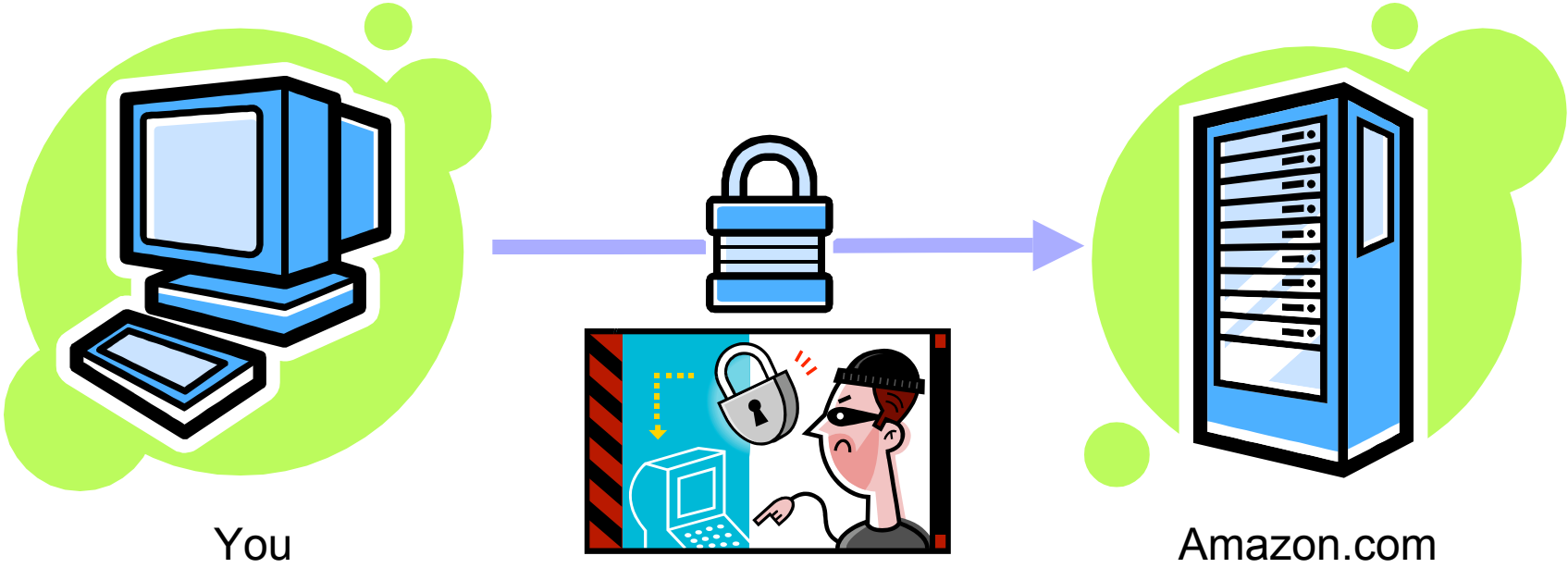
Viruses, Worms, Zombies, and other Beasties

COS 116: 4/19/2007

Adam Finkelstein

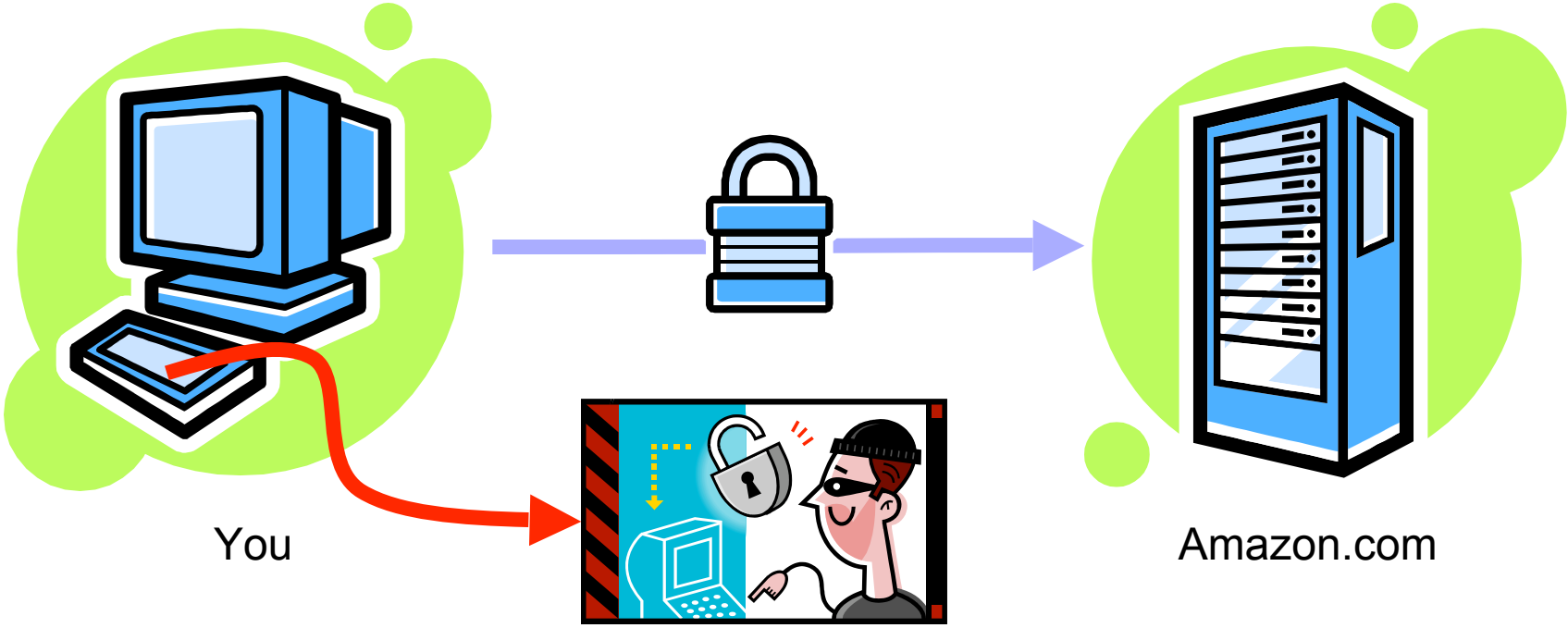
Encrypted vs. Secure



Encryption strongly protects data en route

But attackers will choose weaker targets

Encrypted ≠ Secure



Break into your computer and “sniff” keystrokes as you type

Breaking into a Computer

What does it mean?

How is it done?

Can we prevent it?

What's at Stake?

Kinds of damage caused by insecurity

- Data erased, corrupted, or held hostage
- Valuable information stolen
  (credit card numbers, trade secrets, etc.)
- Services made unavailable
  (email and web site outages, lost business)

Main themes of today's lecture

Computer security is about much more than viruses and worms

The current state of Internet security is like the Wild West: weak or nonexistent policing means citizens have to protect themselves

There is no magic bullet against cyber crime, but following good security practices can help you stay safe

Breaking into a Computer

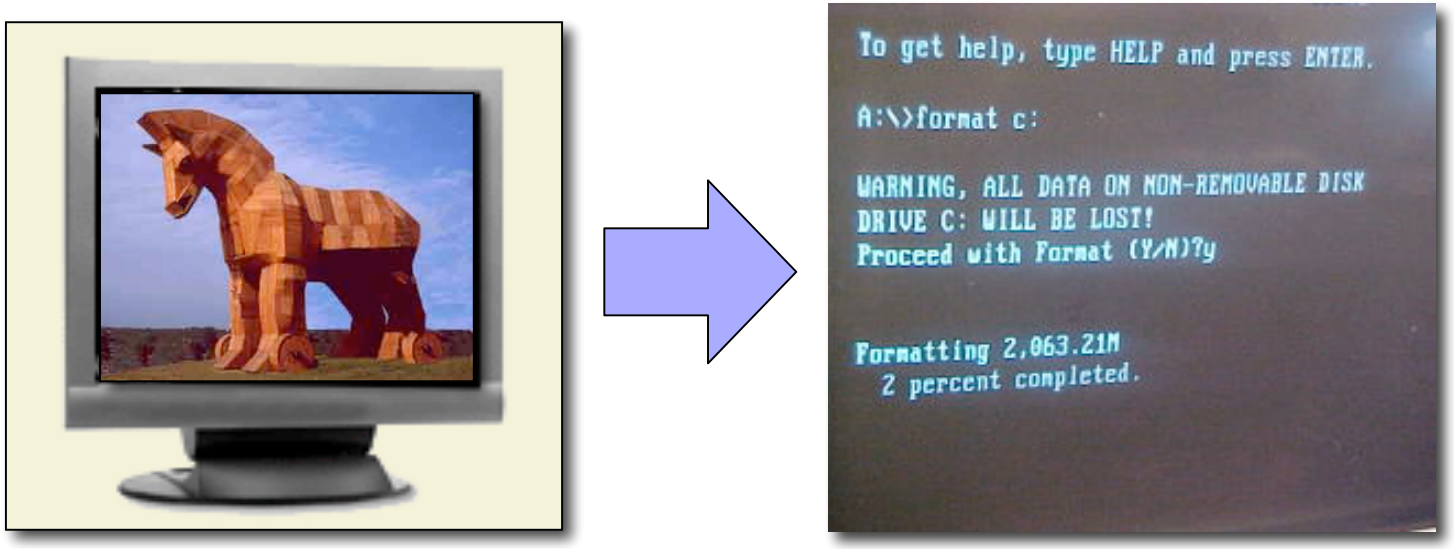
What?

- Run unauthorized software

How?

- Trick the user into running bad software
- Exploit software bugs to run bad software without the user's help

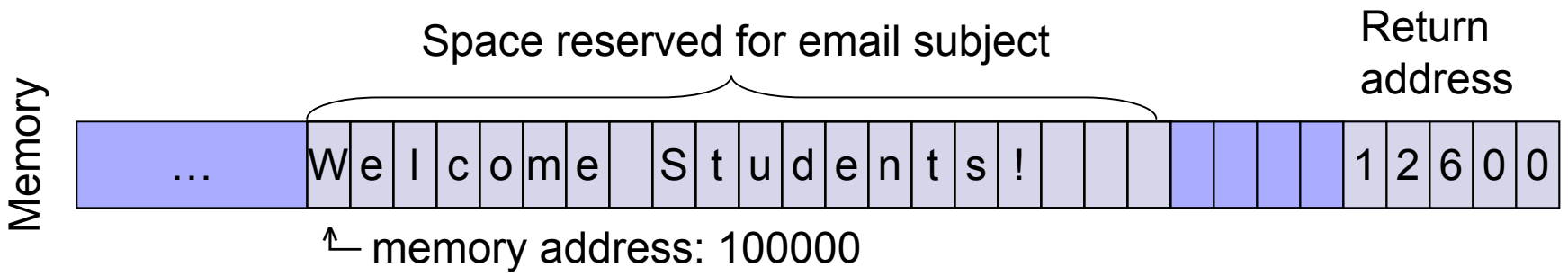
Trojan Horse



CoolScreenSaver.exe

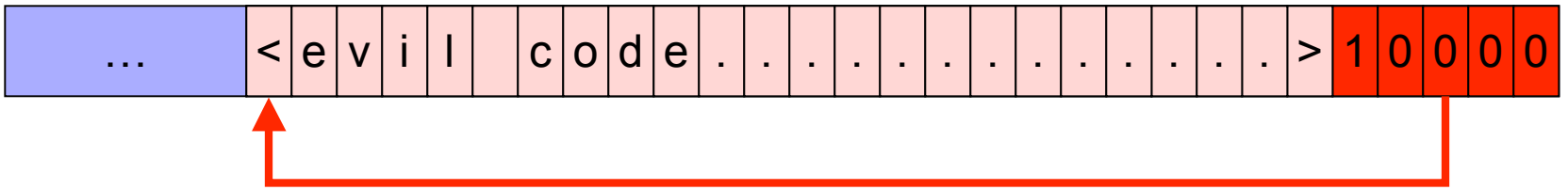
Buffer Overflow Attacks

From: COS 116 Staff
Subject: Welcome Students!



Buffer overflow bug: Forget to check whether input is too big to fit in memory

From: Bad Guy
Subject: <evil code . . . . . >100000



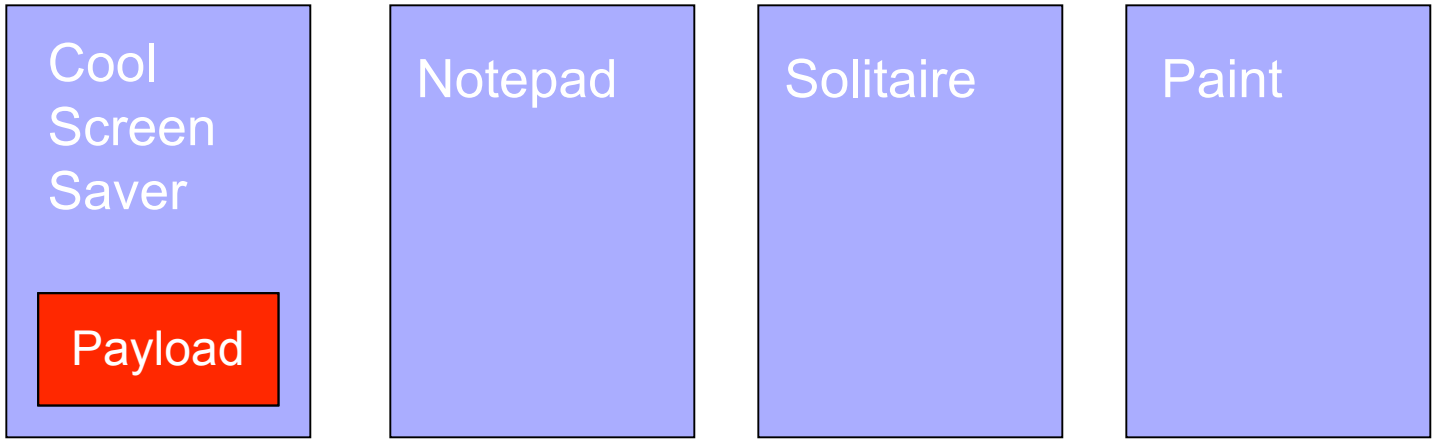
Viruses and Worms

Automated ways of breaking in;

- Use self-replicating programs

Computer Viruses

Self-replicating programs that spread by infecting other programs or data files



Must fool users into opening the infected file

Email Viruses

- Infected program, screen saver, or Word document launches virus when opened
- Use **social engineering** to entice you to open the virus attachment
- **Self-spreading:** after you open it, automatically emails copies to everyone in your address book

The Melissa Virus (1999)

- Social engineering: Email says attachment contains porn site passwords
- Self-spreading: Random 50 people from address book
- Traffic forced shutdown of many email servers
- $80 million damage
- 20 months and $5000 fine

David L. Smith

Combating Viruses

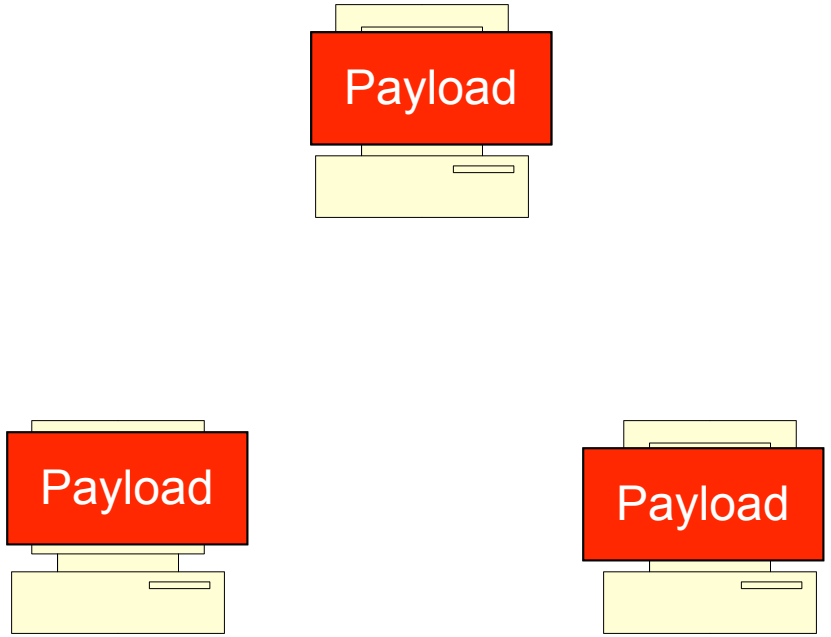
Constant battle between attackers and defenders

Example:

- Anti-virus software looks for “signatures” of known
- Attacker response: *Polymorphic viruses* – change their code when they reproduce to make detection harder
- Anti-virus software adapts to find some kinds of polymorphism
- But an infinite number of ways to permute viruses are available to attackers

Computer Worms

Self-replicating programs like viruses, except exploit security holes to spread on their own without human intervention



The Morris Worm (1988)

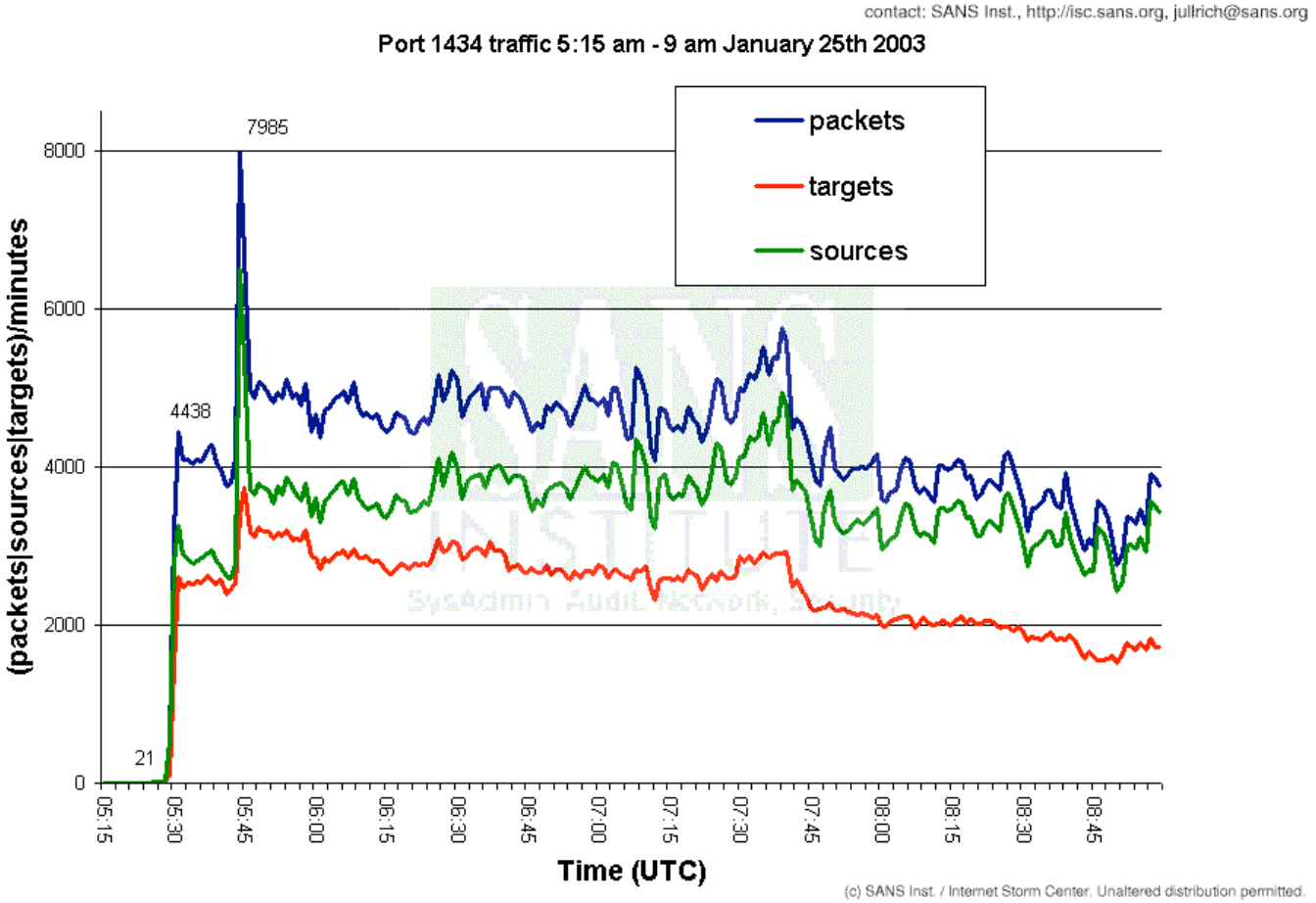
- First Internet worm
- Created by student at Cornell
- Exploited holes in email servers, other programs
- Infected ~10% of the net
- Spawned multiple copies, crippling infected servers
- Sentenced to 3 years probation, $10,000 fine, 400 hours community service

Robert Tappan Morris

The Slammer Worm (2003)

- Fastest spreading worm to date
- Only 376 bytes—Exploited buffer overflow in Microsoft database server products
- Spread by sending infection packets to random servers as fast as possible, hundreds per second
- Infected 90% of vulnerable systems within 10 minutes**!** 200,000 servers
- No destructive payload, but packet volume shut down large portions of the Internet for hours
- 911 systems, airlines, ATMs — $1 billion damage!
- Patch already available months previously, but not widely installed

Can We Stop Worms?



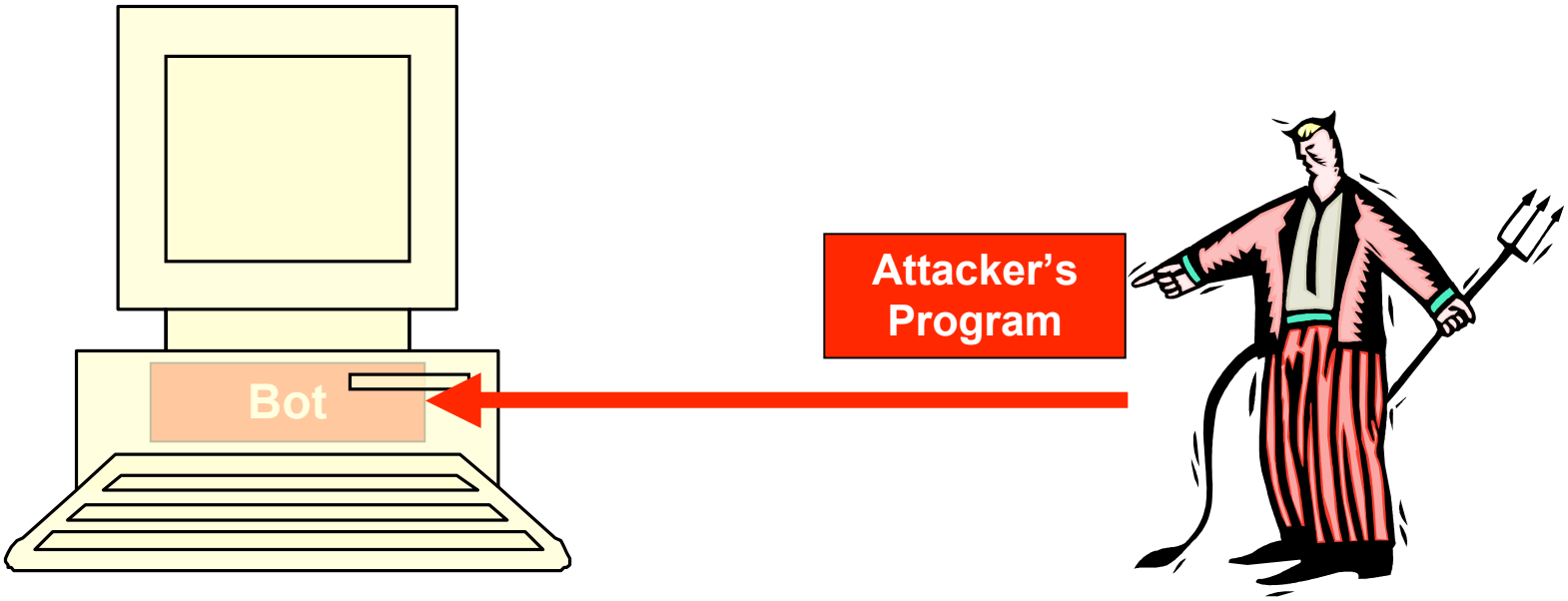
Spread of the Slammer worm

Why do people write worms and viruses?

Botnets

- Virus/worm payload:
  Install *bot* program on target computer
- Bot makes target a *zombie*,
  remotely controlled by attacker
- Many zombies harnessed into armies
  called *botnets* – often 100,000s of PCs

Zombies



Bot program runs silently in the background, awaiting instructions from the attacker

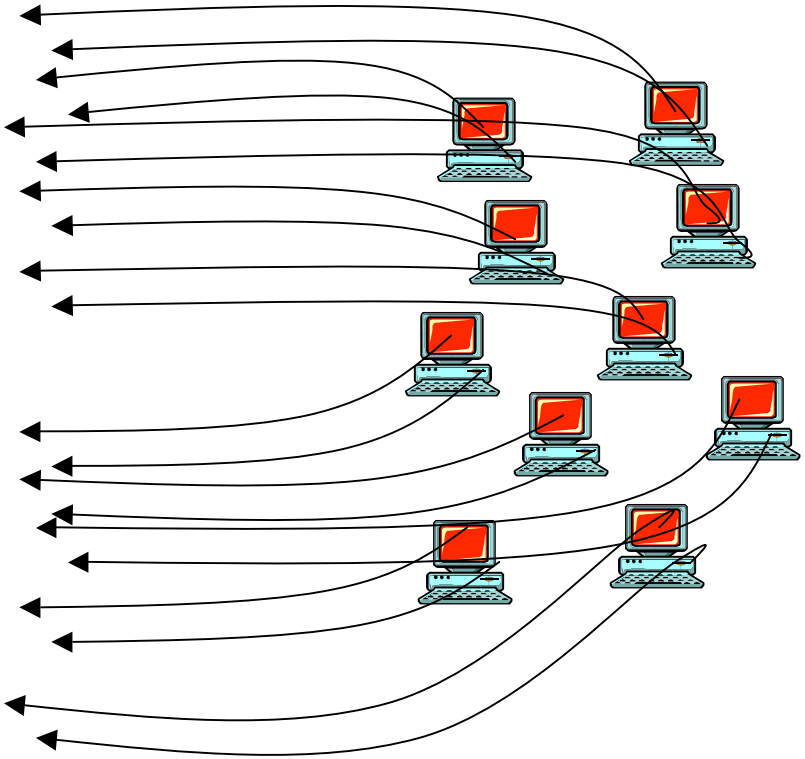
Why go to the trouble of creating a botnet?

Reason 1: DDOS Attacks

"Distributed Denial of Service"

Objective: Overwhelm target site with traffic

Reason 2: Sending Spam



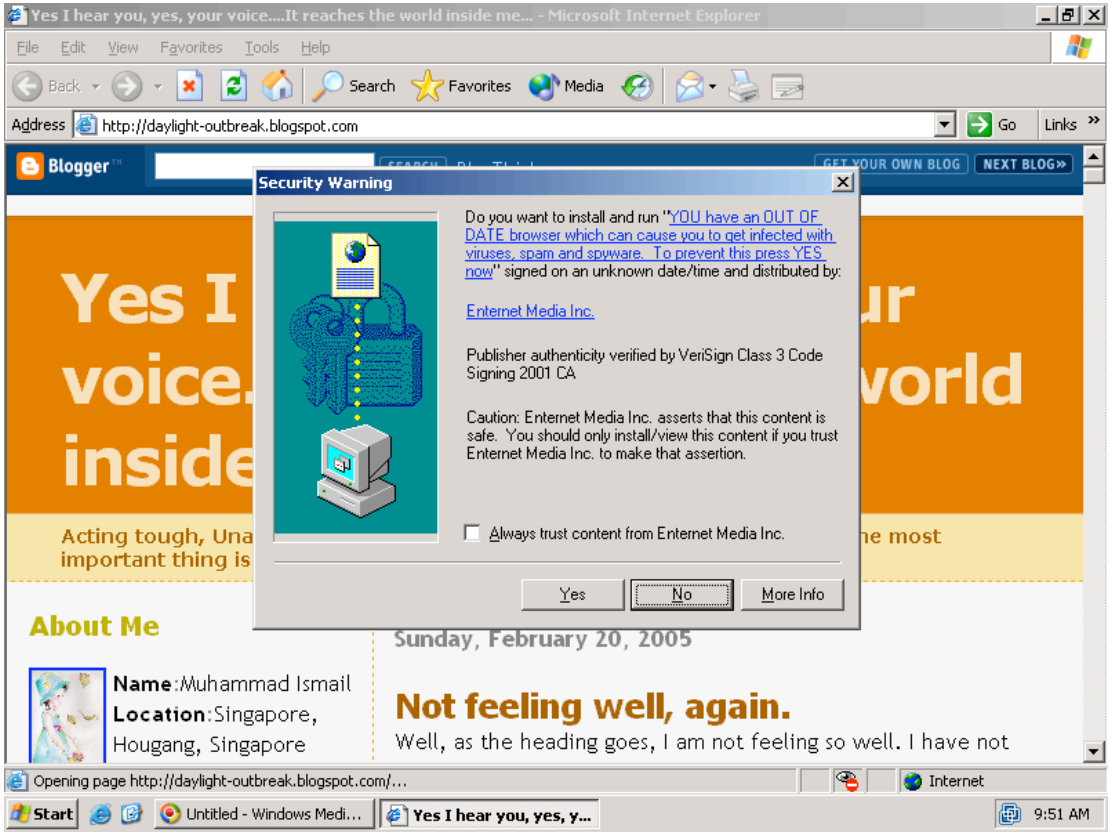
"Forward this message:
Subject: Viagra!
…"

Messages are hard to filter because there are thousands of senders

Other Attacks…

Spyware/Adware

- Hidden but not self-replicating
- Tracks web activity for marketing, shows popup ads, etc.
- Usually written by businesses: Legal gray area



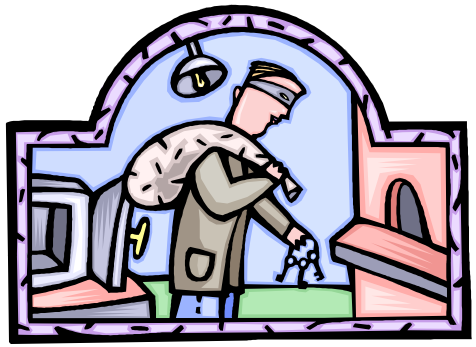
Spoofing Attacks

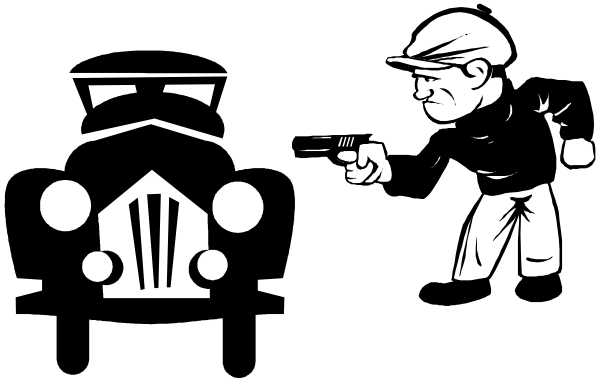
Attacker impersonates the merchant ("spoofing")

Your data is encrypted…

…all the way to the bad guy!

Attackers are Adaptive





Defenders must continually adapt to keep up

Can we stop computer crime?

Probably not!

- Wild West nature of the Internet
- Software will always have bugs
- Rapid exponential spread of attacks

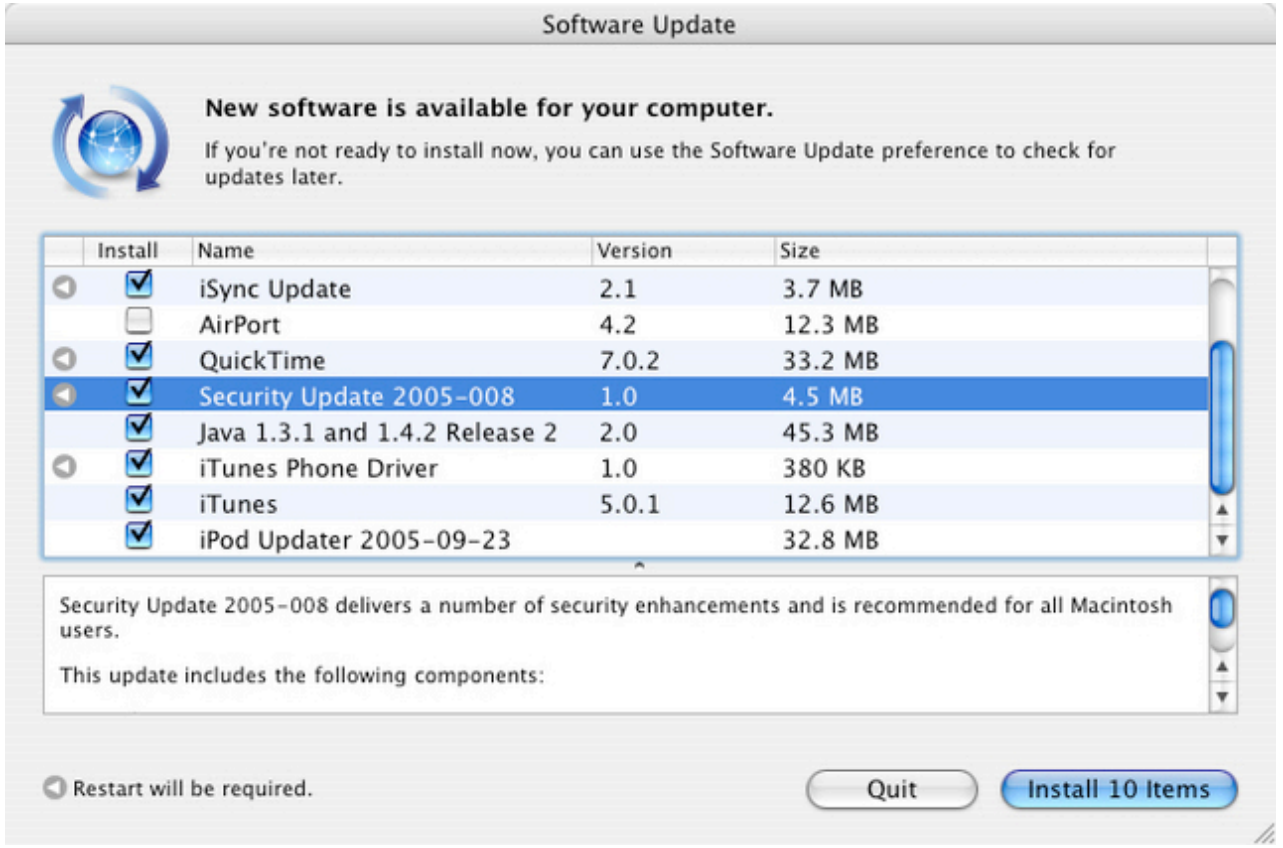
But we can take steps to reduce risks…

Protecting Your Computer

Six easy things you can do…

- Keep your software up-to-date
- Use safe programs to surf the ‘net
- Run anti-virus and anti-spyware regularly
- Add an external firewall
- Back up your data
- Learn to be “street smart” online

Keep Software Up-to-Date

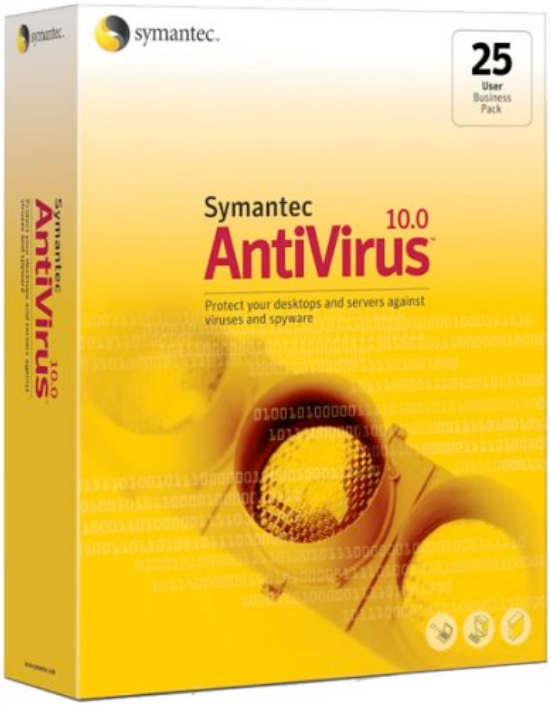


Use Safe Software to Go Online

Firefox
(web browser)

Thunderbird
(email)

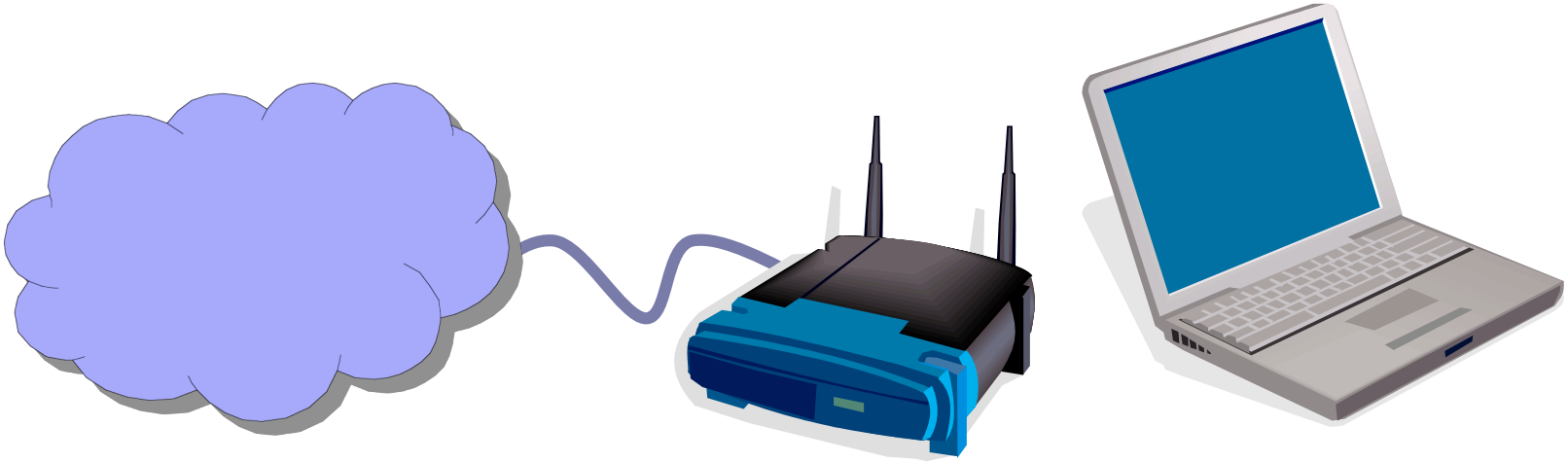
Anti-virus / Anti-spyware Scans



Symantec Antivirus
(Free from OIT)

Spybot Search & Destroy
(Free download)

Add an External Firewall



Provides layered security
(think: castle walls, moat)

Back Up Your Data

Tivoli Storage Manager
(Free from OIT)

Learn Online “Street Smarts”

- Be aware of your surroundings
  - Is the web site being spoofed?
- Don’t accept candy from strangers
  - How do you know an attachment or download isn’t a virus, Trojan, or spyware
- Don’t believe everything you read
  - Email may contain viruses or leads to a phishing attack – remember, bad guys can forge email from your friends