INFORMATION SECURITY

BASIC SECURITY CONCEPTS

BRIEF HISTORY

- In 1983, Kevin Mitnick did an intrusion on a Pentagon’s computer
- Robert Tappan Morris created the first worm and sent it from MIT to the web and caused $50,000 worth of damages
- In 1994, Vladimir Levin intruded in an American bank computer and stole 10 millions dollars
- Jonathan James “c0mrade”, 16 years old, infiltrated a NASA computer in 1999 and had access to data worth 1,7 millions dollars
- In recent times (CSI Report, 2007):
    - 46% of companies have admitted to suffering financial losses due to security incidences. The reported loss amounted to a total of approximately $66,930,000.
    - 39% of companies have been unable (or unwilling) to estimate the cost of their losses.

ncial Losses, Personal losses, Privacy losses, Data ses, Computer Malfunction and more…..

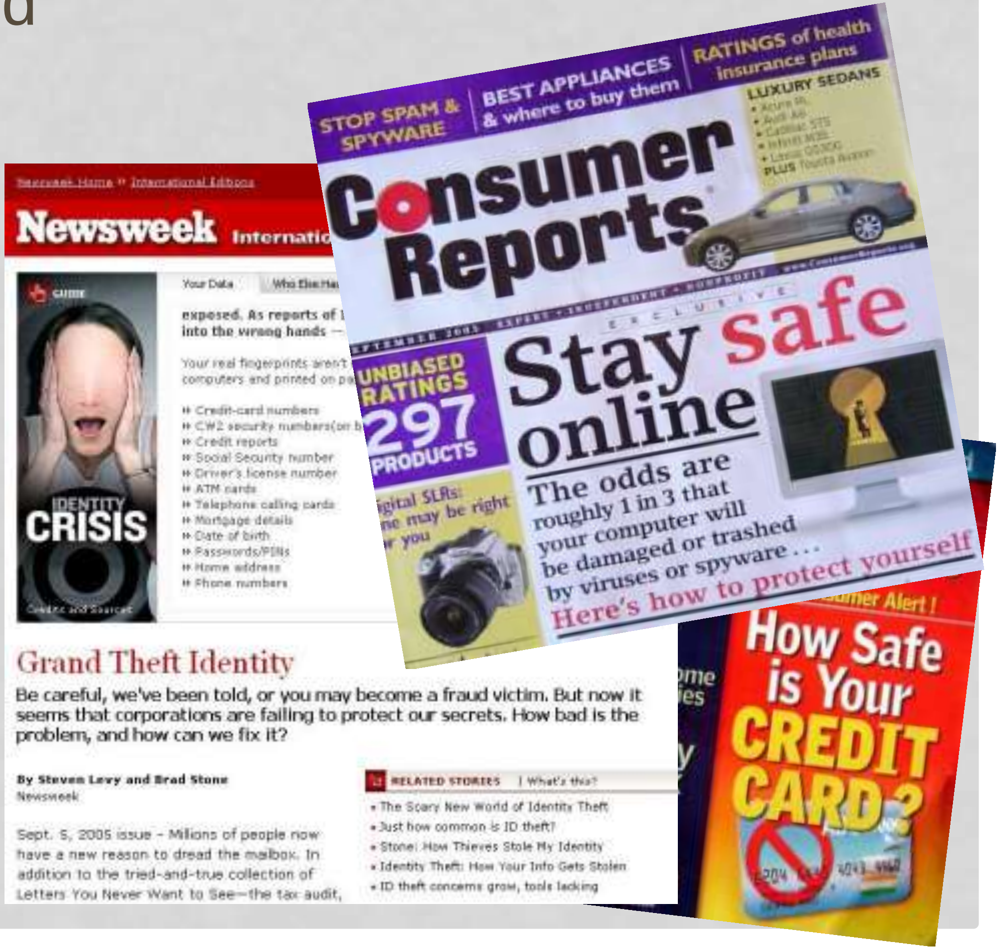
COMPUTER SECURITY

- Computer and Network security was not at all well known, even about 20 years ago
- Today, it is something everyone is aware of the need, but not sure what it really means
- Interesting topic of threats, countermeasures, risks, stories, events and paranoia
  - With some mathematics, algorithms, designs and software issues mixed in
  - Yet, not enough people, even security specialists understand the issues and implications

MEDIA STORIES

- Consumers are bombarded with media reports narrating dangers of the online world
  - Identity Theft
  - Embezzlement and fraud
  - Credit card theft
  - Corporate Loss
- Just “fear mongering”?

So we Thought



Newsweek Home » International Editions

Newsweek International

Your Data | Who Else Ha

exposed. As reports of
into the wrong hands —

Your real fingerprints aren't
computers and printed on pa

- Credit-card numbers
- CW2 security numbers(on b
- Credit reports
- Social Security number
- Driver's license number
- ATM cards
- Telephone calling cards
- Mortgage details
- Date of birth
- Passwords/PINs
- Home address
- Phone numbers

Grand Theft Identity

Be careful, we've been told, or you may become a fraud victim. But now it seems that corporations are failing to protect our secrets. How bad is the problem, and how can we fix it?

By Steven Levy and Brad Stone
Newsweek

Sept. 5, 2005 issue - Millions of people now have a new reason to dread the mailbox. In addition to the tried-and-true collection of Letters You Never Want to See—the tax audit,

RELATED STORIES | What's this?

- The Scary New World of Identity Theft
- Just how common is ID theft?
- Stone: How Thieves Stole My Identity
- Identity Theft: How Your Info Gets Stolen
- ID theft concerns grow, tools lacking

GUIDE
IDENTITY CRISIS
Credits and Sources
STOP SPAM & SPYWARE
BEST APPLIANCES & where to buy them
RATINGS of health insurance plans
LUXURY SEDANS
Acura RL
Audi A6
Cadillac STS
Infiniti M35
Lexus GS300
PLUS Toyota Avalon
Consumer Reports
SEPTEMBER 2005
EXPERT • INDEPENDENT • NONPROFIT
www.ConsumerReports.org
UNBIASED RATINGS 297 PRODUCTS
igital SLRs: ne may be right r you
EXCLUSIVE
Stay safe online
The odds are roughly 1 in 3 that your computer will be damaged or trashed by viruses or spyware...
Here's how to protect yourself
umer Alert!
How Safe is Your CREDIT CARD?

SECURITY? WHAT IS THAT?

- Lock the doors and windows and you are secure
  - NOT
- Call the police when you feel insecure
  - Really?
- Computers are powerful, programmable machines
  - Whoever programs them controls them (and not you)
- Networks are ubiquitous
  - Carries genuine as well as malicious traffic
- **End result:** Complete computer security is unattainable, it is a cat and mouse game
  - *Similar to crime vs. law enforcement*

GOALS OF COMPUTER SECURITY

- Integrity:
  - Guarantee that the data is what we expect
- Confidentiality
  - The information must just be accessible to the authorized people
- Reliability
  - Computers should work without having unexpected problems
- Authentication
  - Guarantee that only authorized persons can access to the resources

SECURITY BASICS

- What does it mean to be secure?
  - “Include protection of information from theft or corruption, or the preservation of availability, as defined in the security policy.” - The Wikipedia
- Types of Security
  - Network Security
  - System and software security
  - Physical Security
- Very little in computing is inherently secure, you must protect yourself!
  - Software cannot protect software (maybe hardware can)
  - Networks can be protected better than software

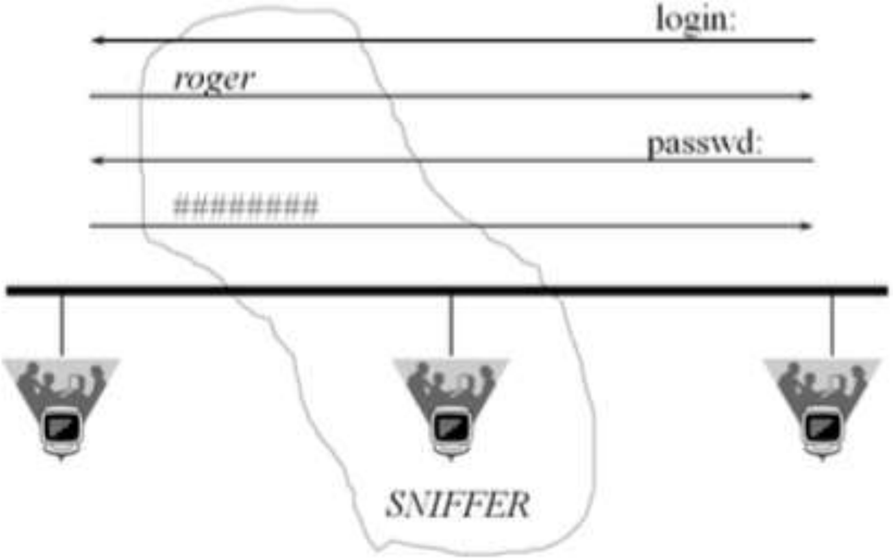
SOME TYPES OF ATTACKS

- What are some common attacks?
  - Network Attacks
    - Packet sniffing, man-in-the-middle, DNS hacking
  - Web attacks
    - Phishing, SQL Injection, Cross Site Scripting
  - OS, applications and software attacks
    - Virus, Trojan, Worms, Rootkits, Buffer Overflow
  - Social Engineering
    - (NOT social networking)
- Not all hackers are evil wrongdoers trying to steal your info
  - Ethical Hackers, Consultants, Penetration testers, Researchers

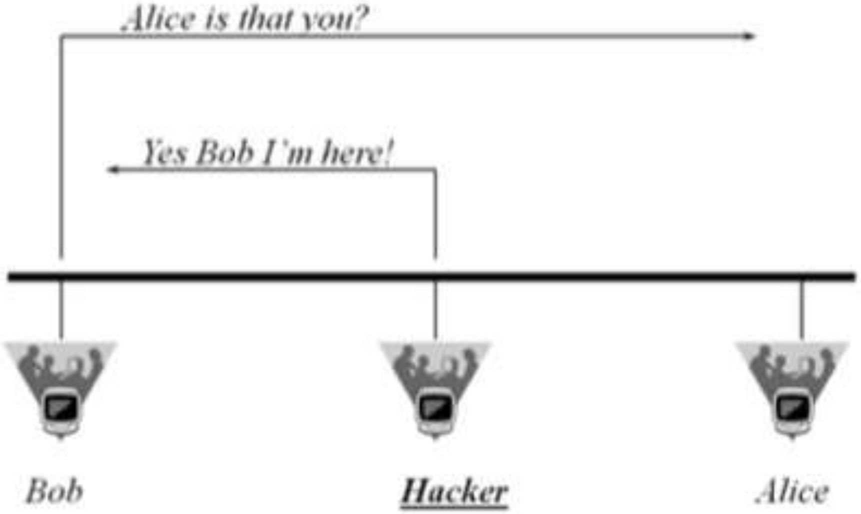
NETWORK ATTACKS

- Packet Sniffing
  - Internet traffic consists of data “packets”, and these can be “sniffed”
  - Leads to other attacks such as password sniffing, cookie stealing session hijacking, information stealing

- Man in the Middle
  - Insert a rogue router in the path between client and server, and change the packets as they pass through
- DNS hijacking
  - Insert malicious routes into DNS tables to send traffic for genuine sites to malicious sites


login:
roger
passwd:
########
SNIFFER

"SNIFF" "SNIFF"


Alice is that you?
Yes Bob I'm here!
Bob
Hacker
Alice

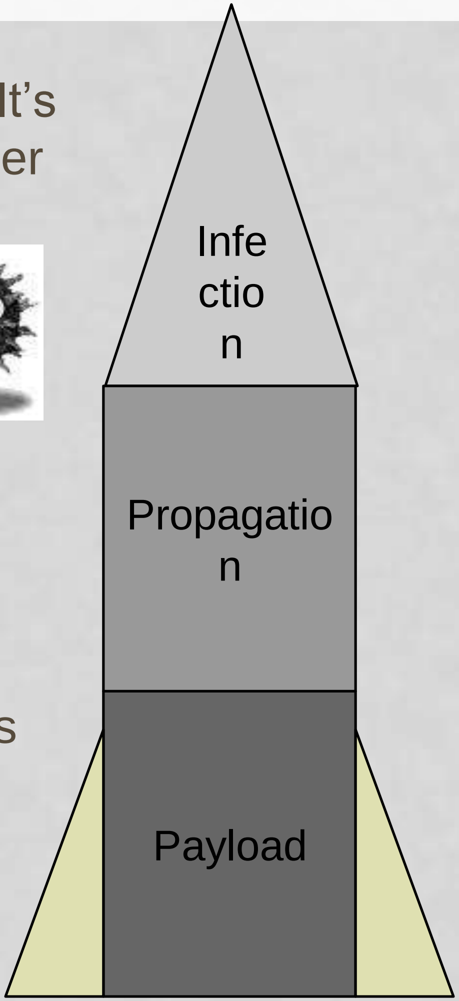
WEB ATTACKS

- Phishing
  - An evil website pretends to be a trusted website
  - Example:
    - You type, by mistake, “mibank.com” instead of “mybank.com”
    - mibank.com designs the site to look like mybank.com so the user types in their info as usual
    - BAD! Now an evil person has your info!
- SQL Injection
  - Interesting Video showing an example
- Cross Site Scripting
  - Writing a complex Javascript program that steals data left by other sites that you have visited in same browsing session

VIRUS

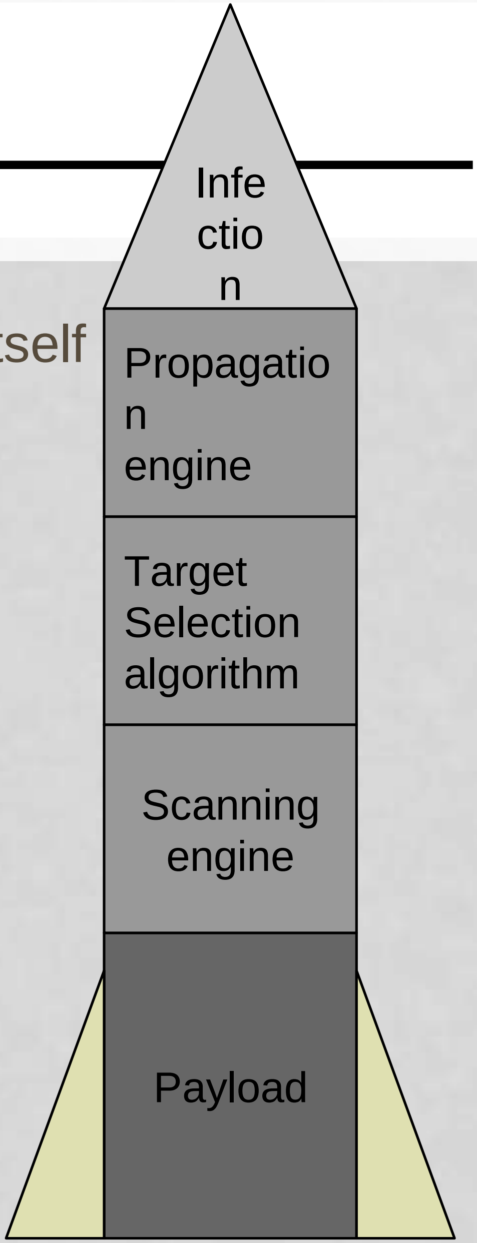
- Definition
  - Piece of code that automatically reproduces itself. It’s attached to other programs or files, but requires user intervention to propagate.
- Infection (targets/carriers)
  - Executable files
  - Boot sectors
  - Documents (macros), scripts (web pages), etc.
- Propagation

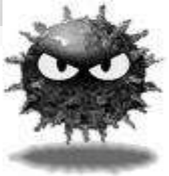
  is made by the user. The mechanisms are storage elements, mails, downloaded files or shared folders



WORM

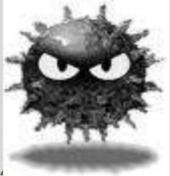
- Definition
  - Piece of code that automatically reproduces itself over the network. It doesn't need user intervention to propagate (autonomous).
- Infection
  - Via buffer overflow, file sharing, configuration errors and other vulnerabilities.
- Target selection algorithm
  - Email addresses, DNS, IP, network neighborhood
- Payload
  - Malicious programs
  - Backdoor, DDoS agent, etc.





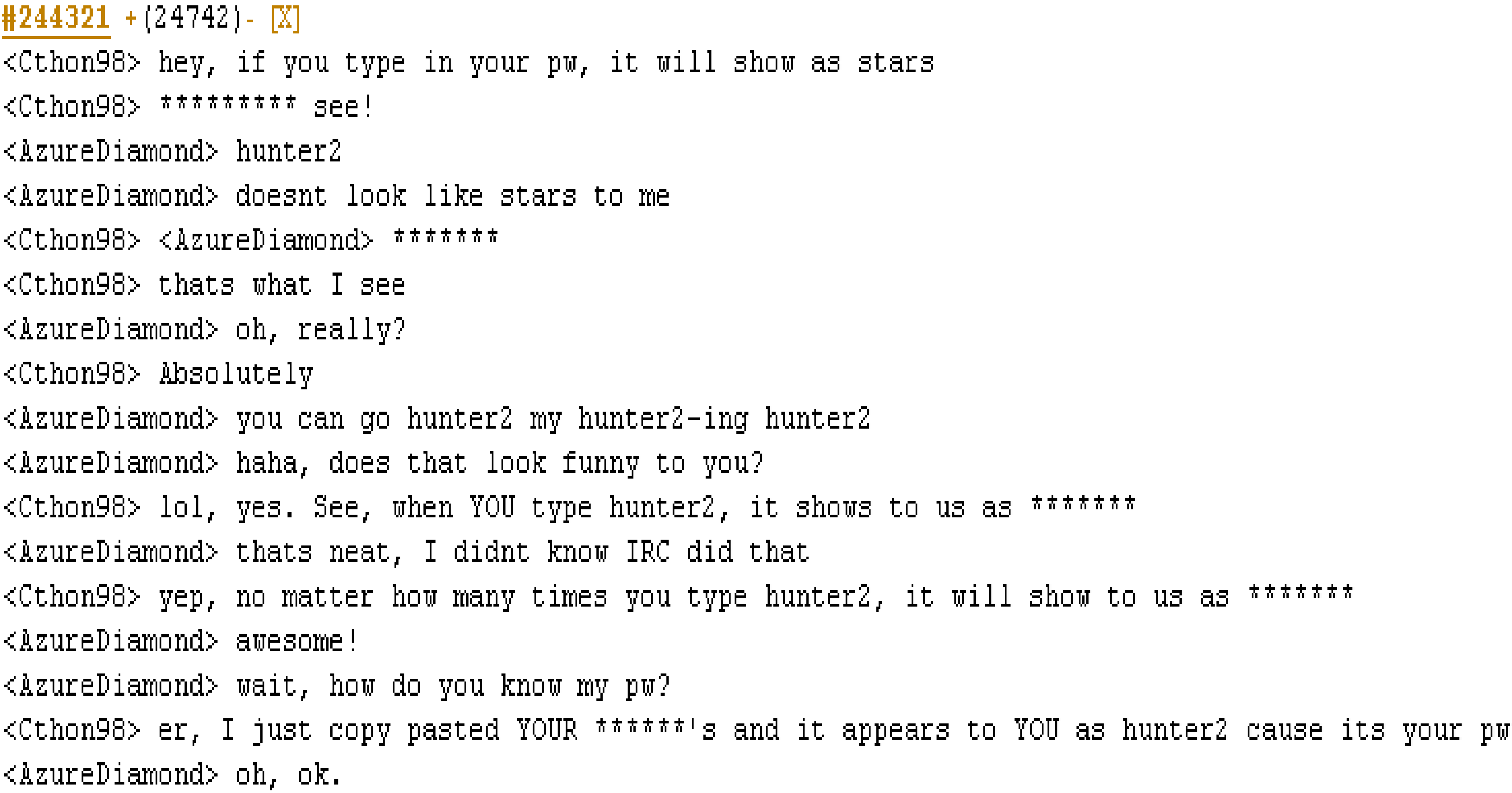
BACKDOOR, TROJAN, ROOTKITS

- Goal
  - The goal of *backdoor*, *Trojan* and *rootkits* is to take possession of a machine subsequently through an infection made via a backdoor.
- Backdoor
  - A *backdoor* is a program placed by a black-hacker that allows him to access a system. A *backdoor* have many functionalities such as keyboard-sniffer display spying, etc.



- Trojan
  - A *Trojan* is a software that seems useful or benign, but is actually hiding a malicious functionality.
- Rootkits (the ultimate virus)
  - *Rootkits* operate like *backdoor* and *Trojan*, but also modify existing programs in the operating system. That allows a black-hacker to control the system without being detected. A *rootkit* can be in user-mode or in kernel-mode.

SOCIAL ENGINEERING



```
#244321 +(24742)- [X]
<Cthon98> hey, if you type in your pw, it will show as stars
<Cthon98> ********* see!
<AzureDiamond> hunter2
<AzureDiamond> doesnt look like stars to me
<Cthon98> <AzureDiamond> *******
<Cthon98> thats what I see
<AzureDiamond> oh, really?
<Cthon98> Absolutely
<AzureDiamond> you can go hunter2 my hunter2-ing hunter2
<AzureDiamond> haha, does that look funny to you?
<Cthon98> lol, yes. See, when YOU type hunter2, it shows to us as *******
<AzureDiamond> thats neat, I didnt know IRC did that
<Cthon98> yep, no matter how many times you type hunter2, it will show to us as *******
<AzureDiamond> awesome!
<AzureDiamond> wait, how do you know my pw?
<Cthon98> er, I just copy pasted YOUR ******'s and it appears to YOU as hunter2 cause its your pw
<AzureDiamond> oh, ok.
```

SOCIAL ENGINEERING

- Why is this social engineering?
  - Manipulating a person or persons into divulging confidential information
- I am not dumb, so does this really apply to me?
  - YES! Attackers are ALSO not dumb.
  - Social Engineers are coming up with much better and much more elaborate schemes to attack users.
  - Even corporate executives can be tricked into revealing VERY secret info
- What can I do to protect myself?
  - NEVER give out your password to ANYBODY.
  - Any system administrator should have the ability to change your password without having to know an old password

PASSWORD ATTACKS

- Password Guessing
  - Ineffective except in targeted cases
- Dictionary Attacks
  - Password are stored in computers as hashes, and these hashes can sometimes get exposed
  - Check all known words with the stored hashes
- Rainbow Tables
  - Trade off storage and computation – uses a large number of pre-computed hashes without having a dictionary
  - Innovative algorithm, that can find passwords fast!
    - e.g. 14 character alphanumeric passwords are found in about 4-10 minutes of computing using a 1GB rainbow table

Need to know:

Data structures, algorithms, cryptography

COMPUTER SECURITY ISSUES

- **Vulnerability** is a point where a system is susceptible to attack.
- A **threat** is a possible danger to the system. The danger might be a person (a system cracker or a spy), a thing (a faulty piece of equipment), or an event (a fire or a flood) that might exploit a vulnerability of the system.
- **Countermeasures** are techniques for protecting your system

VULNERABILITIES IN SYSTEMS

- How do viruses, rootkits enter a system?
  - Even without the user doing something “stupid”
- There are vulnerabilities in most software systems.
  - Buffer Overflow is the most dangerous and common one
- How does it work?
  - All programs run from memory.
  - Some programs allow access to reserved memory locations when given incorrect input.
  - Hackers find out where to place incorrect input and take control.
  - Easy to abuse by hackers, allows a hacker complete access to all resources

Need to know:

Assembly and machine level programming

HOW CAN YOU ACHIEVE SECURITY?

- Many techniques exist for ensuring computer and network security
  - Cryptography
  - Secure networks
  - Antivirus software
  - Firewalls
- In addition, users have to practice “safe computing”
  - Not downloading from unsafe websites
  - Not opening attachments
  - Not trusting what you see on websites
  - Avoiding Scams

CRYPTOGRAPHY

- Simply – secret codes
- Encryption
  - Converting data to unreadable codes to prevent anyone form accessing this information
  - Need a “key” to find the original data – keys take a few million-trillion years to guess
- Public keys
  - An ingenious system of proving you know your password without disclosing your password. Also used for digital signatures
  - Used heavily in SSL connections
- Hashing
  - Creating fingerprints of documents

Need to know:
Mathematics, number theory, cryptographic protocols

WHY CARE?

- Online banking, trading, purchasing may be insecure
  - Credit card and identity theft
- Personal files could be corrupted
  - All school work, music, videos, etc. may be lost
- Computer may become too slow to run
  - If you aren't part of the solution you are part of the problem
- Pwn2Own contest - 2008
  - Mac (Leopard) fell first via Safari, Vista took time but was hacked via Flash Player, Ubuntu stood ground.
- Upon discovery, vulnerabilities can be used against many computers connected to the internet.

рахмат
danke
謝謝
ngiyabonga
spas
teşekkür ederim
Баярлалаа
mersi
kia ora
barka
wefalin
tack
mahalo
tanadh leat
сибо
faafetai lava
vinaka
спасибі
blagodaram
dank je
misaotra
matondo
paldies
grazzi
nanori
kiitos
dankie
dhanyavaad
maururu
thank you
gracias
bayarlalaa
gracie
hvala
köszönöm
dankon
aciu
akun
djiere dieuf
tau
mochchakke
дякую
mam
dziękuję
chnorakaloutioun
grazias
gracies
sulpay
go raibh maith ag
sobodi
dekuji
taiku
gado
mèsi
madloba
sagolun
sukriya
kop khun krap
ありがとう
tanemirt
grazie
arigatô
takk
dakujem
didi madloba
najis tuke
kam sah hamnida
rahmat
terima kasih
rahmet
diolch
dhanyavadagalu
shukriya
merce
мер
তোমাকে ধন্যবাদ
감사합니다
xiexie
ευχαριστώ
merci