

Professional Ethics for Computer Science

Chapter 4: Privacy

Jie Gao

Computer Science Department

Stony Brook University

Privacy Issues

Internet privacy consists of privacy over the media of the Internet:

- the ability to control what information one reveals about oneself over the Internet, and
- to control who can access that information.

Privacy Issues

Example: You send an email through Yahoo mail, and the third party takes a look at it.

- Someone stealing your wireless network.
- Yahoo's system manager

To protect your privacy, use encryption.

Data Encryption

Cryptography

- science of *encoding* messages
- only sender and intended receiver can understand the messages
- key tool for ensuring confidentiality, integrity, authenticity of electronic messages and online business transactions

Encryption

- process of converting electronic messages into a form understood only by the intended recipients

Data Encryption (continued)

Encryption key

- a (large random) value applied using an algorithm to encrypt or decrypt text
- length of key determines strength of encryption algorithm

Private key encryption system

- single key to encode and decode messages
- issue of secretly distributing private key to sender/receiver paramount

Data Encryption (continued)

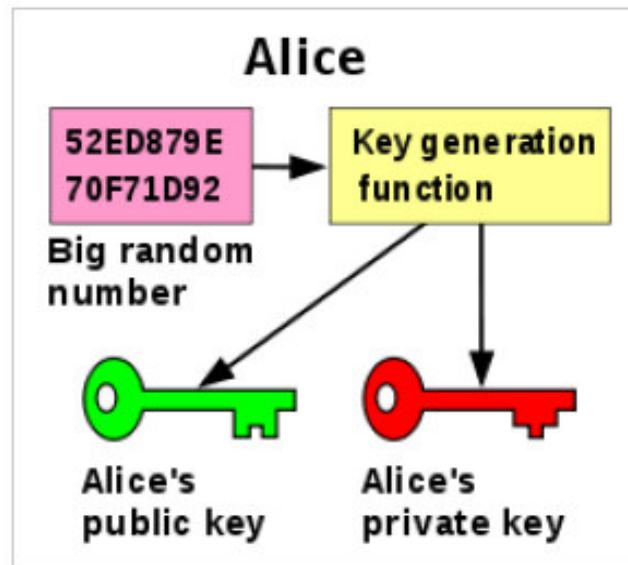
Public key encryption system uses two keys: public and private key

- message recipient's *public* key
 - readily available and used for encryption
 - Posted on the web
- message recipient's *private* key
 - mathematically related to public key
 - kept secret and used for decryption

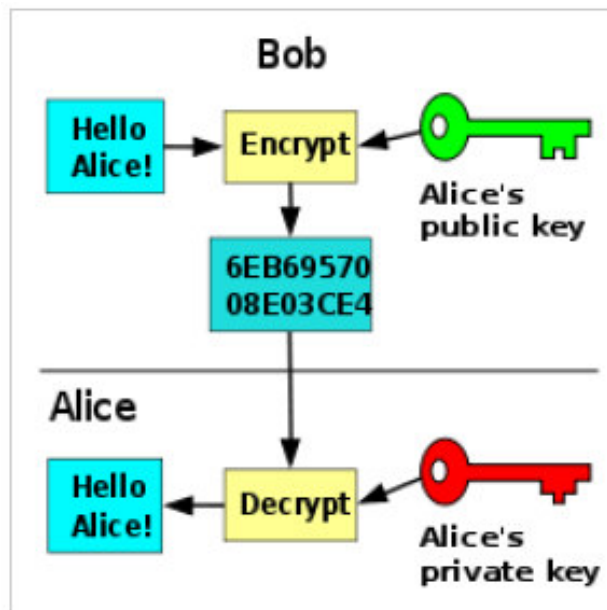
RSA - a public-key encryption algorithm (RSA keys typically 1024–2048 bits long)

RSA

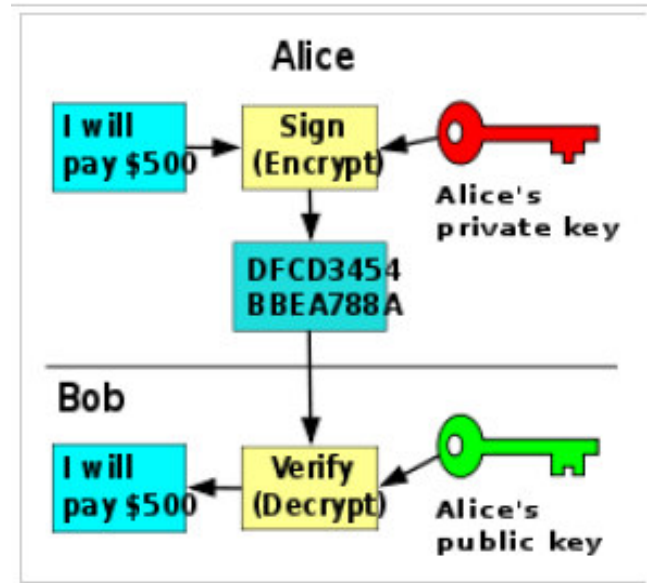
Key generation:



Encryption



Signature



Privacy Issues

Example: You send an email through Yahoo mail, and the third party takes a look at it.

- Someone stealing your wireless network.
- Yahoo's system manager

Home

Products

Topics

Preferences

Help

YAHOO! PRIVACY CENTER

Welcome to the Yahoo! Privacy Center—take a look around. You'll learn how Yahoo! treats your personal information, along with ways to control your preferences and settings. As always, Yahoo! is committed to gaining your trust.



WHAT THIS PRIVACY POLICY COVERS

INFORMATION COLLECTION AND USE

INFORMATION SHARING AND DISCLOSURE

COOKIES

CONFIDENTIALITY AND SECURITY

QUESTIONS AND SUGGESTIONS

 [Email](#)  [Print](#)



WHAT THIS PRIVACY POLICY COVERS

Yahoo! takes your privacy seriously. Please read the following to learn more about our privacy policy.

The federal government and technology industry have developed [practical tips](#) to help you guard against Internet fraud, secure your computer and protect your personal information.

How Yahoo! Uses Your Personal Information

This policy covers how Yahoo! treats personal information that Yahoo! collects and receives, including information related to your past use of Yahoo! products and services. Personal information is information about you that is personally identifiable like your name, address, email address, or phone number, and that is not otherwise publicly available.

This privacy policy only applies to Yahoo!

This policy does not apply to the practices of companies that Yahoo! does not own or control, or to people that Yahoo! does not employ or manage. In addition, some companies that Yahoo! has acquired have their own, preexisting privacy policies which may be viewed on our [acquired companies page](#).

Yahoo!'s participation in the Safe Harbor program

Yahoo! participates in the Safe Harbor program developed by the U.S. Department of Commerce and the European Union. To view our

Highlights

Relevant Advertising

By bringing content and advertising to you that is relevant and tailored to your interests, Yahoo! provides a more compelling online experience. Our customized "smart" services save you time and cut through the clutter. [Learn More about relevant advertising.](#)

RUMOR ALERT

An email circulating since 2000 provides inaccurate information about Yahoo!'s use of web beacons in Yahoo! Groups email messages. We'd like to clarify this once and for all. [Read more about how Yahoo! Groups uses web beacons.](#)

LATEST NEWS

INFORMATION SHARING AND DISCLOSURE

Yahoo! does not rent, sell, or share personal information about you with other people or non-affiliated companies except to provide products or services you've requested, when we have your permission, or under the following circumstances:

- We provide the information to trusted partners who work on behalf of or with Yahoo! under confidentiality agreements. These companies may use your personal information to help Yahoo! communicate with you about offers from Yahoo! and our marketing partners. However, these companies do not have any independent right to share this information.
- We have a parent's permission to share the information if the user is a child under age 13. Parents have the option of allowing Yahoo! to collect and use their child's information without consenting to Yahoo! sharing of this information with people and companies who may use this information for their own purposes.
- **We respond to subpoenas, court orders, or legal process, or to establish or exercise our legal rights or defend against legal claims.**
- **We believe it is necessary to share information in order to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of Yahoo!'s terms of use, or as otherwise required by law.**

Identity Theft

Theft of key pieces of personal information to gain access to a person's financial accounts

- using this info, ID thief may apply for new credit or financial accounts, register for college courses, etc—all in someone else's name

Information includes:

- name
- address
- date of birth
- Social Security number
- passport number
- driver's license number
- mother's maiden name

Identity Theft (continued)

Fastest growing form of fraud in the United States

- victims spend >600 hours over several years recovering from ID theft

Lack of initiative by companies in informing people whose data was stolen

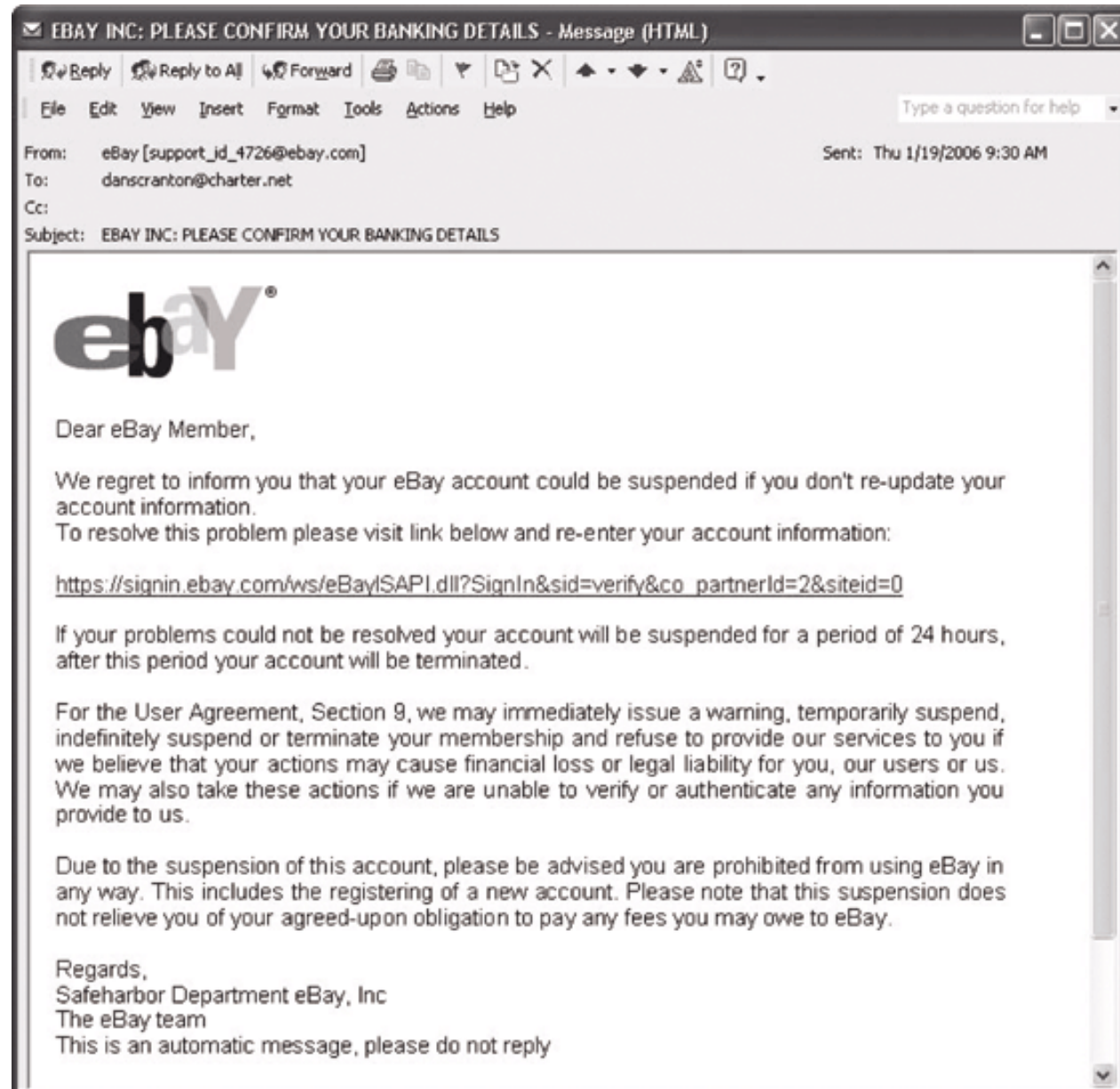
“The personal information of 90,000 people in a Stony Brook University database was accidentally posted to Google & left there until it was discovered almost two weeks later.”

Identity Theft (continued)

Phishing

- attempt to steal personal identity data
- by tricking users into entering information on a counterfeit Web site (spooof emails)
- spear-phishing - a variation in which employees are sent phony e-mails that look like they came from high-level executives within their organization

E-mail Used by Phishers



Identity Theft (continued)

Spyware

- keystroke-logging software downloaded to user's computer without consent
- enables the capture of:
 - account usernames
 - passwords
 - credit card numbers
 - other sensitive information
- operates even if an infected computer is not connected to the Internet
- records keystrokes until users reconnects; data collected then emailed to spy or posted to a web site

Identity Theft (continued)

Identity Theft and Assumption Deterrence Act of 1998 was passed to fight Identity fraud

- makes it a Federal felony (3-25 yrs in prison)

Consumer Profiling

Companies can collect info about consumers without their explicit permission!

Companies openly collect personal information about Internet users

- when they register at web sites, complete surveys, fill out forms or enter contests online

Consumer Profiling

Cookies

- text files a web site places on user's hard drive so that it can remember info
- examples: site preferences, contents of electronic shopping cart
- cookie are sent back to server unchanged by browser each time it accesses that server

Tracking software

- identify visitors to your web site from e.g. pay-per-click accounts

Consumer Profiling (continued)

Similar methods used outside the Web environment

- marketing firms warehouse consumer data
- for example, credit card purchases, frequent flier points, mail-order catalogue purchases, phone surveys

Databases contain a huge amount of consumer behavioral data

Consumer Profiling (continued)

Types of data collected while surfing the Web

- GET data: affiliated web sites visited and info requested
- POST data: form data
- Click-stream data: monitoring of consumer surfing activity

Four ways to limit or even stop the deposit of cookies on hard drives

- set the browser to limit or stop cookies
- manually delete them from the hard drive
- download and install a cookie-management program
- use anonymous browsing programs that don't accept cookies
 - e.g. anonymizer.com allows you to hide your identity while browsing

Consumer Profiling (continued)

Personalization software used by marketers to optimize number, frequency, and mixture of their ad placements

- ***Rules-based:***

uses business rules tied to customer-provided preferences or online behavior to determine most appropriate page views

- ***Collaborative filtering:***

consumer recommendations based on products purchased by customers with similar buying habits

- ***Demographic filtering:***

considers user zip codes, age, sex when making product suggestions

- ***Contextual commerce:***

associates product promotions/ads with content user is currently viewing

Amazon.com

Spamming

Transmission of same e-mail message to *large* number of people

Extremely inexpensive method of marketing

- \$1K vs. \$10K for direct-mail campaign
- 3 weeks to develop vs. 3 months
- 48hrs for feedback vs. 3 weeks

Used by many *legitimate* organizations

- example: product announcements

Can contain *unwanted and objectionable* materials

Email considered Spam: 40% of all email; Daily Spam emails sent: 12.4 billion; Daily Spam received per person: 6; Annual Spam received per person: 2,200; Spam cost to all non-corp Internet users: \$255 million; Spam cost to all U.S. Corporations in 2002: \$8.9 billion; States with Anti-Spam Laws: 26

Spamming (continued)

The *Controlling the Assault of Non-Solicited Pornography and Marketing* (CAN-SPAM) Act 2004

- says it is legal to spam but
 - spammers cannot disguise their identity
 - there must be a label in the message specifying that the e-mail is an ad or solicitation
 - they must include a way for recipients to indicate they do not want future mass mailings (i.e. opt out)
- may have actually *increased* the flow of spam as it legalizes the sending of unsolicited e-mail

Advanced Surveillance Technology

Camera surveillance

- U.S. cities plan to expand surveillance systems
 - London has one of world's largest public surveillance systems
- "Smart surveillance system"
 - singles out people acting suspiciously

Facial recognition software

- identifies criminal suspects and other undesirable characters
- yields mixed results
 - at Boston's Logan airport: 96 failures, 153 successes

Advanced Surveillance Technology (continued)

Global Positioning System (GPS) chips

- Placed in many devices to precisely locate users
 - cars, cellphones, etc.
- **Good:** accurately respond to 911 callers; real-time location-aware marketing
- **Bad:** wireless spamming from local restaurants etc, your whereabouts always known

Advanced Surveillance Technology

Provides exciting new data-gathering capabilities vs. personal-privacy issues

- **advocates:** people have no legitimate expectation of privacy in public places
- **critics:** creates potential for abuse – intimidation of political dissenters, blackmail of people caught with “wrong” person or in “wrong” place

Google's privacy policy

Video

<http://www.youtube.com/watch?v=2IKBke1puFw>