Chapter 12

Privacy and Digital Security

Red text added by Eric Lukens

Slides without Pearson footer added by Eric Lukens
About Me

• Eric Lukens
• IT Security Policy and Risk Assessment Analyst
• ITS-Network Services
• eric.lukens@uni.edu
• security@uni.edu
• http://www.uni.edu/elukens/
Legal Notice

The views and opinions expressed are those of the author and do not imply endorsement by the University of Northern Iowa.
I may provide some legal information, which is not the same as legal advice -- the application of law to an individual's specific circumstances. Always consult an attorney to determine if my information is appropriate to your particular situation.
My financial or tax information is provided for your personal information only, it cannot substitute for professional financial or tax advice. Always seek advice of a competent financial or tax advisor or accountant with any questions you may have regarding a financial or tax matter.
Computers are finicky things. Taking recommended computer actions may result in negative consequences on some computer systems.
Learning Objectives

• Explain the meaning of privacy; discuss the issues surrounding privacy of information
• List and explain the meaning of the OECD Fair Information Practices
• Discuss the issues concerning U.S. privacy: Opt-in/Opt-out, compliance/enforcement, coverage
• List the ways a computer can be compromised
• Explain the security methods used in public key cryptosystems (PKCs)
• Perform simple encryption from cleartext to cipher text and perform the reverse decryption [snakeoil]
Modern Devices and Privacy

• In the past, it was hard for people’s privacy to be violated without their knowledge.

• With modern technological devices, people’s privacy can be violated without their knowing it.

• Your image and your information deserves “sufficient safeguards against improper circulation.”
Privacy: Whose Information Is It?

• Buying a product at a store generates a transaction, which produces information.
  – Paying with cash generally ensures anonymity
  – Paying by check, credit card, or debit card
  – Purchasing through mail order or on the Internet
  – Providing a “preferred customer” number
  – Buying a product that must be registered for a service agreement or warranty
How Can the Information Be Used?

- Transaction information is a normal part of conducting business (keeping a record until our check clears)
  - The information belongs, then, to the store
- If the store decides, based on your previous purchases, to send you ads for other items, the store is using the information for the standard business practice of generating more business
How Can the Information Be Used?

- If the store sells your name to others has the information been misused?
  - Those other businesses are only trying to generate more business.
  - Is it misused if the information gets to the newspaper and is published?
  - Has the store broken the law?
Controlling the Use of Information

• Who controls the use, if any, of the transaction information?

• There are four main possibilities:

  1. **No Uses.** The information ought to be deleted when the store is finished with it.

  2. **Approval or Opt-in.** The store can use it for other purposes, but only if you approve.

  3. **Objection or Opt-out.** The store can use it for other purposes, but not if you object.

  4. **No Limits.** The information can be used any way the store chooses.
Controlling the Use of Information

• [Surprise!] There is also a fifth possibility, *Internal Use*:
  – The store can use the information to conduct business with you (keeping your address, for example), but for no other use
  – It would not include giving or selling your information to another person or business, but it may not require your approval either
Controlling the Use of Information

• If the transaction took place in much of the developed world [exaggeration, the vast majority of the world’s population does not have this protection] outside the US, the law and standards would place it between (1) and (2) on the spectrum, but very close to (1).

• If the transaction occurred in the US, the law and standards would place it between (3) and (4) on the spectrum, but very close to (4)
Controlling the Use of Information

• Many Americans assume that there is a privacy law that is close to the fifth case, internal use [They are making the assumption that most people care. When asked people say they care, but their actions do not seem to correlate to their concern. Critics would say this is because they are unaware of what happens behind-the-scenes, but look at what people post on social media.]
A Privacy Definition

• *Privacy*: The right of people to choose freely under what circumstances and to what extent they will reveal themselves, their attitude, and their behavior to others.

• Privacy is difficult to define [So does that mean what you put above is wrong?]

• Generally, privacy concerns four aspects of our lives: our bodies, territory, personal information, and communication
A Privacy Definition

• This definition emphasizes first that it is the person who decides the circumstances and the extent to which information is revealed, not anyone else.

• Second, it emphasizes that the range of features over which the person controls the information embodies every aspect of the person—themselves, their attitudes, and their behaviors.
Enjoying the Benefits of Privacy

• Sometimes we want publicity, sometimes we don’t
• Strong privacy laws insure that we control the dissemination of our information
Threats to Privacy

• What are the threats to privacy?
• There are only two basic threats:
  – Government
  – Business
  – (Snooping or gossiping private parties, will be handled by security)
Threats to Privacy

• Historically, the governmental threat of spying on its citizens, worries people the most

• The business threat is a more recent worry

• There are two types of business threats:
  – Surveillance of employees [In US, by law, anything you do on company computer or network is free for the snooping and can be used for any legal purpose.]
  – The use of business-related information for other purposes
Voluntary Disclosure

• In principle, a person can enjoy perfect privacy by simply deciding not to reveal anything to anyone

• It may be in our interest to reveal private information, freely in exchange for real benefits

  • If you’re using an online service that’s free, YOU are the product.
Benefits of Voluntary Disclosure

• Doctors receive our personal information so they can help us stay healthy
• Credit card companies get our personal information to check our credit record in exchange for the convenience of paying with a card
• Employers read our email at work, because we are using the employer’s computer for a job
Benefits of Voluntary Disclosure

• The government may have information on us regarding our parents’ names and birthplaces, our race and ethnicity, etc. for the purpose of enjoying the rights of citizenship.

• How private can we be when we reveal so much about ourselves, our attitudes, and our behavior?
Fair Information Practices

• If people or organizations are free to give or sell the information to anyone else, they are also revealing information about us.
• Our privacy is compromised
• There must [WP:EDITORIAL] be clear guidelines adopted for handling private information:
OECD Fair Information Practices

• In 1980 the Organization for Economic Cooperation and Development (OECD) developed an eight-point list of privacy principles that became known as the Fair Information Practices

• They have become a widely accepted standard
OECD Fair Information Practices

- The public has an interest in these principles becoming law [Citation Needed]
- The principles also give a standard that businesses and governments can meet as a “due diligence test” for protecting citizens’ rights of privacy, thereby protecting themselves from criticism or legal action
OECD Fair Information Practices

• An important aspect of the OECD principles is the concept that the **data controller** (the person or office setting the policies) must interact with individuals about their information, if any, and must be accountable for those policies and actions!
OECD’s Fair Information Practices

• The standard eight-point list of privacy principles.
  – Limited Collection Principle
  – Quality Principle
  – Purpose Principle
  – Use Limitation Principle
  – Security Principle
  – Openness Principle
  – Participation Principle
  – Accountability Principle
Table 12.1 A brief explanation of the OECD’s Fair Information Practices guidelines.

<table>
<thead>
<tr>
<th>Limited Collection</th>
<th>There should be limits to the personal data collected; data should be collected by fair and lawful means, and with the knowledge and consent of the person whenever possible.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>The purposes for collecting personal data should be stated when it is collected; the uses should be limited to those purposes.</td>
</tr>
<tr>
<td>Quality</td>
<td>The data should be relevant to the purpose of collection; it should be accurate, complete, and up-to-date.</td>
</tr>
<tr>
<td>Use Limitation</td>
<td>Personal data should not be disclosed or used for purposes other than stated in the Purpose Principle, except with the consent of the individual or by the authority of law.</td>
</tr>
<tr>
<td>Security</td>
<td>Personal data should be protected by reasonable security measures against risks of disclosure, unauthorized access, misuse, modification, destruction, or loss.</td>
</tr>
<tr>
<td>Openness</td>
<td>There should be general openness of policies and practices about personal data collection, making it possible to know of its existence, kind, and purpose of use, as well as the contact information for the data controller.</td>
</tr>
<tr>
<td>Participation</td>
<td>An individual should be able to (a) determine if the data controller has information about him or her, and (b) discover what it is. If the request is denied, the individual should be allowed to challenge the denial.</td>
</tr>
<tr>
<td>Accountability</td>
<td>The data controller should be accountable for complying with these principles.</td>
</tr>
</tbody>
</table>
Privacy Worldwide

• Privacy is not enjoyed at OECD standards in much of the world [Though little is gathered in many of those countries on people without access to technology.]

• Privacy often comes in conflict with the goals of businesses and governments:
  – Example, the United States has not adopted the OECD principles, possible [Something amiss here] because many U.S. companies profit by buying and using information in ways that are inconsistent with the OECD principles
Privacy Worldwide

• The European Union (EU) issued a benchmark law incorporating the OECD principles
  – EU Directive requires that data about EU citizens be protected by the standards of the law even when it leaves their country [Don’t assume this is only for benevolence of their citizens’ privacy. This law also gives a huge boost to their tech industry, which is a documented goal and strategy of the EU, along with strategic lawsuits against large US-based companies (Google, Microsoft, et al.)]

• Other countries adopted it as well including Australia, Canada, Hong Kong, and New Zealand
US Approach

• US uses a *sectoral* approach
• Rather than a single privacy standard, specific regulations apply to specific sectors
• HIPAA regulates medical information privacy
• Other specific laws for auto registration, video rental, *Education (FERPA)*, etc.
Business as Usual [WP:NPOV]

• US businesses and government gathers data contrary to the OECD rules [Only under a supposed moral obligation.]

• Patriot Act makes it a crime to say that data gathering is taking place [That’s a major oversimplification. Judges have always had that power as well for search warrants. Wiretaps wouldn’t work if the people knew right away that a tap was in place. What’s new is the National Security Letter, that is often rubber-stamped by the FISA Court, and the frequency and large-scope of these warrants—including one for a daily report of all calls occurring on the nation’s largest cell phone carrier.]
Almost every store and company you do business with has information about you
– if you want to know what they are doing with that information you must read their privacy policies
– often it says, “We use the information however we like.” [Yep, though they generally do have to tell you what they plan to do, and there have been successful consumer pushbacks against changes when they were too extreme.]
Opt-in/Opt-out

• An important test of privacy policies the opt-in/opt-out test
• When a data collector wants permission to repurpose data, how is that attained?
• Opt-in: The subject must give explicit permission
• Opt-out: Permission is assumed unless the subject takes action to object
• Frequently, permission is assumed when the subject continues to use the collector’s services
Targeted by Target

• “Big Data” is the statistical analysis of huge information archives
• The retailer Target can track the purchases of a customer who has a loyalty card
• Target can figure out if a woman is pregnant from her buying habits
  – was able to develop a ‘pregnancy prediction’ score by analyzing the customer’s purchases
Government, as Usual [WP:NPOV]

• In June 2013, Edward Snowden revealed that the U.S. government was collecting complete metadata records from telephone carriers – it is still unknown if these allegations are true*

• The government was also collecting online activity from Facebook, Microsoft, Google, etc.

• Included data to calls to other countries with OECD laws in place [Silly, that’s the part of the NSAs stuff that is constitutional.]
Tracking

• In electronic privacy, tracking is used in two different ways
  – **online tracking**: Web site automatically sending details about your visit to other content providers (to show you ads and other products)
  – **cell phone tracking**: positioning information, used to map your physical location
Online Tracking

- We assume it is used to target advertising and marketing organizations.
- But anyone could arrange to follow your “click streams”.
- HTTP has a “Do Not Track” flag that tells Web servers your tracking preferences.
  - It is up to the Web server to honor your request.
- Browsers will send the flag, but you must set an option to tell them to do so.
Even More Private

• “Do Not Track” is controversial because consumer behavior is very valuable, but people [some people, especially the author] don’t want anyone following them around (even online)

• Two additional protections [I do not recommend these]
  – National Advertising Initiative opt-out program
    • http://www.networkadvertising.org/choices/
  – DoNotTrackMe offers a free blocker
    • https://www.abine.com/index.php
Anti-Tracking Software

• Adblock Plus https://adblockplus.org/, provides option on site to add known trackers and social media plugins. Blocks ads too. Integrates with most browsers on desktops.

• Ghostery https://www.ghostery.com, provides options to see who is tracking you on various sites and block as desired.

• Privacy Badger https://www.eff.org/privacybadger, made by EFF to block spying ads and trackers.

• Options for mobile too varied depending on device, do research online.
Private Browsing

• “client side” facility
  – only concerns the information stored locally on your machine, not what's stored on servers
• all cookies, cached files, and history are deleted at the end of the session
• useful when using a public computer
Cell Phones

• Phone companies log cell phone calls
  – Call details: numbers, duration, etc.
  – Cell towers used, which determines the
general location of the phones, even if
“location services” (GPS) is off [Needed
for customer billing and payment from
carrier to roaming tower.]
• These records are kept for various periods
  by the various phone companies [Wow, what a
completely worthless statement.]
Cell Phones

• National Security Agency collects many of these records [Foreign spy agencies do just as much on their domestic networks as well—even in OECD countries!]

• May keep them indefinitely

• Combine data from all phone providers

• Form a large database which invites misuse
  – No opt-out from official uses
  – Unauthorized private use by officials
<table>
<thead>
<tr>
<th>Information Type</th>
<th>Verizon</th>
<th>T-Mobile</th>
<th>AT&amp;T/Cingular</th>
<th>Sprint</th>
<th>Nextel</th>
<th>Virgin Mobile</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subscriber Information</td>
<td>Post-paid: 3–5 years</td>
<td>5 years</td>
<td>Depends on length of service</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Call detail records</td>
<td>1 rolling year</td>
<td>Pre-paid: 2 years</td>
<td>Pre-paid: varies</td>
<td>18–24 months</td>
<td>18–24 months</td>
<td>2 years</td>
</tr>
<tr>
<td>Cell towers used by phone</td>
<td>1 rolling year</td>
<td>Officially 4–6 months, really a year or more.</td>
<td>From July 2008</td>
<td>18–24 months</td>
<td>18–24 months</td>
<td>Not retained—obtain through Sprint</td>
</tr>
<tr>
<td>Text message detail</td>
<td>1 rolling year</td>
<td>Pre-paid: 2 years</td>
<td>Post paid: 5–7 years</td>
<td>18 months (depends on device)</td>
<td>18 months (depends on device)</td>
<td>60–90 days</td>
</tr>
<tr>
<td>Text message content</td>
<td>3–5 days</td>
<td>Not retained</td>
<td>Not retained</td>
<td>Not retained</td>
<td>Not retained</td>
<td>90 days (search warrant required with “text of text” request)</td>
</tr>
<tr>
<td>Pictures</td>
<td>Only if uploaded to Web site (customer can add or delete pictures any time)</td>
<td>Can be stored online and are retained until deleted or service is canceled</td>
<td>Not retained</td>
<td>Contact provider</td>
<td>Contact provider</td>
<td>Not retained</td>
</tr>
<tr>
<td>IP session information</td>
<td>1 rolling year</td>
<td>Not retained</td>
<td>Only retained on non-public IPs for 72 hours. If public IP, not retained.</td>
<td>60 days</td>
<td>60 days</td>
<td>Not retained</td>
</tr>
<tr>
<td>IP destination information</td>
<td>90 days</td>
<td>Not retained</td>
<td>Only retained on non-public IPs for 72 hours. If public IP, not retained.</td>
<td>60 days</td>
<td>60 days</td>
<td>Not retained</td>
</tr>
<tr>
<td>Bill copies (post-paid only)</td>
<td>3–5 years, but only last 12 months readily available</td>
<td>Not retained</td>
<td>5–7 years</td>
<td>7 years</td>
<td>7 years</td>
<td>n/a</td>
</tr>
<tr>
<td>Payment history (post-paid only)</td>
<td>3–5 years, check copies for 6 months</td>
<td>5 years</td>
<td>Depends on length of service</td>
<td>Unlimited</td>
<td>Unlimited</td>
<td>n/a</td>
</tr>
<tr>
<td>Store Surveillance Videos</td>
<td>Typically 30 days</td>
<td>2 weeks</td>
<td>Depends. Most stores carry for 1–2 months</td>
<td>Depends</td>
<td>Depends</td>
<td>n/a</td>
</tr>
<tr>
<td>Service Applications</td>
<td>Post-paid: 3–5 years</td>
<td>Not retained</td>
<td>Not retained</td>
<td>Depends</td>
<td>Depends</td>
<td>Not retained</td>
</tr>
</tbody>
</table>

*Figure 12.2 Retention periods for information held by cellular phone providers.*
Cookies

• Cookies are a standard computer science concept originally used by Netscape engineers to connect the identity of a client across a series of independent client/server events.

Like everything, cookies are a tool that can be used for good or evil. They can be used to maintain your identity to a site on multiple visits. They can store data locally so the server doesn’t have to. Without cookies, the web as we know it would not work.
Cookies

• Imagine this is your bank’s server, and you are a client
• The server is helping many clients, and to know who’s who, the server stores an identification record called a **cookie** on each one [and hopefully does server-side session monitoring as well]
Cookies

- Cookies are exchanged between the client and the server on each transmission of information, allowing the server to know which of the many clients is sending information.
Cookies

Many sites use cookies, even when the interaction is not intended to be as secure as a bank transaction (National Air and Space Museum sent the above).

- The meaning of the fields is unimportant.
- The first is the server and the last is the unique information identifying the session.
Cookie Abuse

• There is a loophole called a third-party cookie [not always “evil,” usually though]
• A cookie is exchanged between the client and server making the interaction private
• But, if the Web site includes ads on its page, the page may link to the ad company to retrieve the ad
• This new client/server relationship places a cookie on your computer
• The various ad trackers can monitor trends across all pages you visit with that ad.
Cookie Abuse

• All browsers allow users to control how cookies are processed
• You could turn them off, or force the browser to ask you every time whether you will accept a cookie or not [good luck with that]
• Turning off cookies prevents you from being able to bank online
• Simply set your browser’s cookie policy to your own comfort level
• Consider clearing on exit or disabling third-party cookies
The Right To Be Forgotten

• EU thing currently – trying to force it beyond their borders.

• It can be hard to escape your past on-line
  – An arrest after which you were cleared
  – A minor crime you did commit, but long ago
  – A video of something silly you did in college

• Google will find them

• Should sources add some notation?

• Should search engines bury the link?

• A developing issue

• Ask yourself this, would we prevent people from searching published news articles on LexisNexis or Infotrac because somebody does not want that information known any longer?

How about looking through old newspaper clippings? Is this concern just because it is *EASY-TO-DO* now compared to the past?
Identity Theft

- **Identity theft** is the crime of posing as someone else for fraudulent purposes
  - Using someone else’s credit card
  - Taking a loan in someone else’s name
- When a data collector fails to secure the contents of a database, third parties can misuse the data
- Identity theft is a frequent result
Identity Theft

• In 2005, ChoicePoint leaked personal data on 145,000 persons
  – Or just weren’t careful whom they sold to
• Initially admitted to only 32,000, later forced to admit the rest
• Over 800 identity thefts were attributed to this failure
• The US government fined ChoicePoint $10M, plus $5M in consumer redress
• There are tons of breaches, why’d they pick ChoicePoint?
Ah, here’s why (from Wikipedia):

ChoicePoint was a data aggregation company based in Alpharetta, near Atlanta, Georgia, United States, that acted as a private intelligence service to government and industry. It was purchased in February 2008 by Reed Elsevier (parent corporation of LexisNexis) in a cash deal for $3.6 billion USD. The company was rebranded as LexisNexis Risk Solutions.

ChoicePoint combined personal data sourced from multiple public and private databases for sale to the government and the private sector.
Identity Theft

• [https://www.annualcreditreport.com](https://www.annualcreditreport.com)
• Check credit report annually for problems (or 3 times a year)
• Always read account statements
• Report problems immediately to the account provider and the credit reporting agencies to put a fraud alert on your file
• Police report/report to FTC
Identity Theft

• Debit card vs. credit card
  – Credit Card $50 liability, generally $0
  – Banking PIN unlimited liability

• 60 day banking rule

• https://www.optoutprescreen.com

• Credit Freeze
  – Each agency, $10 or free with police report

• Fraud Alert
  – Report to one, forwarded to others

• https://www.dmachoice.org/
• https://donotcall.gov/
Signs of ID Theft

• Unusual or unexplainable charges on your bills
• Phone calls or bills for accounts, products, or services that you do not have
• Failure to receive regular bills or mail
• New, strange accounts appearing on your credit report
• Unexpected denial of your credit card
Digital Security

• Computer security is a topic that is in the news almost daily
• Remember the long list of “dos and don’ts” for online behavior?
  – Do check with the sender before opening an attachment you’re unsure about
  – Don’t fall for phishing emails
  – And the others from Chapter 11
Phishing

- Don't email personal or financial information—ever. Any legitimate entity that asks you to needs to change their business practices.
- Don't reply to email or pop-up messages that ask for personal or financial information, and don't click on links in the message.
- Never provide your passwords to anyone. UNI will not ask for them, nobody else should either.
Phishing

• If it sounds too good to be true, it probably is.
• Use sound judgment. Ask yourself if a particular request received makes sense.
• While not universal trait, many phishing attempts include poor spelling and grammatical errors.
• Be very suspicious of any request to “verify your information.”
CatID Self-Service

CatID SignOn

Username: 
Passphrase: 
Date of Birth: 

What is my username?

Submit

Maintained by Information Technology Services.
Send comments or suggestions to the Computer Consulting Center.
Last Updated: 05/29/2013

Copyright © 2014 University of Northern Iowa. All rights reserved. | Privacy Statement | Policies & Procedures
For security reasons, please Log Out and Exit your web browser when you are done accessing services that require authentication!

**What is my CatID?**

Your CatID is the combination of your username and passphrase used for systems authenticated through the Central Authentication System. The CatID logo is your clue to use this username/passphrase combination to log in. Click here for more information.

**Forgot your passphrase?**

Use the CatID Self-Service Passphrase Reset to answer your Challenge Questions and reset your passphrase. Note: You must have previously set your Challenge Questions in order to reset your passphrase.

**First time user**

Information about your new CatID including initial login help.

**Passphrase requirements**

See complete passphrase requirements.

**Best viewing tips**

Your browser must support SSL encryption, Javascript, allow pop-ups, and have cookies enabled. See more information.
The Risks: What can happen?

• **Mischief**: infecting a computer, causing a nuisance, erasing files, trashing files, etc

• **Information theft**: stealing personal information

• **Spying**: surreptitiously recording videos of the user, logging keystrokes, compromising secure online activities

• **Resource theft**: taking over a computer
Terms and Jargon

• **Malware**: software that harms computers
• **Virus**: shared program that contains code to reproduce itself
• **Worm**: program that is often embedded in an email attachment, reproduces itself and sends a copy to everyone on your contact list
• **Exploit**: when software takes advantage of bugs in commercial software
• **Trojan**: apparently benign, but malicious, program that performs unauthorized activities
What Does Malware Do?

- **Backdoors**: software that creates an access path allowing attackers to run any program on your computer
- **Trojans**: may record every key you type (trying to find passwords), extort money, watch for banking and credit card information
  - Watch-out for crypto-locker type Trojans, demand a ransom to get your data back
- **Rootkits**: infects your computer and then fights back against security systems
Your Browser - WOT

• Web of Trust
• “WOT’s traffic-light style rating system can be understood by the smallest of web surfers. Green means safe, yellow means caution and red means stop.”
• Can set to block “red” sites
• Can block adult content***
Anti-Malware Software (Windows)

- Plenty in the stores, most of those are fine.
- Free ones as well, they work ok.
  - Avast
  - Avira
  - Microsoft Security Essentials
  - AVG Free has had problems in the past, paid versions are fine.
- Non-commercial use only
Anti-Malware Software (Mac)

• As with Windows, several paid solutions, most are fine.
• Free solutions as well
  – Sophos – Quite Good Actually
  – Avast
    • http://www.avast.com/free-antivirus-mac
  – Avira
    • http://www.avira.com/en/avira-free-antivirus
• Non-commercial use only
Plan of Action

• Turn off Bluetooth when not in use
  • Stores can track you with wifi broadcasts from your phone as well—unless you have an iPhone, which lies until you actually connect to a network

• Keep your phone and other computers locked

• Do not automatically click on email attachments

• Never enter sensitive information in a pop-up [or any site that doesn’t deserve it]
Plan of Action

• Thinking of getting something for nothing
  – Think again
• Know where you’re going
  –<a href=”www.evil.net”>nice.com</a>
• Be somewhat skeptical
• Use extreme care when visiting notorious sites [“Notorious” is a euphemism for what now?]
If Something Really Bad Happens

• Turn off your computer immediately
• Use a different computer to do a web search about what happened
• Use an external source for the OS to reboot [I think they meant rebuild, If infected, backup data, reinstall the OS from Microsoft, Apple, or computer manufacturer media.]
Plan of Action

• Run “modern” software
• Install updates often
• Install anti-virus software [aka anti-malware]
• Set your Wi-Fi router to security level of at least WPA2 [and choose good PSK]
• Password-protect your phones and computers with appropriate passwords (chapter 11)
• Use your knowledge, be wise
Passwords

• Only thing that stops people from getting into your stuff.
• Consider password safe
Passwords

• Passphrases are better if you can use them
  – My cat Willow demands food at 5:00AM.

• Creative passwords
  – Ittr@b0htrbikfa
  – I'm trying to read a book on how to relax, but I keep falling asleep.
Uncommon (non-gibberish)
Base word

Order unknown

Common substitutions

Numerical

Punctuation

Troub4dor & 3

Difficulty to guess: Easy

Difficulty to remember: Hard

Correct horse battery staple

Difficulty to guess: Hard

Difficulty to remember: You've already memorized it

2^28 = 3 days at 1000 guesses/sec (plausible attack on a weak remote web service. Yes, cracking a stolen hash is faster, but it's not what the average user should worry about.)

2^44 = 550 years at 1000 guesses/sec

Through 20 years of effort, we've successfully trained everyone to use passwords that are hard for humans to remember, but easy for computers to guess.
Encryption

• Information sent over the Internet is liable to interception
• WiFi uses radio signals that can be received by anyone in range
• Wired networks can be snooped by other connected computers
• *Encryption* is used to keep your messages hidden from snoops [Not hidden, unreadable. Unless you’ve mastered quantum communications.]
Encryption

• Your readable message is **cleartext**
• It is transformed into gibberish known as **ciphertext**
• Using a magic number called a key
• The two ends of communication agree on a **key**
• This same key is used to decode the ciphertext at the receiving end
• There are many encryption algorithms
Encryption & Decryption

- One-way cipher: Encryption system that cannot be easily reversed (For example, used for passwords and message validation—making sure the data has not been modified.)
  - P@ssw0rd=161ebd7d45089b3446ee4e0d86dbcf92
- AES, DES, 3-DES, Twofish, Blowfish, Serpent
- Diffie-Hellman key exchange
- RSA
- Prime numbers, Random Numbers, Elliptic Curve Cryptography
Encryption

• Example encryption algorithm:
  1. The sender breaks the message into groups of letters
  2. “Multiply” each group of letters times the key
  3. Send the “products”/results from the “multiplications” to the receiver
  4. The receiver “divides” the “products” by the key to recreate the groups
  5. Assemble the groups into the message
Encryption

• This works because the math works [wtf]

• The “reversibility” of encryption makes them 2-way ciphers
  – Only the sender and receiver know the key, making the products useless numbers

• This is a secure communication [not with your example]

• The technique just explained is form of private key encryption, or symmetric-key cryptography
Encryption Example

1. Break into groups, say, ME ET b@ b9. (The blank is a letter, too; I have coded as b.) These letters are, when the ASCII is converted to decimal: 7769 6984 3264 3257.

2. “Multiply” each group by the key, 13:
   7769 × 13 = 100997
   6984 × 13 = 090792
   3264 × 13 = 042432
   3257 × 13 = 042341
   (The “lost zeroes” make all number six digits)

3. Send the “products” 100997 090792 042432 042341 to the receiver.

4. The receiver “divides” by the key, 13:
   100997/13 = 7769
   090792/13 = 6984
   042432/13 = 3264
   042341/13 = 3257
   producing numbers mapped by ASCII: ME ET b@ b9

5. Reassembling the message, MEET @ 9.
Cryptosystem Schematic Diagram

Figure 12.4 Schematic diagram of a cryptosystem. Using a key $K_{SR}$ known only to them, the sender encrypts the cleartext information to produce a cipher text, and the receiver decrypts the cipher text to recover the cleartext. In the middle, where the content is exposed and can be snooped, it is unintelligible.
Private Key Encryption

• Real encryption systems use much longer blocks (hundreds of letters) and larger keys
• Multiplication, division are not the only operations that can be used for encryption
• All that is needed is for an operation to have an inverse (divide is the inverse of multiply)
Private Key Encryption

• Private key encryption works very well
• Only one small problem: The sender and receiver must agree on the key, which means they need to communicate somehow
• And communicate without interception
• Usually, they meet face-to-face (they can’t email, they don’t have a key yet!)
Public Key Encryption

• To avoid that face-to-face meeting, publish the key!

• Requires a key with very special properties:
  – Encryption and decryption use different keys
  – The encryption [public] key cannot decrypt

• Only the encryption [public] key is published [Secret key often password protected itself with layer of symmetric encryption]
Public Key Encryption Steps

• The receiver computes key $K$ based on two large prime numbers
• The receiver publishes $K$, and the sender:
  1. Breaks up the message into blocks as before
  2. Cubes each block, and divides by $K$, keeping only the remainders
  3. Transmits the remainders

That’s not quite right, close though.
Public Key Encryption Steps

• To decrypt, the receiver:
  4. Raises each remainder to a high power determined by the prime numbers and known only to him
  5. The receiver divides by $K$, too, and saves only the remainders, which are the original blocks.
  6. The receiver assembles the message

That’s not quite right, close though.
Public/Private Key

Alice

Large Random Number

Key Generation Program

Public

Private
Public/Private Key

Alice

I will pay $500

Sign (Encrypt)

DFCD3454 BBEA788A

Alice's private key

Bob

I will pay $500

Verify (Decrypt)

Alice's public key
Public/Private Key

Alice

Bob's public key

Alice's private key

Combine keys

751A696C
24D97009

Alice and Bob's shared secret

Bob

Alice's public key

Bob's private key

Combine keys

751A696C
24D97009

Alice and Bob's shared secret
Encryption & Decryption

• Typically, data is encrypted with a symmetric encryption key randomly chosen by the computer, BUT, the symmetric key is transmitted with the file.
• The symmetric key is then encrypted and can only be decoded by the private key
• Public/Private (asymmetric) encryption is slow, so it is only used to encrypt the symmetric key.
• Keys chosen using random numbers and large primes. The key selection and random numbers are the primary vulnerabilities of concern right now, not the encryption algorithm itself.
Encryption & Decryption

• Data can also be targeted while it is being viewed or before it is even encrypted if the computer is compromised.

• Edward Snowden used software called GPG—used offline computer with the secret key. Encrypted and decrypted documents only on the offline machine. Used second internet machine to transmit and receive.

• Some Attacks on Encryption:
  – Prime number factorization.
  – Plain text attacks.
  – Side-channel attacks.
How Do We Know It Works?

• \( K \), the magic public key, is just two prime numbers, \( p \) and \( q \), multiplied together
• It is possible to figure out those two numbers from the published key in theory.
• This process, called factoring, is tough if the numbers \( p \) and \( q \) are large (60 digits apiece)
• It is impractical to factor them no matter how powerful the computer! [Well, maybe.]
Redundancy Is Very, Very, Very Good

• Data can be lost
  – Disasters: fire, flood, etc.
  – Theft
  – Hackers
  – Disks simply wear out eventually

• It’s nice to have a back-up copy
Backing Up a Personal Computer

• First, you need a place to keep the copy, and you need software to make the copy
• The two easiest “places” to keep the copy are on an external hard disk or “in the cloud”
• The “cloud” company’s computers store the information for you and they take responsibility of keeping it available to you
Backing Up a Business

• Take precautions with your technology!
• Businesses archive files daily and store these backups off-site
• They have a system recovery team to clean up after a disaster strikes
• They also have system redundancy—multiple computers performing the same work, so that when one fails, another is up and running
Fault Recovery Program

• Full backup
  – A complete copy of everything written on the system as of a date and time

• Partial backup [incremental or differential]
  – Changes since the last full (or partial) backup are saved [incremental]
  – “Changes” means to keep a copy of any files or folders that have been created or modified since the full backup
  – Differential – all changes since the last full.
Fault Recovery Program

• After a disaster, recover by installing the last full backup copy

• Then make the changes saved in the partial backups in order

• Continue with each partial backup until the most recent [differential’s advantage since only the full and the one differential need to be restored]

• That’s as close to “full recovery” as possible
Backups

• You don’t have to back up the following:
  – Information that can be recreated from some permanent source [Unless recreation time is so long as to be cumbersome, which happens more than you might think.]
  – Information that was saved but that has not changed [So, stuff in a previous backup?]
  – Information that you don’t care about [Which probably should be deleted. If you can’t delete it, then it is data you care about.]
Recovering Deleted Information

• Backups are usually kept a long time [Depends really. In some places the goal is only disaster recovery, in which case you want to restore to a recent backup, not an old one. Other places retain deleted data and old versions for long periods for recovery. Often retentions are based on data type and business needs balanced against the cost of the backups.]

• If you accidentally delete important files, file restoration (that backup copy!) is great!

• You can recover your accidentally-deleted file
Recovering Deleted Information

• Backups can also work against you
  • Companies often have a data retention schedule. Some even use products to force data to be deleted when it expires.

• Backups can save evidence of crimes or inappropriate behavior

• Email is hard to get rid of: when you push send
  – One copy in the sent folder
  – Another on the server
  – Eventually one in the recipient’s mail box
Summary

• Revealing personal information can be beneficial, so the people and organizations that receive the information must keep it private [WP:EDITORIAL]
  – The guidelines for keeping data private have been created by several organizations, including the Organization for Economic Cooperation and Development (OECD)
Summary

• Guidelines often conflict with the interests of business and government, so some countries like the United States have not adopted them
  – Because the United States takes a sectoral approach to privacy, adopting laws only for specific business sectors or practices, much of the information collected on its citizens is not protected by OECD standards
Summary

• The Do Not Track flag should be set, and DoNotTrackMe should be installed to avoid third parties building a profile of your Web surfing behavior [Not that effective]

• The best way to manage privacy in the Information Age is to have OECD-grade privacy laws [WP:EDITORIAL]

• There are two encryption techniques: private key and public key [No, no, no. Symmetric (just a PW) and Public/Private]
Summary

• Public key cryptography (PKC) is an amazing idea built on familiar concepts [well, that’s nice]

• Computer scientists have not yet proved the invincibility of the RSA scheme, but it can be “made more secure” simply by increasing the size of the key. [Again, not necessarily true.]
Summary

• Viruses and worms cause damage
  – We can reduce the chance of infection by installing and running anti-virus software
  – We must be aware of hoaxes and phishing scams

• We can implement a plan of action to ensure that our personal computers remain private and secure
Summary

• Backing up computer files is an essential safeguard
  – It ensures that your files will survive for a long time
  – Whether you want them or not