University of Massachusetts Amherst

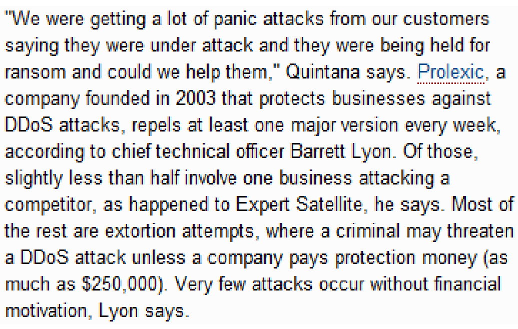
ECE697AA – Lecture 12

Security: Firewalls, IDS

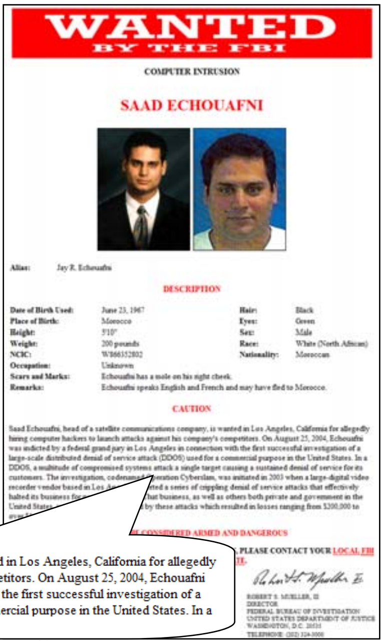
Tilman Wolf
Department of Electrical and Computer Engineering
10/16/08

Cyber crime

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

Alias: Jay R. Echouafni

DESCRIPTION

Date of Birth Used:	June 23, 1967	Hair:	Black
Place of Birth:	Morocco	Eyes:	Green
Height:	5'10"	Sex:	Male
Weight:	200 pounds	Race:	White (North African)
NCIC:	W866152802	Nationality:	Moroccan
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 25, 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 DDOS, a multitude of compromised systems attack a single target causing a sustained denial of service for its customers. The investigation, codenamed Operation Cyberslam, was initiated in 2003 when a large-digital video recorder vendor based in Los An ted a series of crippling denial of service attacks that effectively halted its business fo hat business, as well as others both private and government in the United States d by these attacks which resulted in losses ranging from $200,000 to

E CONSIDERED ARMED AND DANGEROUS

, PLEASE CONTACT YOUR LOCAL FBI
TE.

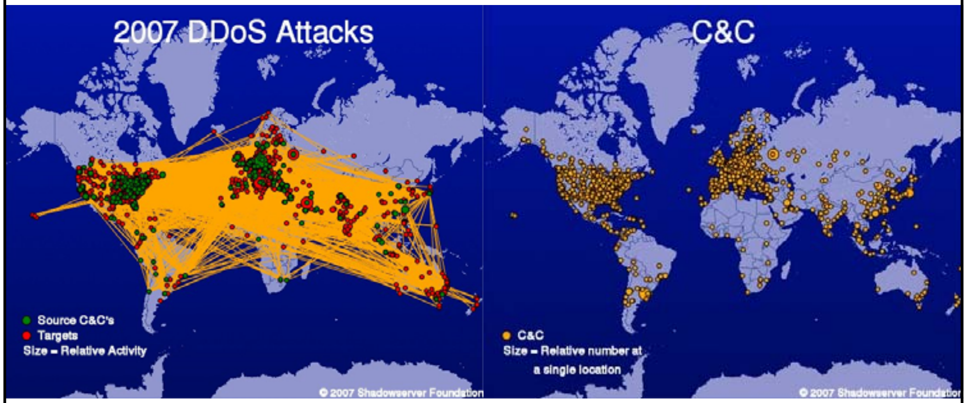
Robert S. Mueller III

ROBERT S. MUELLER, III
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION
UNITED STATES DEPARTMENT OF JUSTICE
WASHINGTON, D.C. 20535
TELEPHONE: (202) 324-3000

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 25, 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

Cyber crime

- Botnets

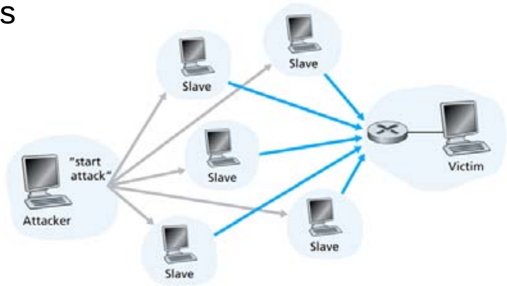

2007 DDoS Attacks
● Source C&C's
● Targets
Size – Relative Activity
© 2007 Shadowserver Foundation
C&C
● C&C
Size – Relative number at a single location
© 2007 Shadowserver Foundation

Internet attacks

- Mapping
  - Analysis of target domain
    - » Network topology
    - » Contact information
  - Tools
    - » Ping, traceroute
    - » Port scanners
- Packet sniffing
  - Ethernet interface in promiscuous mode
- Spoofing
  - Forging of IP source address
  - Actual sender hard to identify
- End-system intrusion
  - Exploit software vulnerabilities to gain access
  - Steal data or control system to launch attacks

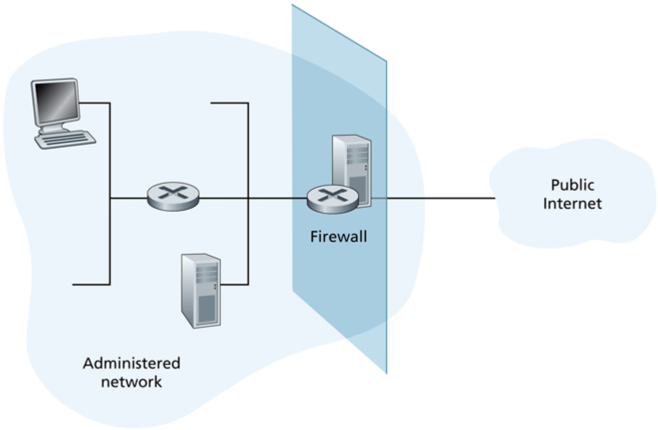
Internet attacks

- 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
- Hijacking of connections
  - Eavesdrop on connection state
  - DoS attack on one side
  - Spoof towards other side



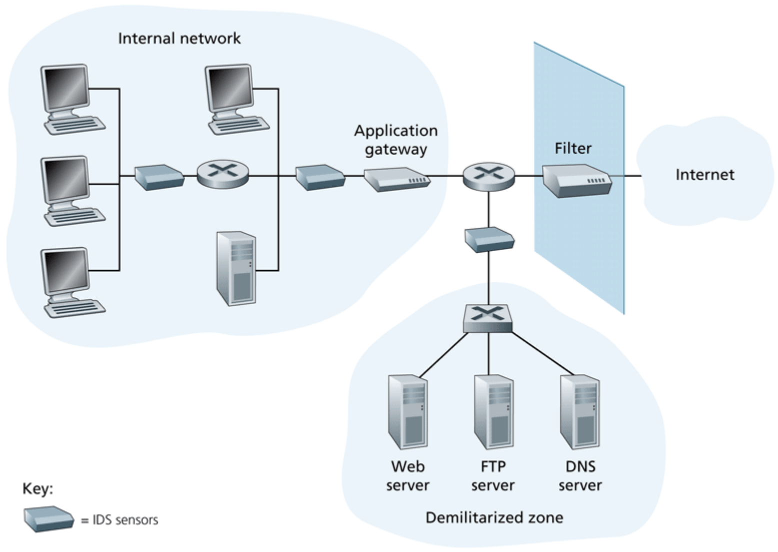
Firewalls

- Forwarding if connection established from inside
  - Firewall keeps connection state
  - Binary decision



Intrusion Detection Systems

- IDS checks packet content



Intrusion Detection Systems

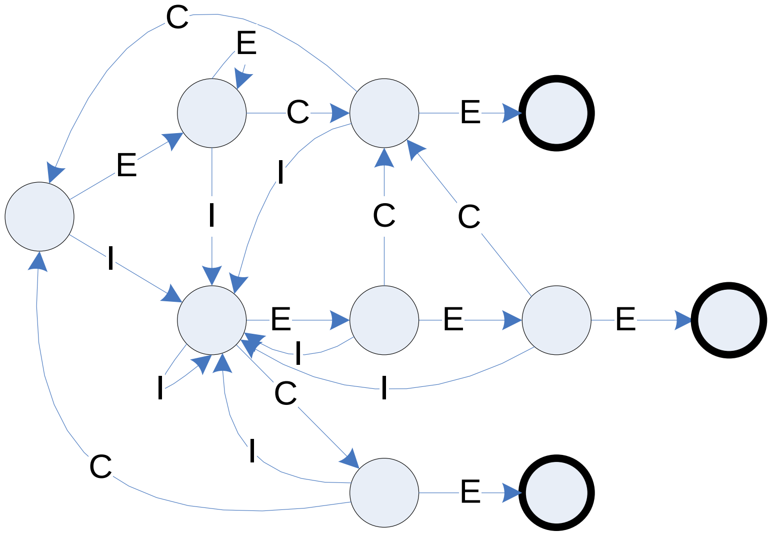
- IDS scan packet to find suspicious patterns
- De-facto standard: snort
  - Tool for scanning
  - Set of rules
- Snort rule example

```
alert tcp any any -> any 80 (content: "cgi-bin/phf"; offset:4; depth:20;)
```

  - IP addresses and port numbers from packet header
  - Content rules requires payload scanning
- Payload scanning
  - Translation of rules (regular expressions) into automata
  - Automata can become large depending on type of rule
- Example
  - Automaton to detect “ECE” or “IEEE” or “ICE”
    - » Alphabet {C,E,I}

Payload scanning

- Complex state machine even for simple expressions



Payload scanning

- Implementation
  - Ideal for specialized hardware
    - » Custom ASIC
    - » FPGA
- Many extensions for special cases
- Probabilistic methods
  - Possible false positives in initial scan
  - Careful scan of packets with potential detections
- Firewalls and IDS are provide first level of defenses
  - How can protocols provide security (in the broadest sense)?

Secure communication

- What are the properties of secure communication?
- 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
- Examples in the Internet?

Assignments

- Read
  - Kurose & Ross: Chapter 8
- SPARK
  - Assessment quiz