data; data shall be deleted upon fulfillment of the purpose for which the data are used.

Protection of Privacy : Laws and Ethics
Data Privacy Laws and Agencies

- **DPP 3** – Use of personal data
  - Unless the data subject has given prior consent, personal data shall be used for the purpose for which they were originally collected or a directly related purpose.
- **DPP 4** – Security of personal data
  - All practicable steps shall be taken to ensure that personal data are protected against unauthorized or accidental access, processing or erasure.
- **DPP 5** – Information to be generally available
  - Formulates and provides policies and practices in relation to personal data.
- **DPP 6** – Access to personal data
  - Individuals have rights of access to and correction of their personal data. Data users should comply with data access or data correction request within the time limit, unless reasons for rejection prescribed in the Ordinance are applicable.

Privacy Policy Statement (PPS)

- Examples
  - PPS of PCPD, HKSAR
    - http://www.pcpd.org.hk/english/about/pps.html
  - PPS and Practices of Immigration Dept, HKSAR
    - http://www.immd.gov.hk/ehtml/statement.htm
  - PPS of RGS, CUHK
    - http://rgsntm.rgs.cuhk.edu.hk/rws_prd_life/rws_usrdoc/main0000_008c.asp

Without a Trace?

- How can we keep anonymous?
- How often we are anonymous?
  - …when we are using our own PC’s?
  - …when we are using our mobile phones?
  - …when we are not logging in?
  - …when we are shopping offline or online?
  - …what are “cookies”?

Internet Website Cookies

- When we visit a website, we may provide certain information such as username, password, color and layout preference, visit date and time, etc.
- A website may store such information on its server(s) AND/OR store such information on the computer you are using
- Cookies on the computer you are using is used for storing such information
- When you re-visit the same website on the same computer, the cookies will be sent to the website

Internet Website Cookies

- What are the advantages of using cookies?
- What are the risks associated with using cookies?
- Any suggestions?

All About Ourselves

- There may be lots of personal data sources about us:
  - Personal Blog and Facebook
  - Address book of our friends
  - Public accessible government data
    - Voters' Registry
    - Land and Property Registry
    - Company Registry
  - Corporate managed data sets
    - Credit database
    - Phone operators and ISPs'
    - Marketing firms and departments
    - Shipping information and invoices

Longer we Live, More we Expose

- Data fusion and data mining technologies could be used to reveal our personal data and identity from multiple data sets
- Avoid revealing personal data and identity in surveys and questionnaires
- Beware of participating in marketing campaigns such as lucky draws and souvenir traps

With reference to materials from:

A Gift of Fire

Third edition

Sara Baase

Chapter 2: Privacy

Chapter 5: Crime

also materials and photos from the Internet!

References

- HKCERT http://www.hkcert.org
- Office of the Privacy Commissioner for Personal Data (PCPD) http://www.pcpd.org.hk
- Privacy, Wikipedia http://en.wikipedia.org/wiki/Privacy
- Information security, Wikipedia http://en.wikipedia.org/wiki/Information_security
- Information security for general users: http://www.infosec.gov.hk/english/genuser/genuser.html
- Information security for IT professionals: http://www.infosec.gov.hk/english/itpro/itpro.html
- Information security in CUHK: http://www.cuhk.edu.hk/itsc/security/index.html

Disclaimer

- We do not provide legal advice and have no liability for any loss or damage caused to anyone relying on any information in this ppt