

ECE 671 – Lecture 19

Network security
Network attacks

Security issues in networks

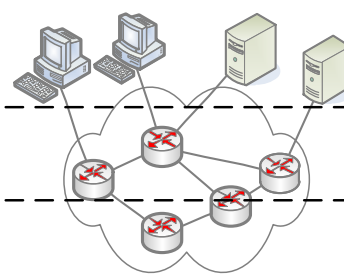
- What is security in context of networks?
- What are potential attacks?
- What can an attacker gain?

Security principles

- Confidentiality
 - Content is hidden
- Authentication
 - Source is verified
- Message integrity and non-repudiation
 - Message is unchanged and undeniable
- Availability and access control
 - Legitimate users should have access
- Today: availability; next lecture: “CIA triad”

Attack types

- Classification of attacks by target:



Attack target	Goal of attack	Attack examples	Defenses
End-system	Data access and modification	Hacking, phishing, espionage, etc.	Virus scanner, firewall, network intrusion detection system, etc.
	Denial-of-service	Denial-of-service attack via botnets, etc.	
Control plane	Data access and modification	Malicious route announcement, DNS cache poisoning, etc.	Secure routing protocols (with cryptographic authentication), secure DNS (DNSSEC), etc.
	Denial-of-service	DNS recursion attack, etc.	
Data plane	Data access and modification	Eavesdropping, man-in-the-middle attack, etc.	Secure network protocols (IPSec, TLS), etc.
	Denial-of-service	Exploit of vulnerable packet processing code	Processing monitor, etc.

End system attacks

- End-system intrusion
 - Exploit software vulnerabilities to gain access
 - Steal data or control system to launch attacks
- Denial of service
 - Overwhelm system with traffic
- Defenses
 - Firewalls
 - Intrusion detection systems

Control plane attacks

- Mapping
 - Analysis of target domain (network topology, contact info)
Tools: ping, traceroute, port scanners
- Hijacking of connections
 - Eavesdrop on connection state
 - DoS attack on one side
 - Spoof towards other side
- DNS attacks
 - DoS attack on root server

Control plane attacks

1 March 2007

Factsheet

Root server attack on 6 February 2007

Executive summary

- The Internet sustained a significant distributed denial of service attack, originating from the Asia-Pacific region, but stood up to it.
- Six of the 13 root servers that form the foundation of the Internet were affected; two badly. The two worst affected were those that do not have new Anycast technology installed.
- The attacks highlighted the effectiveness of Anycast load balancing technology.
- More analysis is needed before a full report on what happened can be drawn up. The reasons behind the attack are unclear.
- Root server operators worked together in a fast, effective

On 6 February 2007, starting at 12:00 PM UTC (4:00 AM PST), for approximately two-and-a-half hours, the system that underpins the Internet came under attack. Three-and-a-half hours after the attack stopped, a second attack, this time lasting five hours, began.

Fortunately, thanks to the determined efforts of engineers across the globe and a new technology developed and implemented after the last DNS attack of this size, on 21 October 2002, the attack had a very limited impact on actual Internet users.

This factsheet provides the most important details of the attack and briefly explains how the domain name system works and the systems in place to protect it. It also outlines how such attacks are possible and discusses possible solutions to future attacks.

What happened?

The core DNS servers of the Internet were hit with a significant distributed denial of service attack, or DDoS. In such an attack, billions of worthless data packets are sent from thousands of different points on the Internet to specific computer servers in order to overwhelm them with requests and so disrupt the smooth running of the Internet.

The Internet works by splitting up information into very small packets, and

ECE 6717

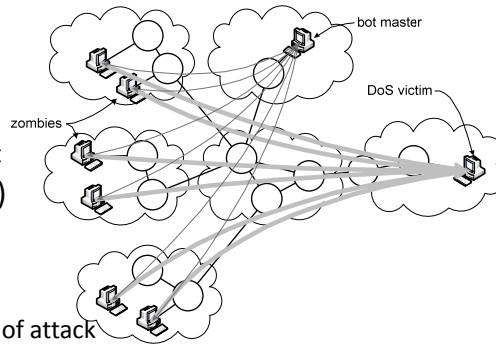
Data plane attacks

- Packet sniffing
 - Ethernet interface in promiscuous mode
- Spoofing
 - Forging of IP source address
 - Actual sender hard to identify
- Denial of Service attacks
 - Use up network or end-system resources

Denial of Service attacks

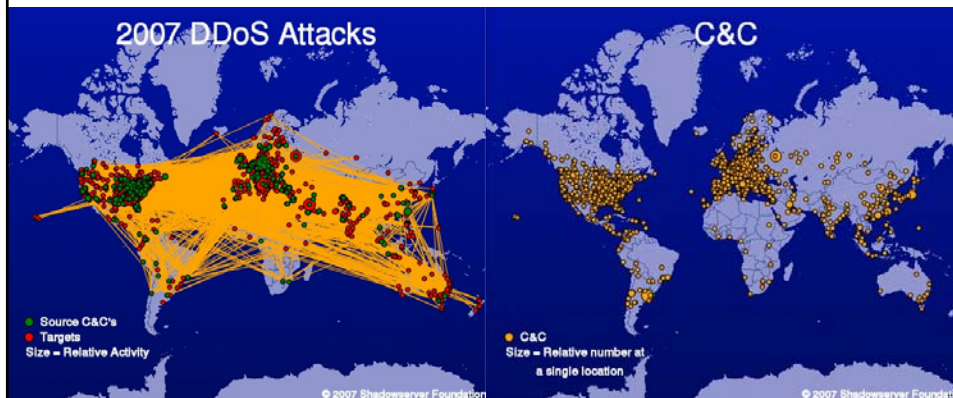
- Denial of service (DoS) attack

- SYN flooding
 - TCP state exhaustion
- Smurf attack
 - ICMP echo request converge on single host
- Distributed DoS (DDoS) attacks
 - Large number of hosts attack single node
 - Much better scalability of attack
 - Often based on botnets



Botnets

- Geographic distribution of botnets



DoS attack for economic gain

PC World: Web of Crime
August 22, 2005

"We were getting a lot of panic attacks from our customers saying they were under attack and they were being held for ransom and could we help them," Quintana says. Prolexic, a company founded in 2003 that protects businesses against DDoS attacks, repels at least one major version every week, according to chief technical officer Barrett Lyon. Of those, slightly less than half involve one business attacking a competitor, as happened to Expert Satellite, he says. Most of the rest are extortion attempts, where a criminal may threaten a DDoS attack unless a company pays protection money (as much as \$250,000). Very few attacks occur without financial motivation, Lyon says.

WANTED BY THE FBI

COMPUTER INTRUSION

SAAD ECHOUAFNI

Aliases: Jay R. Echouafni

DESCRIPTION

Date of Birth	June 23, 1967	Race	Black
Place of Birth	Morocco	Eyes	Green
Height	5'07"	Sex	Male
Weight	200 pounds	Hair	White (Dyed, Adorned)
Wingspan	6'00"	Nationality	Moroccan
SCAC	W3461282		
Occupation	Unknown		
Scars and Marks	Echouafni has a mole on his right cheek.		
Remarks	Echouafni speaks English and French and may have fled to Morocco.		

CAUTION

Saad Echouafni, head of a satellite communications company, is wanted in Los Angeles, California for allegedly hiring computer hackers to launch attacks against his company's competitors. On August 21, 2004, Echouafni was indicted by a federal grand jury in Los Angeles in connection with the first successful investigation of a large-scale distributed denial of service attack (DDoS) used for a commercial purpose in the United States. In a 2004, multi-state distributed denial of service attack, Echouafni hired a group of computer hackers to launch a single target causing a sustained denial of service for its customers. The act of commission was a violation of the Computer Fraud and Abuse Act (CFAA).

As a result of ongoing denial of service attacks that effectively shut business, as well as others both private and government in the United States, Echouafni is being sought by these attacks which resulted in losses ranging from \$200,000 to \$1,000,000.

SEEKING INFORMATION

IF YOU HAVE INFORMATION THAT MAY BE HELPFUL TO THE FBI IN THIS MATTER, PLEASE CONTACT YOUR LOCAL FBI OFFICE.

CONTACT YOUR LOCAL FBI OFFICE AT 1-800-388-TIPS

FOR MORE INFORMATION, VISIT US AT www.fbi.gov

Saad Echouafni, head of a satellite communications company, is wanted in Los Angeles, California for allegedly hiring computer hackers to launch attacks against his company's competitors. On August 21, 2004, Echouafni was indicted by a federal grand jury in Los Angeles in connection with the first successful investigation of a large-scale distributed denial of service attack (DDoS) used for a commercial purpose in the United States. In a

ECE 671

DoS attack as cyber warfare

Digital Protection
Editors: Michael Lesk, lesk@acm.org
Martin R. Styja, mstyja@it.tut.fi
Roland L. Tropic, rtropic@wortson.net

The New Front Line

Estonia under Cyberassault

During the night of 26 April 2007, the Estonian government moved the Bronze Soldier—a memorial statue honoring Soviet World War II war dead—from the central square of its capital city, Tallinn, to a cemetery on the city's outskirts. Russians in Estonia and Russia protested, as did various Russian parliament members, officials from former Soviet Union countries, and the Patriarch of Moscow, the Russian Orthodox Church's spiritual leader. Riots broke out in Tallinn, leaving one dead, several hundred injured, and more than a thousand arrested (<http://news.bbc.co.uk/2/hi/country/660371.stm>). The Russian parliament called for the Estonian government's resignation, and the state-owned Russian Railway announced it would cancel passenger train running between St. Petersburg and Tallinn. Simultaneously distributed-denial-of-service (DDoS) attacks began against Estonian computers.

Have we seen the first national cyberwar?

Estonia, although small (half the size of the US state of Maine, with

subscriber penetration rate of 16.6 percent, compared with 19.7 percent in the US and 14 percent in Italy, according to the Economist Intelligence Unit (http://globaleconomy.com/index.asp?loc=rich_story&ch=4&cat=4&categoryid=20&aid=e-Estonia%3A+Lea+using+by+example&doc_id=10764). According to the Christian Science Monitor, the Estonian Parliament declared Internet access a "fundamental human right" in 2000, and Mart Laar (Estonian Prime Minister from 1992-94 and 1999-2002) declared that Estonia was "the first paperless government." Estonia is so proud of its high technology that it calls itself "E-estonia," and its citizens can vote over the Internet (<http://news.bbc.co.uk/2/hi/technology/3673619.stm>).

The DDoS attacks began on the foreign minister's Web site, but spread to all government institutions.

F Secure, fears that the attack would've been more effective if the Russian government had been involved. Certainly, many informal postings on the Internet asked Russians to participate (www.mememorynews.com/search/1_5941544).

Jose Nazario of Arbor Networks recently posted attack measurements (<http://www.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/>). He found that most of the attacks were Internet Control Message Protocol (ICMP) floods (that is, lots of "ping"). The maximum bandwidth flood was roughly 90 Mbps, with 10 attacks lasting 10 hours or more. Although the media portrayed this in apocalyptic terms—Mark Laster and John Markoff of the *International Herald Tribune* described it as "downloading the entire Windows XP operating system every six seconds for 10 hours"—it isn't actually that much data. Plenty of corporations have that much bandwidth; in Japan, for example, it costs roughly US\$50 per month to obtain 100Mbps. Estonia's problem is that it's a very small country, and its systems aren't configured for that kind of load.

By comparison, in May 2006, the anti-spam company Blue Secu

ECE 671

12

Network attacks

- Internet is based on “on-by-default” principle
 - Any node can send traffic to any other node
- Open approach is good for cooperative environment
 - Difficult to deal with malicious users
- Some network attacks can be solved with crypto
 - Confidentiality, integrity, authentication in protocols
- Availability of resources still an open problem
 - New network architectures aim to address security at core