

CSE 120

Principles of Operating Systems

Fall 2001

Lecture 15: Security

Geoffrey M. Voelker

Today

- Some principles of computer security
 - Cribbed from Steve Gribble at UW, who based it on slides from David Wagner at Berkeley
 - Why security is a computer systems issue
- Example UCSD security-related project
 - Backscatter: Detecting DoS attacks
 - David Moore (CAIDA), Voelker and Stefan Savage (CSE)

Security

- Computer Security
 - ♦ Techniques for computing in the presence of adversaries
 - » Three categories of security goals
 - Confidentiality: preventing unauthorized release of info
 - Integrity: preventing unauthorized modification of info
 - Availability: preventing denial of service attacks
 - » Protection is about providing all three on a single machine
 - Usually considered the responsibility of the OS
- Cryptography
 - ♦ Techniques for communicating in the presence of adversaries

November 26, 2001

CSE 120 – Lecture 15 – Security

3

Trusted Computing Base (TCB)

- Think carefully about what you trust with your data
 - ♦ If you type your password on a keyboard, you're trusting
 - » The keyboard manufacturer
 - » Your computer manufacturer
 - » Your OS
 - » The password library
 - » The application that is checking the password
 - ♦ TCB = set of components (hardware, software, people) that you trust your secrets with
- Public Web kiosks should not be in your TCB
 - ♦ Should your OS? (Think about IE and ActiveX)

November 26, 2001

CSE 120 – Lecture 15 – Security

4

Design Principles for Security-Conscious Systems

- Security is much, much more than just crypto
 - ♦ If there is a fundamental flaw in the design of the system, then all of the crypto in the world won't help you
 - ♦ It is usually easier to find a bug in an implementation than circumvent a crypto systems
- Unfortunately, systems design is still as much an art as it is a science
 - ♦ But, decades of building systems the wrong way have helped us cull some learned wisdom
 - ♦ We'll cover some in the rest of this part of the lecture

November 26, 2001

CSE 120 – Lecture 15 – Security

5

Principle of Least Privilege

- Figure out exactly which capabilities a program needs to run, and grant it only those
 - ♦ Not always easy, but one algorithm: start with granting none, run and see where it breaks, add new privileges, repeat
- Unix
 - ♦ Good example: Should not normally run as root to prevent against accidents
 - ♦ Bad example: Some programs run as root just to get a small privilege, such as using a port < 1024 (privileged port)
 - » E.g., ftpd
 - » Exploit these programs, and you get root access to system

November 26, 2001

CSE 120 – Lecture 15 – Security

6

Tractorbeaming wu-ftpd

- wu-ftpd tries to run with least privilege
 - ♦ But occasionally tries to elevate its privilege with:

```
seteuid(0);  
// privileged critical section runs here  
seteuid(getuid());
```
 - ♦ However, wu-ftpd does not disable Unix signals
 - » While in a critical section, can be “tractor-beamed” away to a signal handler
 - Does not return to original control flow
 - » Remote user can cause a signal handler to run by terminating a download in midstream!
 - But need to catch wu-ftpd in the critical section
 - » wu-ftpd doesn’t relinquish privileges after signal handler
 - Result: Can abort a download and then use wu-ftpd as root

November 26, 2001

CSE 120 – Lecture 15 – Security

7

Principle of Least-Common Mechanism

- Basic lesson: Be careful of shared code
 - ♦ Assumptions made may no longer be valid with shared code
- Eudora/Outlook and Internet Explorer
 - ♦ Windows exports an API to IE’s HTML rendering code
 - » Eudora and other programs use this to display HTML in email
 - » By default, JavaScript and Java parsing are enabled
 - ♦ HTML rendering code knows Java(Script) is unsafe
 - » Disables it when JavaScript is downloaded from Internet
 - Internet is untrusted
 - » But enables it when JavaScript is loaded off of disk
 - Your own file system is trusted
 - ♦ But...email is loaded off of disk!
 - » Fertile ground for email viruses...

November 26, 2001

CSE 120 – Lecture 15 – Security

8

Even More Pernicious

- VMS password checking flaw
 - ♦ Password checking algorithm

```
for (I = 0; I < password.length(); I++) {
    if (password[I] != entered_password[I])
        return false;
}
return true;
```
 - ♦ What is the problem here?
 - » Hint: Think about virtual memory...
 - » Another hint: Think about page faults...
 - » Final hint: Who controls where in memory entered_password lives?

November 26, 2001

CSE 120 – Lecture 15 – Security

9

Principle of Complete Mediation

- Check every access to every object
 - ♦ In rare cases, can get away with less (caching)
 - » But only if sure nothing relevant in environment has changed (which is a lot)
- Ex: NFS and file handles
 - ♦ NFS protocol
 - » Client contacts remote “mountd” to get a file handle to a remotely exported NFS file system
 - Remote mountd checks access control at mount time
 - » File handle is a capability: client presents it to read/write file
 - Access control is not checked after mount time
 - » Can use network sniffer to get file handle and access file system

November 26, 2001

CSE 120 – Lecture 15 – Security

10

Fail-Safe Defaults

- Start by denying all access, then allow only that which has been explicitly permitted
 - Oversights will then show up as “false negatives”
 - » Somebody is denied access who should have it
 - Opposites lead to “false positives”
 - » Somebody is given access that shouldn’t get it
 - » Not much incentive to report this kind of failure...
- Examples
 - SunOS shipped with “+” in /etc/hosts.equiv
 - » Essentially lets anyone login as any local user to host
 - Irix shipped with “xhost +”
 - » Any remote client can connect to local X server

November 26, 2001

CSE 120 – Lecture 15 – Security

11

No Security Through Obscurity

- Security through obscurity
 - Attempting to gain security by hiding implementation details
 - Claim: A secure system should be secure even if all implementation details are published
 - » In fact, systems become more secure as people scour over implementation details and find flaws
 - » Rely on mathematics and sound design to provide security
- Ex: GSM cell phones
 - GSM committee designed their own crypto algorithm, but hid it from the world
 - » Social engineering + reverse engineering revealed the algorithm
 - » Turned out to be relatively weak, easy to subvert
- Ex: Netscape SSL

November 26, 2001

CSE 120 – Lecture 15 – Security

12

Outlook For The Future

- Doesn't look bright...
 - ♦ More and more complex systems are being deployed
 - » More and more lives are being trusted to them
- Bruce Schneier: 3 waves of security attacks
 - ♦ 1st wave: physical attacks on wires and hardware
 - » Physical security to defend against this
 - ♦ 2nd wave: syntactic attacks on crypto protocols and systems
 - » E.g., buffer overflows, DDoS attacks
 - ♦ 3rd wave: semantic attacks: humans and computers trust information that they shouldn't
 - » E.g., falsified press announcements
 - Emulex corp stock hoax: CEO "resigns", 61% stock drop
 - Semantic attack against people with preprogrammed sell orders

Denial of Service Attacks

- Example of net security-related research at UCSD
 - ♦ Measuring extent of denial of service attacks (DoS) in Internet
- Paper appeared this August:
 - ♦ David Moore, Geoffrey M. Voelker, and Stefan Savage, *Inferring Internet Denial-of-Service Activity*, 2001 USENIX Security
 - ♦ Won best paper award (wool!)

Goal

- Basically, we were interested in answering a simple question:

How prevalent are denial-of-service attacks in the Internet?

November 26, 2001

CSE 120 – Lecture 15 – Security

15

Anecdotal Data

Press reports:



Analysts: “Losses ... could total more than \$1.2 billion”
- *Yankee Group* report

Surveys: “38% of security professionals surveyed reported denial of service activity in 2000”
- *CSI/FBI* survey

November 26, 2001

CSE 120 – Lecture 15 – Security

16

Quantitative Data?

- Is not available (i.e., no one knows)
- Inherently hard to acquire
 - Few content or service providers collect such data
 - If they do, its usually considered sensitive
- Infeasible to collect at Internet scale
 - How can you monitor enough of the Internet to obtain a representative sample?

November 26, 2001

CSE 120 – Lecture 15 – Security

17

Our Contributions

- Backscatter analysis
 - New technique for estimating global denial-of-service activity
- First data describing Internet-wide DoS activity
 - ~4,000 attacks per week (> 12,000 over 3 weeks)
 - Instantaneous loads above 600k pps
 - Characterization of attacks and victims

November 26, 2001

CSE 120 – Lecture 15 – Security

18

Key Idea

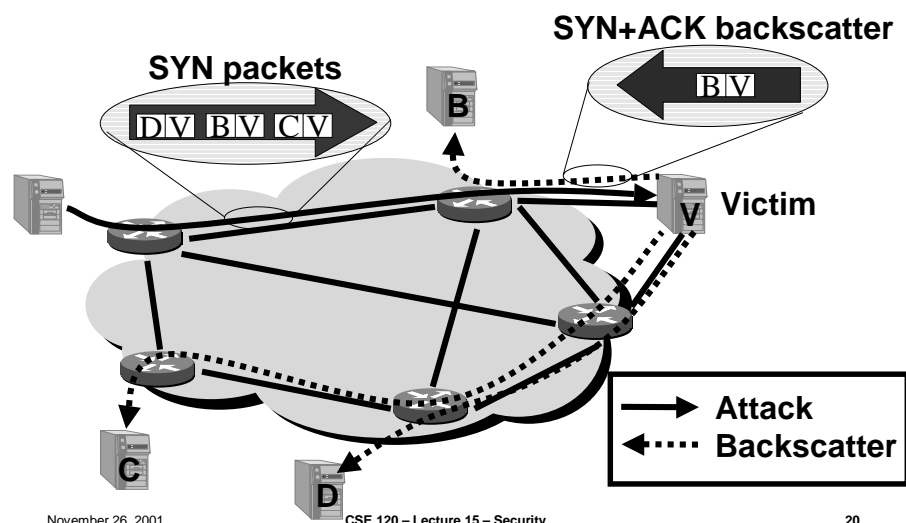
- Flooding-style DoS attacks
 - e.g. SYN flood, ICMP flood
- Attackers spoof source address randomly
 - True of all major attack tools
- Victims, in turn, respond to attack packets
- Unsolicited responses (*backscatter*) equally distributed across IP space
- Received backscatter is evidence of an attacker elsewhere

November 26, 2001

CSE 120 – Lecture 15 – Security

19

Backscatter Example



November 26, 2001

CSE 120 – Lecture 15 – Security

20

Backscatter Analysis

- Monitor block of n IP addresses
- Expected # of backscatter packets given an attack of m packets:

$$E(X) = \frac{nm}{2^{32}}$$

- Extrapolated attack rate R' is a function of measured backscatter rate R :

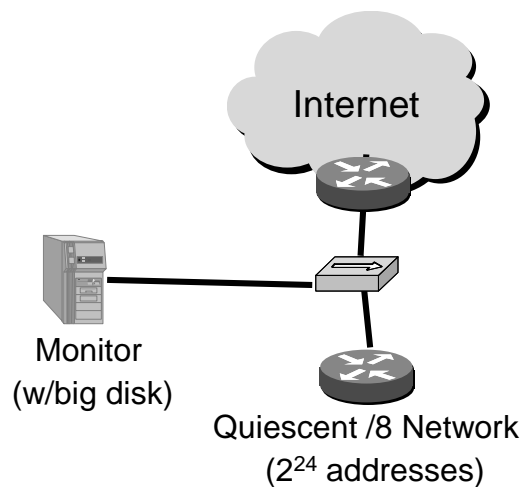
$$R \geq R' \frac{2^{32}}{n}$$

November 26, 2001

CSE 120 – Lecture 15 – Security

21

Experimental Setup



November 26, 2001

CSE 120 – Lecture 15 – Security

22

Methodology

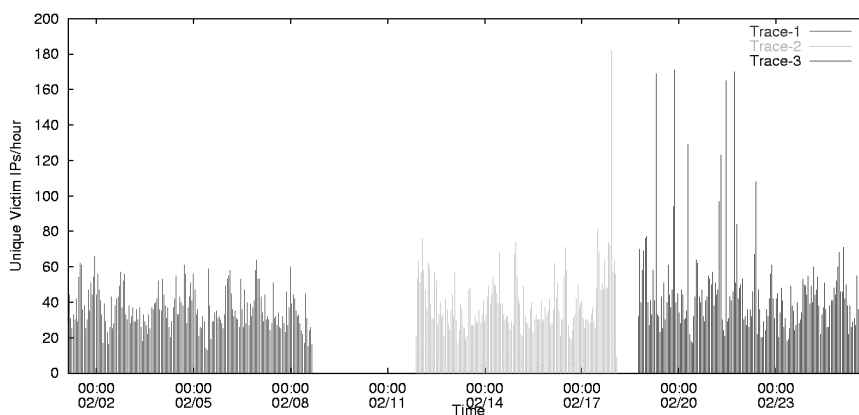
- Collected three weeks of traces (February 2001)
- Analyzed trace data from two perspectives
- Flow-based analysis (categorical)
 - ◆ Number, duration, kinds of attacks
 - ◆ Keyed on victim IP address and protocol
 - ◆ Flow duration defined by explicit parameters (min threshold, timeout)
- Event-based analysis (intensity)
 - ◆ Rate, intensity over time
 - ◆ Attack event: backscatter packets from IP address in 1 minute window

November 26, 2001

CSE 120 – Lecture 15 – Security

23

Attacks Over Time



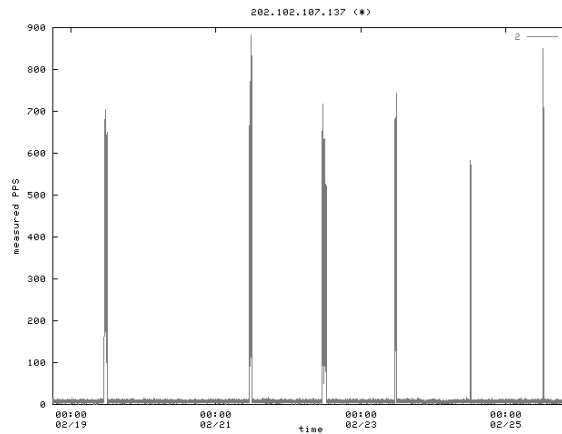
(Surprisingly uniform, no diurnal effects)

November 26, 2001

CSE 120 – Lecture 15 – Security

24

Periodic Attack (Daily)



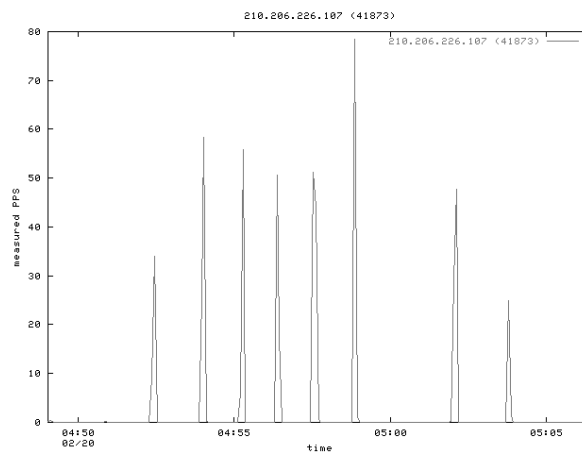
(Every day like clockwork)

November 26, 2001

CSE 120 - Lecture 15 - Security

25

Punctuated Attack (1 min)



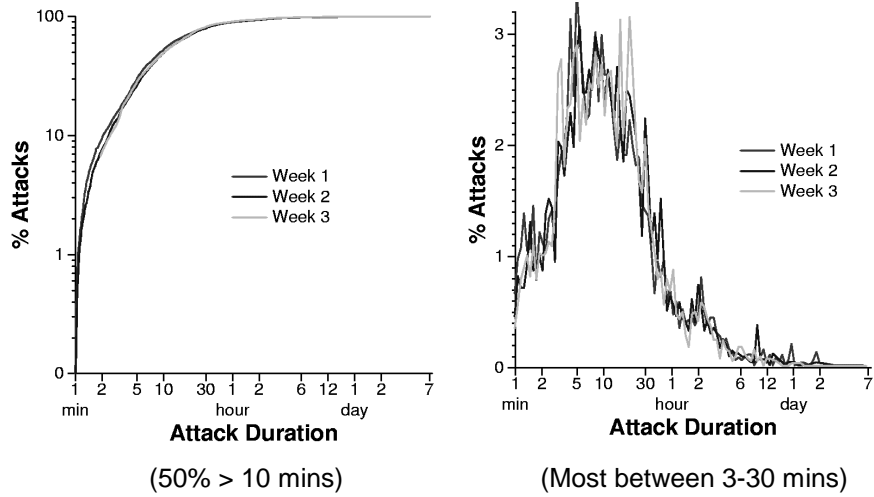
(Fine-grained behavior as well)

November 26, 2001

CSE 120 - Lecture 15 - Security

26

Attack Duration

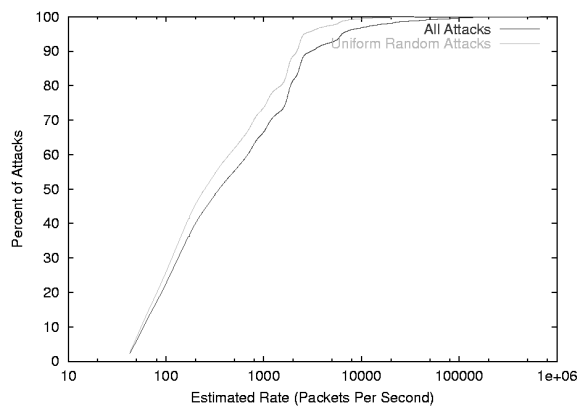


November 26, 2001

CSE 120 - Lecture 15 - Security

27

Attack Rate



November 26, 2001

CSE 120 - Lecture 15 - Security

28

Victim Characterization (DNS)

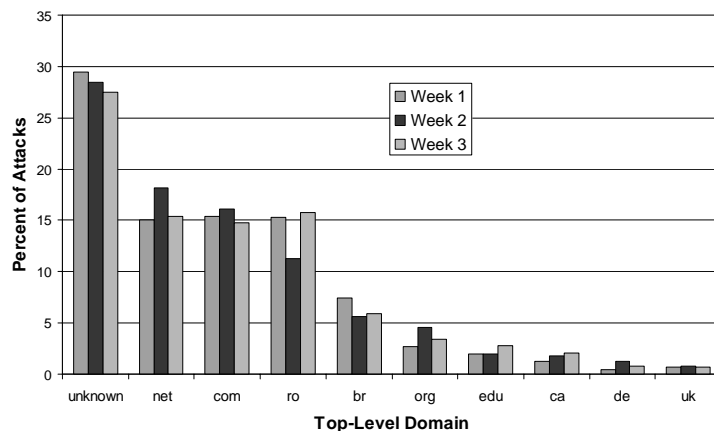
- Entire spectrum of commercial businesses
 - Yahoo, CNN, Amazon, etc. and many smaller biz
- Evidence that minor DoS attacks used for personal vendettas
 - 10-20% of attacks to home machines
 - A few very large attacks against broadband
 - Many reverse mappings clearly compromised (e.g. is.on.the.net.illegal.ly and the.feds.cant.secure.their.shellz.ca)
- 5% of attack target infrastructure
 - Routers (e.g. core2-core1-oc48.paol.above.net)
 - Name servers (e.g. ns4.reliablehosting.com)

November 26, 2001

CSE 120 – Lecture 15 – Security

29

Victim Top-Level Domains



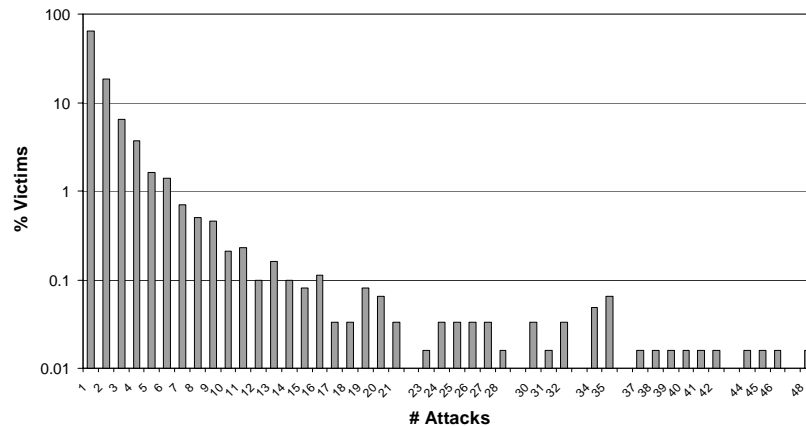
(net == com, edu small, ro and br unusual)

November 26, 2001

CSE 120 – Lecture 15 – Security

30

Victim Popularity



(Most victims attacked once, but a few are unfortunate favorites)

November 26, 2001

CSE 120 – Lecture 15 – Security

31

Summary

- Lots of attacks – some very large
 - ♦ >12,000 attacks against >5,000 targets in a week
 - ♦ Most < 1,000 pps, but some over 600,000 pps
- Everyone is a potential target
 - ♦ Targets not dominated by any TLD, 2LD or AS
 - » Targets include large e-commerce sites, mid-sized business, ISPs, government, universities and end-users
 - ♦ Something weird is happening in Romania
- New attack “styles”
 - ♦ Punctuated/periodic attacks
 - ♦ Attacks against infrastructure targets & broadband

November 26, 2001

CSE 120 – Lecture 15 – Security

32