## Security

- Discuss Web security and encryption
- Email security

- Chapter 2



## Acceptable Use Policies

- All computer accounts and some public Internet servers are subject to an acceptable use policy
- An AUP is a policy that outlines appropriate use of the Internet and is enforced by system administrators

- Q1: Does Pacific University have an AUP?
- Q2: Can you find it?



## Security

- What do we mean by security?
  - Network security
    - send data across the Internet securely
    - getting data safely from the user via a web page
    - not emailing sensitive information *insecurely*
  - Personal security
    - not giving away information to untrustworthy web sites
    - keeping your password safe
    - not emailing sensitive information

Q3: Have you ever received an email or instant message asking for your password?

## Let's see an example...

- Open a web browser and connect to:

http://zeus.cs.pacificu.edu/chadd/cs120f06/quizform.html

- Fill in a few answers and click Submit Answers!

Q4: What information does the URL show?
Q5: How is that data transferred?
Q6: What if the form asked for your password or SSN?



## Transferring data on the Internet

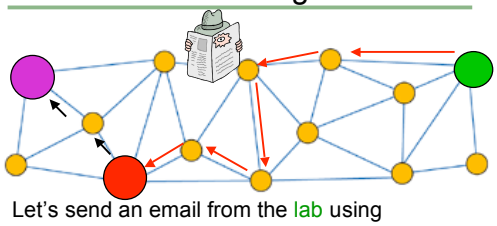
- Unless you specify otherwise, data on the Internet is sent as plain ASCII text
  - web page downloads
  - web page form data
  - emails
  - Instant Messages

Q7: Why do we transfer most of our data in ASCII?

Q8: Why does transferring data in ASCII cause a security problem?



## Where does our data go?



- Let's send an email from the lab using webmail.pacificu.edu to a friend in New York
- Remember, the data will try to avoid congestion
- Q9: How many computers that we don't own will our data pass through?

## Encryption

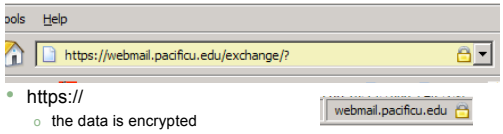
- Scramble the data so it is not plain ASCII text
- Very simple encryption, Caesar cipher:
  - Pacific University becomes
  - Cnpvsvp Havirefvgl

| In | a | b | c | d | e | f | g | h | i |
|---|---|---|---|---|---|---|---|---|---|
| Out | n | o | p | q | r | s | t | u | v |

  - If the spy does not know how the data was encrypted, they cannot get the original data from the encrypted data



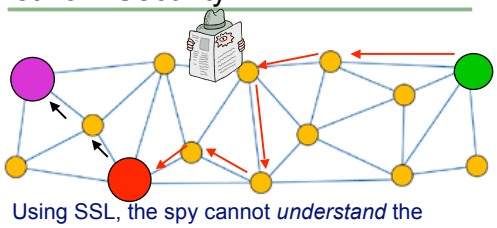
## Encryption in a Web Browser




- https://
  - the data is encrypted
    - Secure Sockets Layer (SSL)
    - much better encryption than the Caesar Cipher
  - reputable online stores use this as well
    - Amazon, BestBuy, Target, Wells Fargo, etc.
  - Before you give away your credit card number or SSN check to make sure the connection is secure!



## Network Security



- Using SSL, the spy cannot *understand* the encrypted data we send the webserver
- Q11: What happens when that email is sent on to your friend in New York? Is it still encrypted?

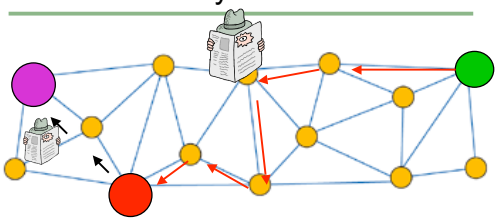
## Email Encryption

- Email is sent as ASCII text
- Use a program to encrypt your email for privacy (page 649 in your book)
  - PGP for example
  - many of these work with your existing email program
  - make sure your friend has the same encryption program and the key to decrypt the message

Q12 How many of your emails contain sensitive information you need to protect?



## Network Security



- Using SSL, the spy cannot read the data we send the webserver because it is encrypted
- If we encrypt the email, the data sent from the email server to New York will also be encrypted



## Privacy

- 12 ways to protect your privacy:
- http://www.eff.org/Privacy/eff_privacy_top_12.html
  - Do not give away personal information
  - Be aware of 'cookies'
    - what is a cookie? (page 98)
  - Realize your computer usage may be monitored at work
  - Do not reply to spam
  - Use up-to-date anti-virus software
    - what is a virus? (section 2.4 & 2.5)
  - Use up-to-date firewall software
    - what is a firewall? (section 2.6)

## Cookies, page 98

- What is a cookie?
  - file created by your web browser to allow a web server to store some information on your computer
  - may contain data to 'personalize your experience'
    - personalize web page layout
    - personalize advertisements!
  - may be used to track customers
  - allow people to see where you have been
  - web browsers can be configured to reject cookies or delete them when you close the browser



## Virus, section 2.4 & 2.5

- Virus: computer program that can replicate itself to move from one computer to another
  - may cause harm to your computer
    - delete files/download undesired data/send spam
- Where do they come from?
  - malicious programmers!
  - be wary of what you download!
  - be wary of what email attachments you open!
- Use Anti-Virus software
  - watches for common viruses and deletes them
  - often sold as a subscription, all the updates for a year!



## Firewall, section 2.6

- When you are on the Internet your computer may act as a server (even if you do not realize it)
  - why is that?
- A firewall is a piece of software that prevents other people from connecting to your computer
  - only allow specific applications to act as a server
  - get notices when someone tries to connect to you

## Personal Security Tips

- Don't give sensitive information to someone unless you know why they need it
  - why does Radio Shack need your home address when you buy batteries?
- Don't give away your password
  - your ISP or credit card company should never ask you for your password via email
  - use a hard to guess password
  - no words or names or dates



## Email

- Don't open *unexpected* email attachments
  - many computer viruses spread this way
  - a Word file could contain a virus
- Don't respond to *unexpected* emails asking for information
  - don't click on a link in an email
    - copy and paste the URL
  - most email programs display HTML

Q13: What will the following hyperlinks display?

```
<a href="http://badplace.com">http://yourbank.com</a>
<a href="http://badplace.com/virus.exe">ExamAnswers.doc</a>
```



## Email Phishing attacks

TrustedBank™

**Q14: Where does that hyperlink go?**

Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

**http://en.wikipedia.org/wiki/Image:PhishingTrustedBank.png**