Past and Future Internet Disasters: DDoS attacks

survey and analysis

Thomas Dübendorfer <duebendorfer@tik.ee.ethz.ch>
Arno Wagner <wagner@tik.ee.ethz.ch>

April 8th, 2003

A talk in the seminar on “Security Protocols and Applications”

TIK
Computer Engineering and
Networks Laboratory

ETH
Eidgenössische Technische Hochschule Zürich

Agenda

1) **Survey** of DDoS Attacks (TD)

2) **DDoS Case Studies**:
   - Smurf attack (TD)
   - SQL Slammer (TD)

3) **P2P as DDoS Platform** (AW)

4) **Questions & Answers**

TD: Thomas Dübendorfer
AW: Arno Wagner

1) Survey: "The CIA triad"

Classic security guarantees:

C – Confidentiality (90 % of security research papers)

I – Integrity (9 % of security research papers)

A – Availability (1 % of security research papers)

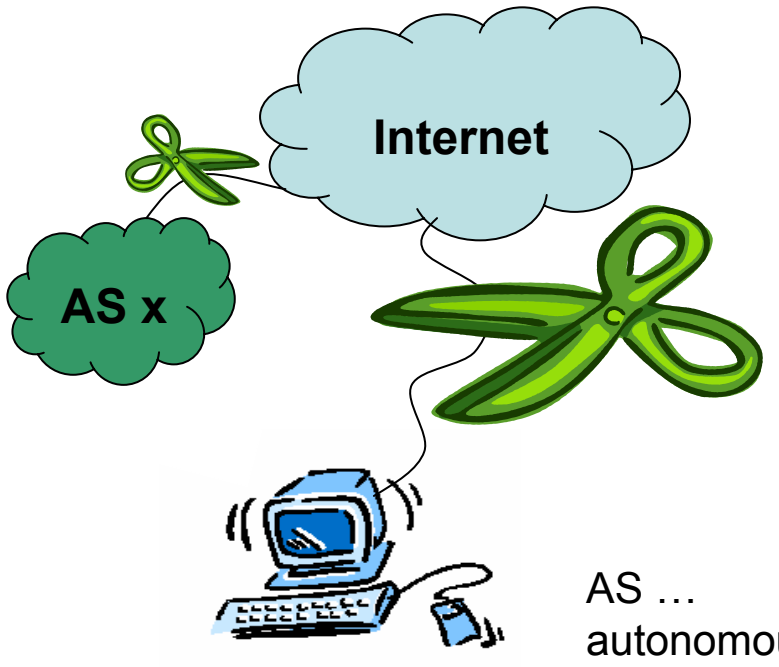
→ (Distributed) Denial of service (**D)DoS attacks** in the Internet **disrupt the *availability*** of a service or resource.

Cf. [1] for the distribution of security papers published in the CIA areas.

1) Survey: Potential damage of DDoS attacks

The Problem:

Massive distributed DoS attacks have the potential to severely decrease backbone availability and can virtually detach a network from the Internet.



AS … autonomous system

1) **Survey:** Motives for DDoS attacks

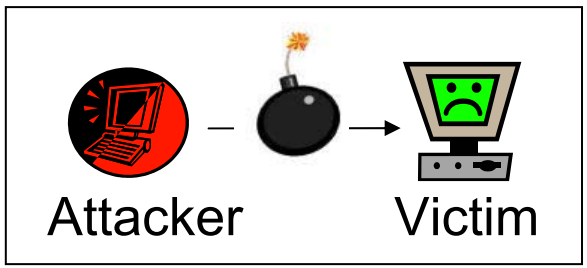
- Cyber warfare: Prevent information exchange
- A means to blackmail a company or even country and cause image and money loss
- Youthful mischief (Übermut) and desire to feel the power „to rule the world“
- Proof of technical excellence to „the world“ and oneself
- Outbreak of worms from Internet security research ;-)
- ??

1) Survey: (D)DoS Attack types I

Denial of service attacks have many "faces" as they are based on manifold techniques and exploits.

A) DoS attacks:

A1) Exploitation of a system weakness



Examples:

- Ping-of-Death: Fragmented ICMP Echo request of > 65,535 bytes
- Teardrop attack: fragmented packets that overlap
- Land attack: TCP SYN with sender IP := victim's IP
- others: WinNuke/Out-of-band

Effect: Host crashes, hangs up (blue screen etc.) or reboots

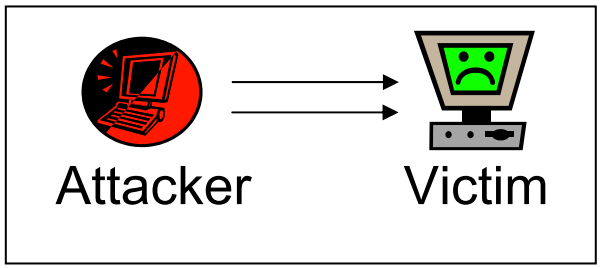
Countermeasures: Install system patches issued by vendor

1) Survey: (D)DoS Attack types II

A) DoS attacks (continued):

A2) Computational system overload

Impose a computationally intensive task on a victim



Examples:

- Trigger many public key de-/encryption
- Trigger many Diffie-Hellman key exchange secret computations
- Trigger many expensive DB queries

Effect: system performance degradation; high response times

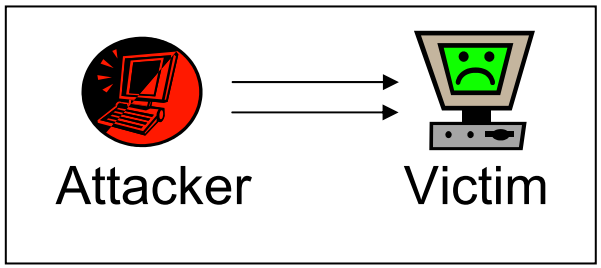
Countermeasures: Protect protocol from being misused;
e.g. cookies in IKE (Internet Key Exchange), Anti-Replay protection in IPSec

1) Survey: (D)DoS Attack types III

A) DoS attacks (continued):

A3) Misusing a protocol

Inject packets and disturb protocol handlers



Examples:

- ICMP unreachable attack (spoof sender)
- TCP RST attack (spoof sender)
- WLAN authentication rejection attack (spoof sender)

Effect: system appears to be unavailable

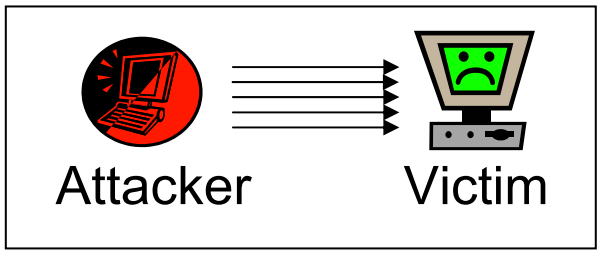
Countermeasures: Protect protocol from being misused; authenticate sender; prevent spoofing

1) Survey: (D)DoS Attack types IV

A) DoS attacks (continued):

A4) Flooding-based attacks

Use up all available bandwidth by fast sending many attack packets



Examples:

- Ping-flooding (congest a link with ICMP echo requests)
- SYN-flooding (create many half-open TCP connections and let connection handles run out)
- Mailbombing/Spamming (exceed mailbox quota)
- Most IP based protocols can be used to congest a link

Effect: high response times; unavailable system/network resources

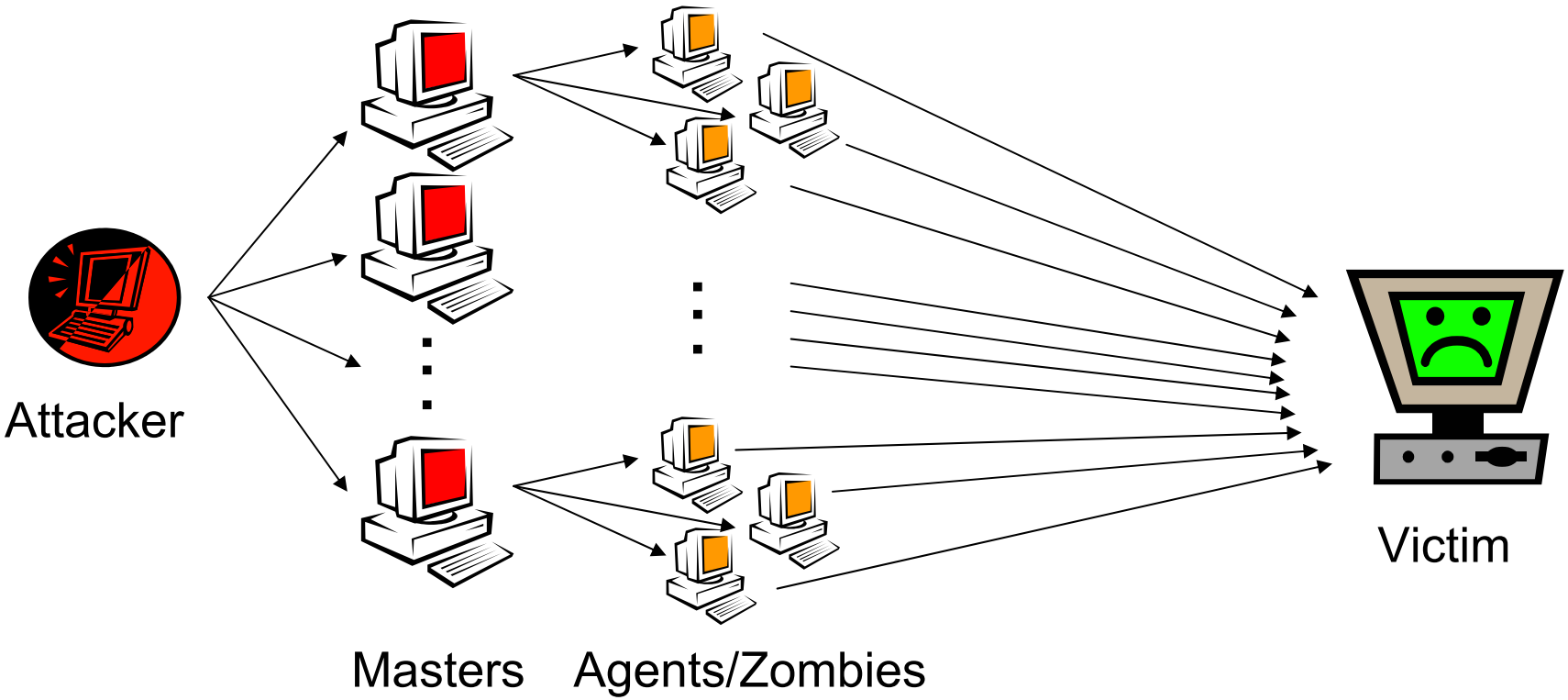
Countermeasures: Rate-limiting or QoS, where possible at all

1) Survey: (D)DoS Attack types V

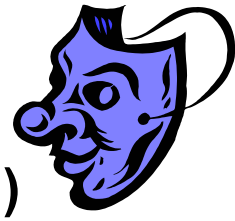
B) DDoS attacks:

In a DDoS attack there is at least an attacker, a victim, and an *amplifying network.*

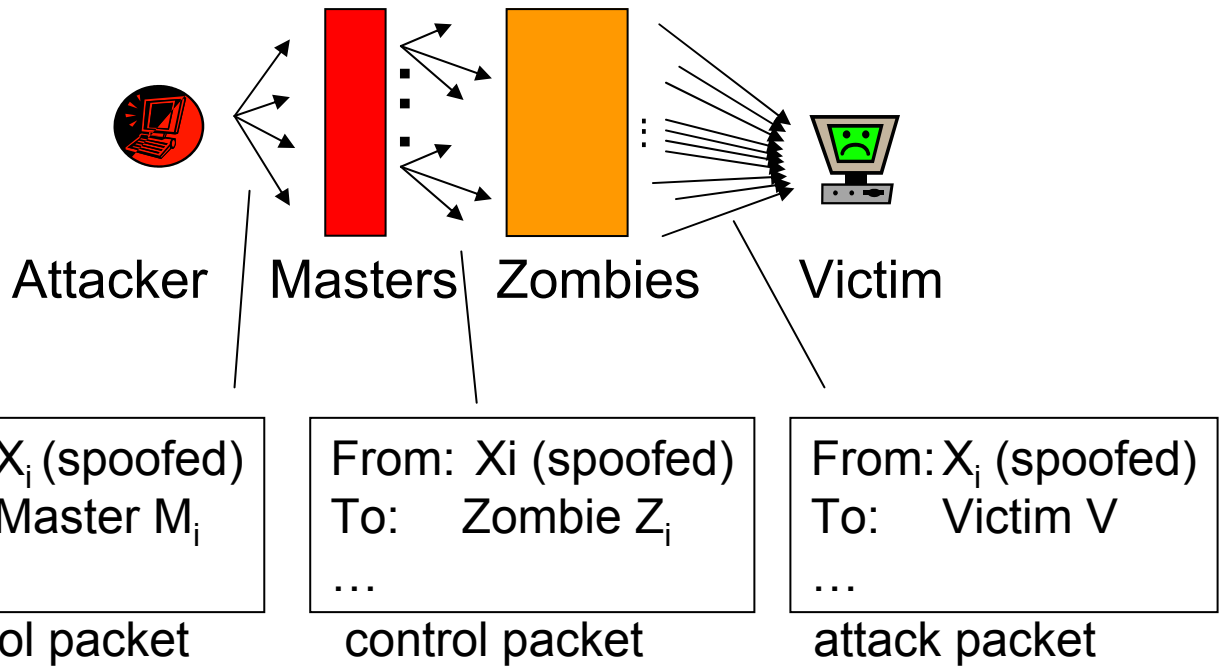
B1) The amplifying network in “direct DDoS attacks”



1) Survey: (D)DoS Attack types VI



B1) The amplifying network in “direct DDoS attacks” (cont.)



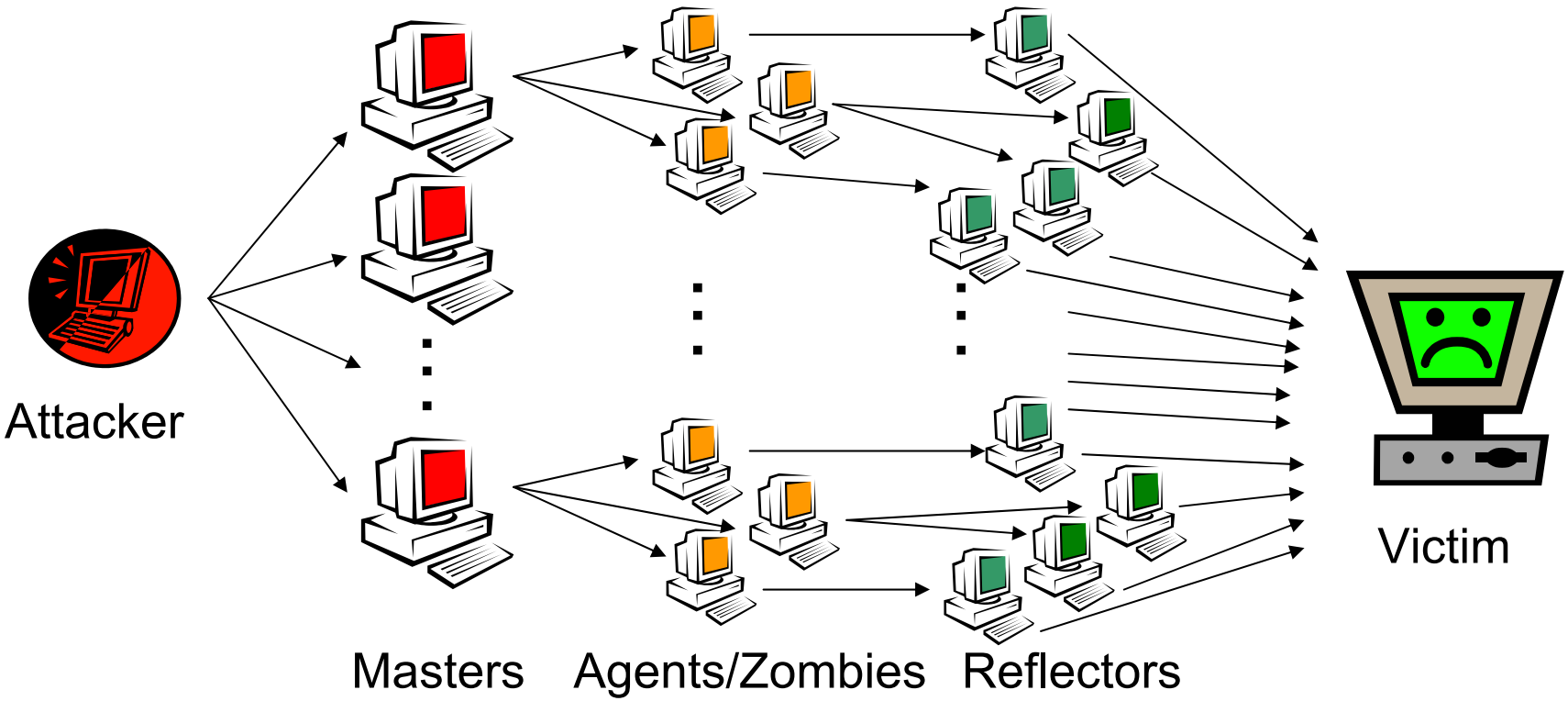
- Masters and Agents/Zombies are *compromised* computers running attacker‘s code
- There are many variants: communication can be bidirectional or based on polling rather than pushing; IP addresses are not always spoofed etc.

1) Survey: (D)DoS Attack types VII

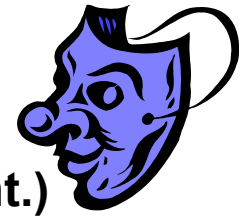
B) DDoS attacks (continued):

In a DDoS attack there is at least an attacker, a victim, and an *amplifying network.*

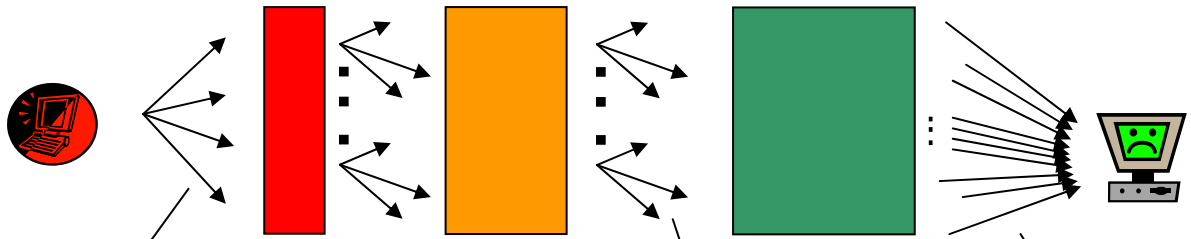
B2) The amplifying network in "reflector DDoS attacks"



1) Survey: (D)DoS Attack types VIII



B2) The amplifying network in "reflector DDoS attacks" " (cont.)



From: X_i (spoofed) To: Master M_i …	From: X_i (spoofed) To: Zombie Z_i …	From: X_i (spoofed) To: Reflector R_i …	From: R_i (**not** spoofed) To: Victim V …
control packet	control packet	attack packet	legitimately looking attack packet

- Masters and Agents/Zombies are *compromised* computers running attacker's code
- Reflectors are ***un****compromised* systems that merely send replies to a request
- There are many variants of communication, number of indirections etc.

1) Survey: (D)DoS Attack types Summary

A) DoS attacks:

A1) Exploitation of a system weakness
A2) Computational system overload
A3) Misusing a protocol
A4) Flooding-based attacks

B) DDoS attacks:

B1) The amplifying network in “direct DDoS attacks”
B2) The amplifying network in “reflector DDoS attacks”

What is exactly “amplified” in an amplifying network?

- **rate** of packets (if each computer in one of s stages sends x packets to n neighbours: x*s^n exponentially many packets are sent to the victim!!)
- **size** of packets (if requests size > reply size)
- **difficulty** to trace back an attack to the initating attacker

2) Case studies: Smurf Attack

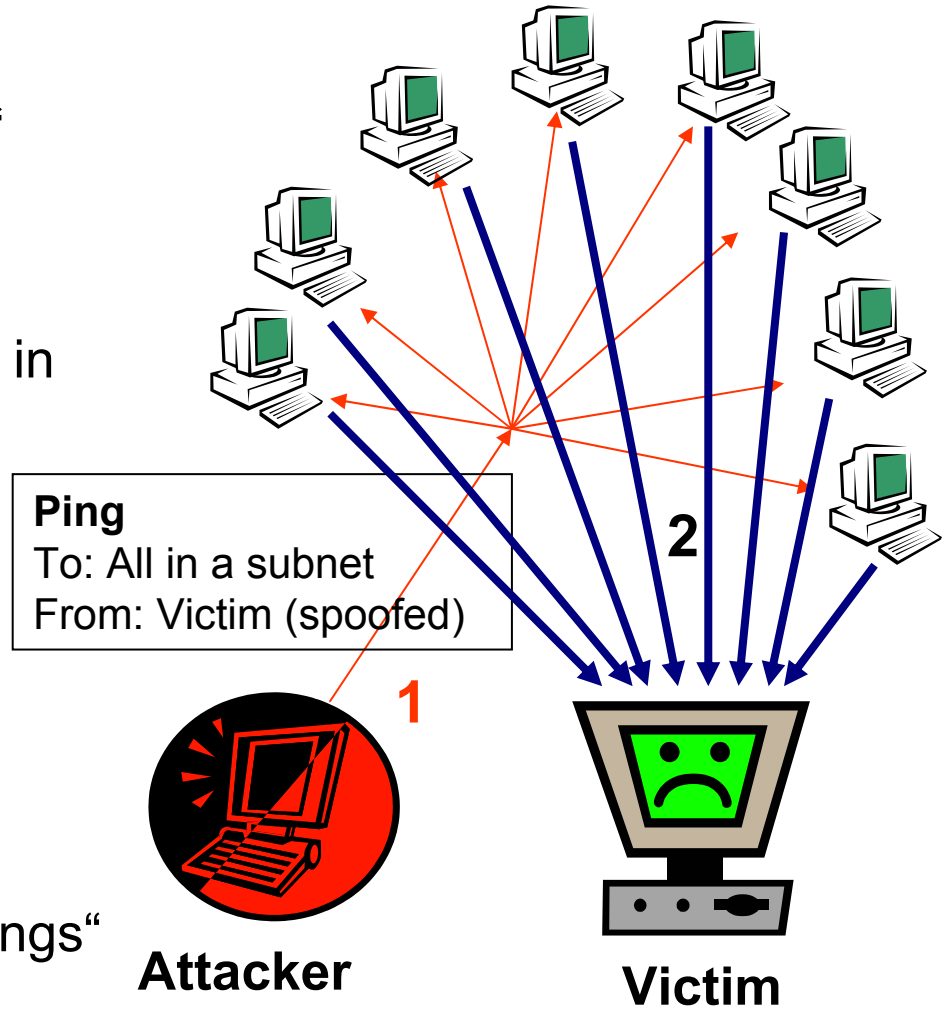
How it works:

The attacker sends many „pings“ (ICMP echo requests) to an IP address that identifies a subnet while spoofing the sender as the victim‘s IP address. All computer in that subnet reply to the victim, which is flooded by replies.

ICMP … Internet Control Message Protocol

Countermeasures:

- Routers: Filter subnets „pings“
- Host: Do not reply to subnet „pings“



2) Case studies: SQL Slammer I

Or: How 376 bytes can shut down the Internet

Damage history (extract):

On January 25, 2003

- **over 260,000 unique IP addresses infected** by the Slammer worm within Internet Security Systems' monitored networks
- Propagation of the worm overpowered Internet connections with millions of UDP/IP probes hours after the activity began.
- **ETH Zurich** was not connected to the Internet for about 3 hours. Service for e-mail and web pages were only partially available.

On February 5, 2003

(W)LAN for visitors and vendors at the **Internet Expo in Zurich** (with 330 vendors present) was not available due to SQL Slammer infections of vendor's computers. Conference room had no Internet access.

RP ONLINE MULTIMEDIA ONLINE

Notrufnummern und Geldautomaten lahm gelegt

Milliardenschäden: Computerangriff in USA schlimmer als erwartet

Slammer/Helkern hat in den USA Milliardenschäden verursacht. Foto: rpo

Washington (rpo). Der von Virenexperten als höchst gefährlich eingestufte Wurm "Slammer" hat bei seinem Angriff am Wochenende in den USA einen weitaus größeren Schaden angerichtet als bislang angenommen.

Noch am Montag waren viele Web-Sites zum Beispiel von Kreditunternehmen außer Betrieb. Der Schaden geht vermutlich in die Milliarden Dollar. Der Angriff sei "vergleichbar mit dem Schlimmsten, was das Internet bisher erlebt hat", sagte der Computerexperte Miles McNamee.

2) Case studies: SQL Slammer II

Or: How 376 bytes can shut down the Internet

How the SQL Slammer DDoS attack works

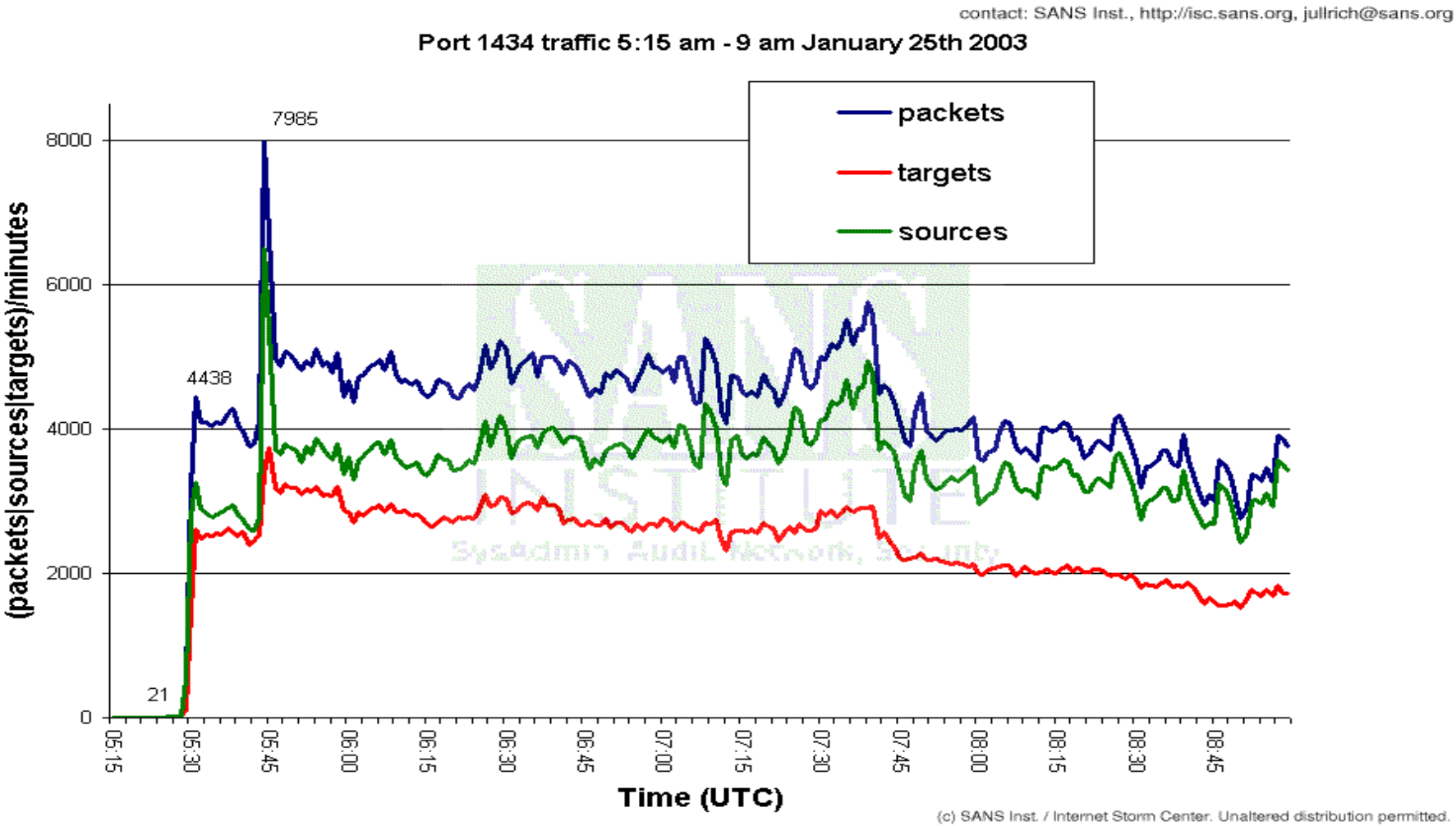
- The **amplifying network** of zombies is built fast by **worm** spreading based on exploiting a system vulnerability
- System vulnerability: Exploit Microsoft SQL Servers and MSDE-enabled products vulnerable to the SQL Server resolution service **buffer overflow.**
- Slammer's main function is **propagation**, sending 376 bytes of code across port 1434/UDP until the SQL Server shuts down
- Scanning/infection/attack code is combined

Countermeasures:

- Patch the vulnerable SQL server installations
- Filter attack traffic to port 1434/UDP

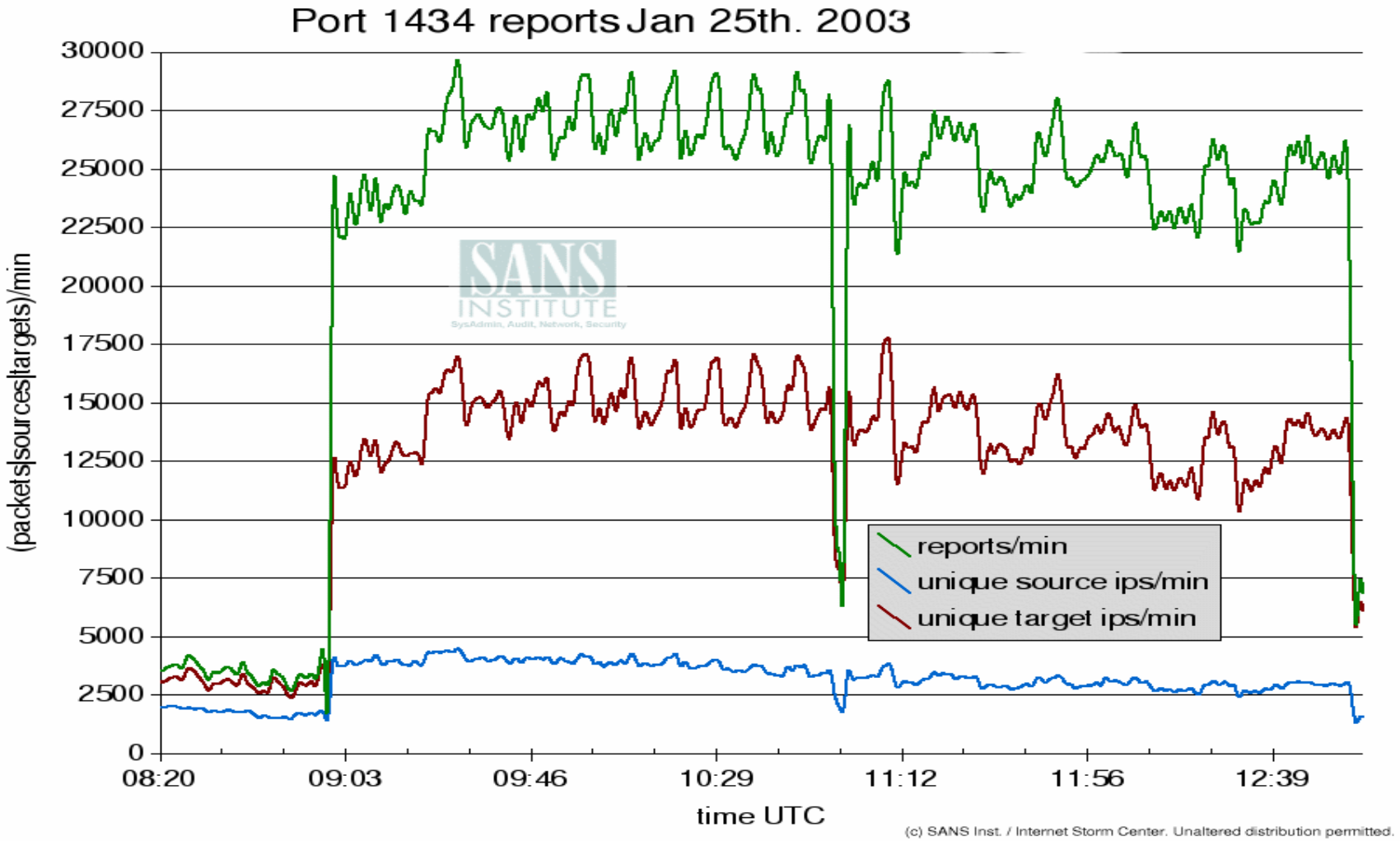
2) Case studies: SQL Slammer III

Or: How 376 bytes can shut down the Internet



2) Case studies: SQL Slammer IV

Or: How 376 bytes can shut down the Internet



References

[1] Haggerty, J.; Qi Shi; Merabti, M., "**Beyond the Perimeter: the Need for Early Detection of Denial of Service Attacks"**, 18th Annual Computer Security Applications Conference (ACSAC 2002)

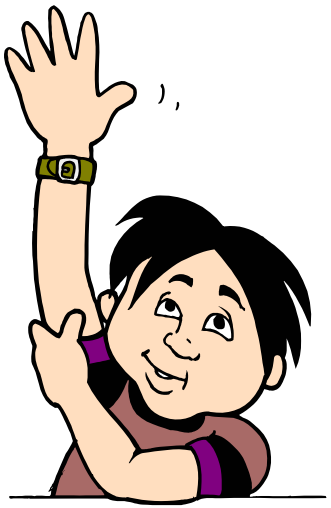
[2] Rocky K. C. Chang, **"Defending against Flooding-Based Distributed Denial-of-Service Attacks: A Tutorial"**, IEEE Communications Magazine, October 2002, pages: 42-51

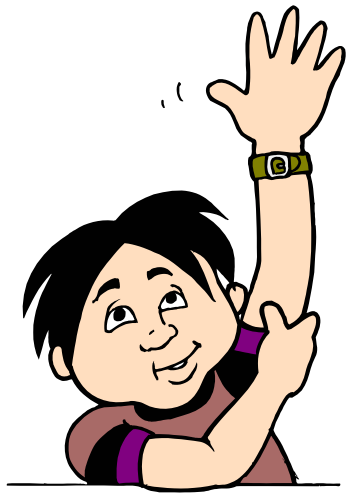
P2P as an attack platform

presented by

Arno Wagner

Thanks for your attention!





Any questions?