MITACS 4th Annual Conference
May 9, 2003 - Ottawa NAC

Computer Worms and the Telecommunications Infrastructure

Prof. Paul Van Oorschot (Carleton C.S.)
Dr. Jean-Marc Robert (Alcatel Canada)
Dr. Miguel Vargas Martin (Carleton C.S.)

Worm (November 2)

- software on one Internet machine
  - collected host, network and user info
  - broke into other machines
- replicated itself; replica continued likewise
- infected 10% of Internet machines (Unix variants)

Worm (November 2)

- software on one Internet machine
  - collected host, network and user info
  - broke into other machines
- replicated itself; replica continued likewise
- infected 10% of Internet machines (Unix variants)

Why important?

- Morris Worm (Nov.2, 1988)

How was Morris Worm Possible?

- configuration error *(Sendmail)*
- weak passwords (dictionary size: 432)
  - (where are we today?)
- trusted connections *(.rhosts* file)
- buffer overflow (*finger* daemon)
  - feature of C; still #1 flaw per CERT

- diversity: one worm felled 10% of Internet
- was patch available? YES ... but

Sapphire/Slammer worm (Jan. 25, 2003)

- fastest in history - doubling time: 8.5s
  - 90% of vulnerable hosts infected in 10 min
  - two orders magnitude faster than Code Red
  - hosts: 75K vs. 359K
- after 3 min: scanning rate 55M scans/s
- no malicious payload (would have been easy)

Carleton UNIVERSITY

Sapphire/Slammer worm (contd)

- buffer overflow: MSFT SQL server & desktop s/w
  - patch available: July 2002
  - only affected those behind on patches

- single-packet worm
  - 376 bytes (404-byte UDP packet)
  - bandwidth limited (100 Mbps servers)

significant milestone in evolution of worms

Carleton UNIVERSITY

Trends - Patches

- more frequent than ever
- installed only by minority
- Red Queen syndrome:

  [Here] it takes
  all the running you can do
  just to keep in the same place

Trends (cont'd)

- *Warhol worms* (15 minutes)
  - conference paper, Aug. 2002
    "How to Own the Internet in your Spare Time"
  - Slammer worm (Jan. 2003)

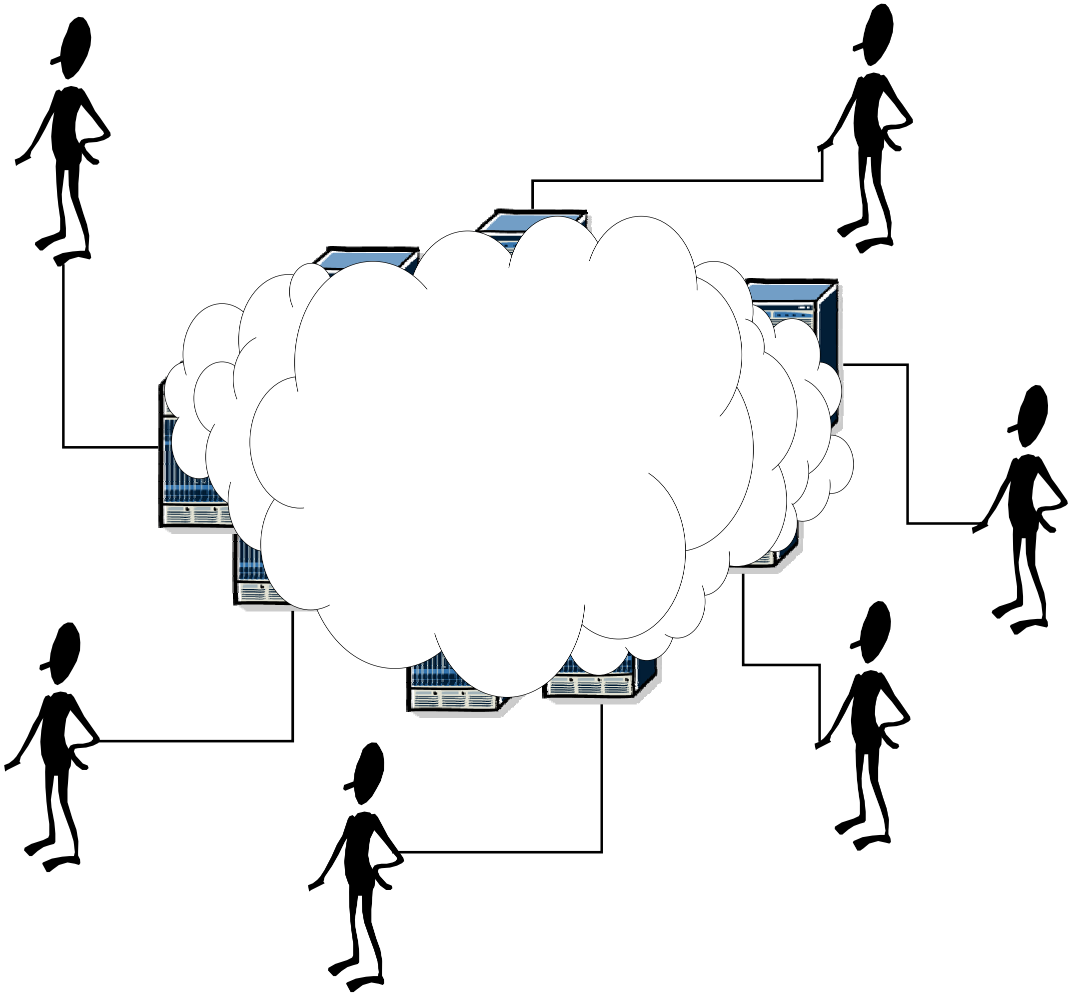
- *flash worms* (10's of seconds)
  - consider responses requiring human interaction

Carleton UNIVERSITY

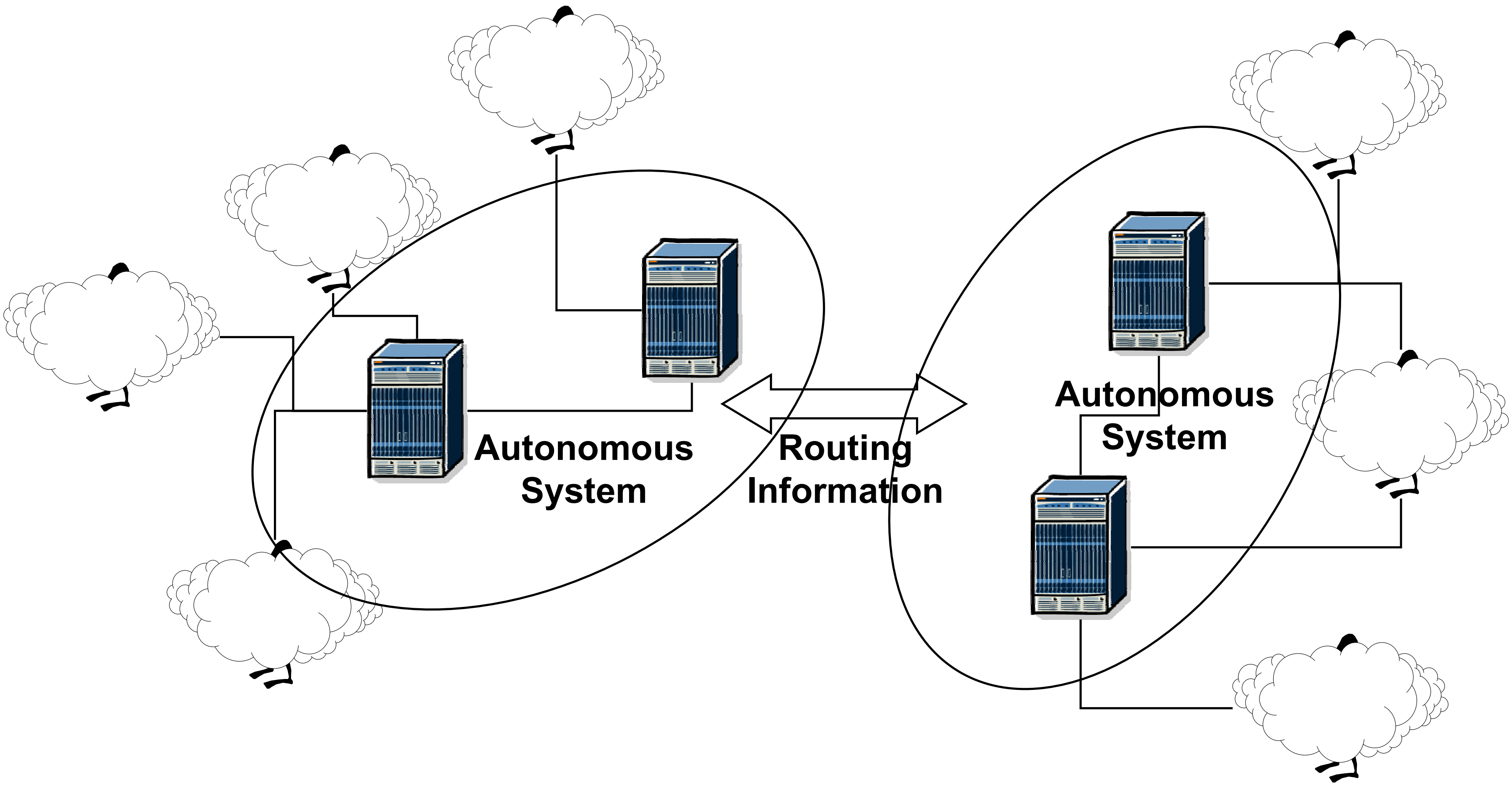
Computer Worms and the Telecommunications Infrastructure (Part II)

Jean-Marc Robert Ph.D.
Alcatel R&I Security Group

Typical View of the Internet User point of view



Our View of the Internet Telcos point of view



Challenge

Survivability

“... is the ability of a system to fulfill its mission, in a timely manner, in the presence of attacks, failures, or accidents”

Who is at Risk?

From the viewpoint of the telecommunication systems, there are two targets:

- The ***network equipment***
  - According to a report of the CERT Coordination Center of the CMU Software Engineering Institute, a recent attack trend is to target or to use infrastructure elements, such as routers.
- The ***systems*** connected to network equipment.

Denial-of-Service Attack Taxonomy

From the viewpoint of the telecommunication systems, the attacks can be divided into two groups:

- The ***DoS-Victim attacks*** correspond to attacks against the network equipment themselves
  - E.g. *SYN Flood* or *Ping-of-Death* against a router
- The ***DoS-Carrier attacks*** correspond to attacks against systems connected to network equipment
  - E.g. *SYN Flood* or *Slammer* against an end-user using resources at the network-level ***and*** at the end-user-level

Worms and Routing Infrastructure

Worms Target:

- Slammer → MySQL
- Nimda → IIS
- Code Red → IIS

Why are they impacting the routing infrastructure?

ALCATEL

Worms Potential Impact

Due to some extreme conditions heavy traffic load routers are more sensitive to:

- Software vulnerabilities
- Resource exhaustion
  - CPU Overload
  - Buffer overflows
  - Memory exhaustion

Classical Software Engineering Problems

ALCATEL

But the Major Impact May Be Elsewhere

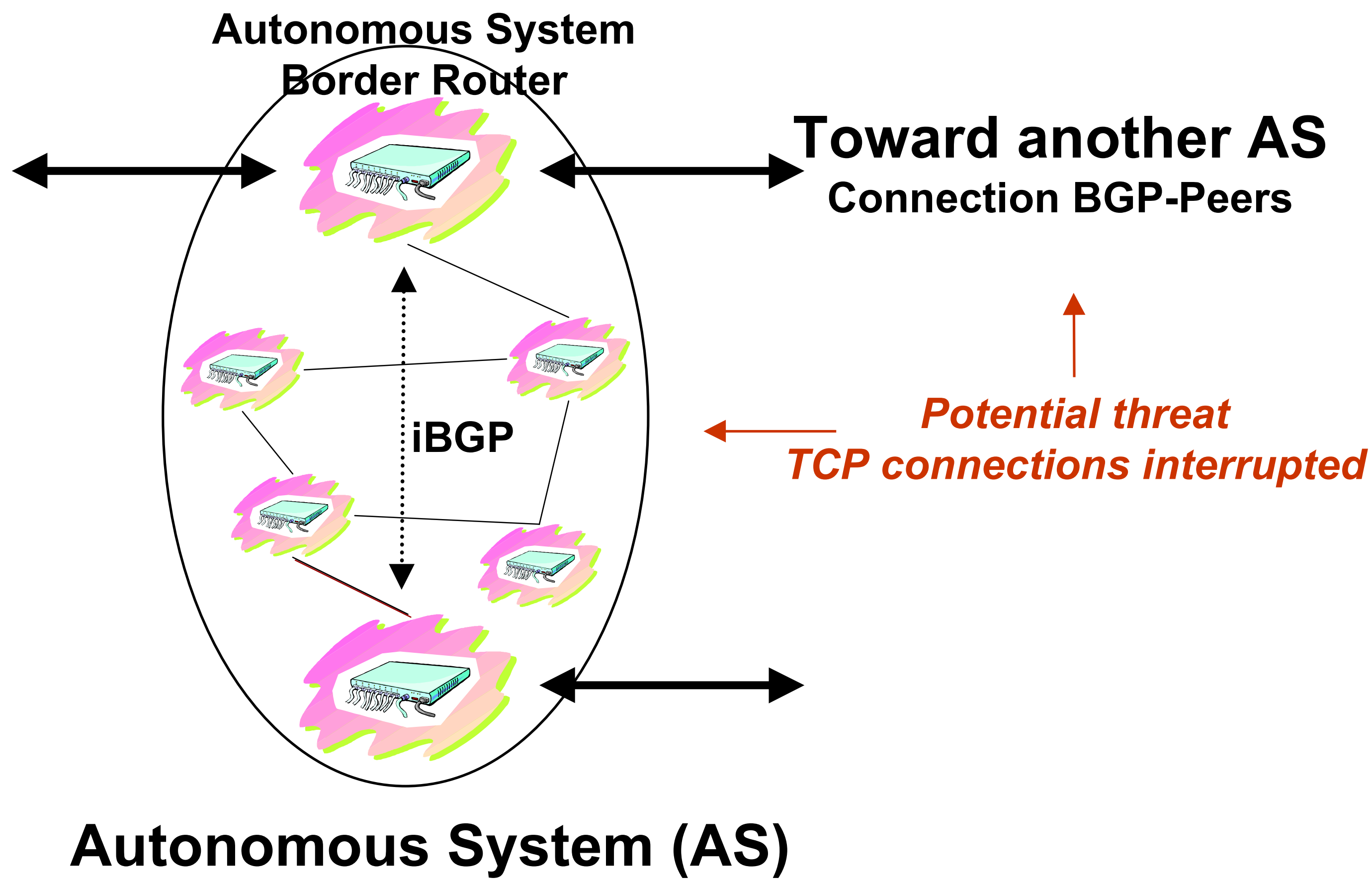
Traffic diversity i.e. many new flows

- Caching problem in routers → CPU overload
- Non-existing routers → "ICMP storms"

Instability in the routing information (???)

- The *Border Gateway Protocol (BGP)* is a routing protocol used to exchange information between Autonomous Systems

Routing Architecture



BGP (Potential) Instabilities

Instability observed under stress conditions

- Intra-AS flapping and routing failures
- High BGP message load
- Route computation → CPU overload

Reason (?)

- Potential failures in the TCP connections between BGP peers
  - Forcing exchange of BGP Tables (~100,000 entries)

BGP (Potential) Instabilities

Unfortunately, only a few results have been published on this research area *and they are contradictory*

Problems

- Hard to simulate a complex system such as the Internet
- Hard to monitor automatically a complex system without any bias

Conclusion

The impact of worms on routing infrastructure shall be studied more thoroughly by the industry and by the academic community. For example, what are the real impact

- On the routing protocols
- On the congestion algorithms
- On the quality-of-service approaches

An important step toward those objectives is a better understanding of the worm behavior

MITACS 4th Annual Conference

May 9, 2003 - Ottawa NAC

Classification of Worms

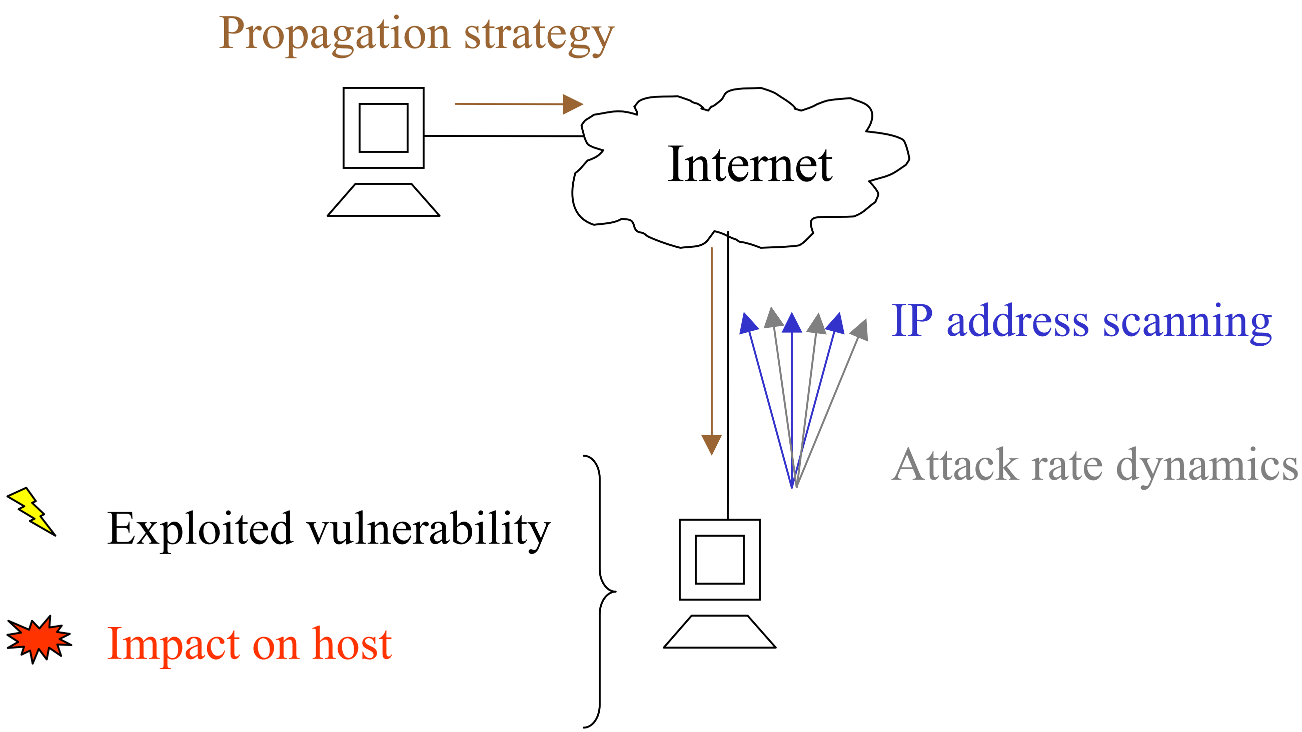
Miguel Vargas Martin

Digital Security Group

School of Computer Science

Carleton University

Characteristics of Worms



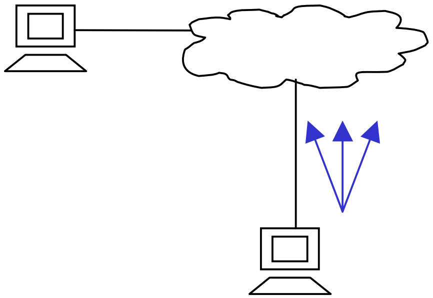
Carleton UNIVERSITY

Worms Studied

1 Morris	5 Code Red II
2 Sadmind	6 Nimda
3 Code Red v2	7 Slammer
4 Sircam	8 Code Red III

Carleton UNIVERSITY

IP Address Scanning



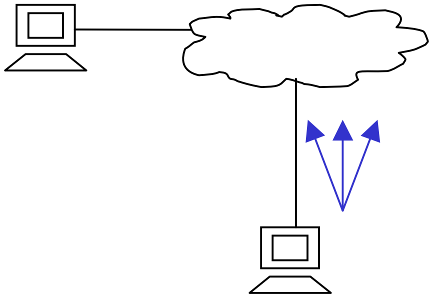
random

host related

local subnet
- *probabilistic*
- *non-probabilistic*

hitlist

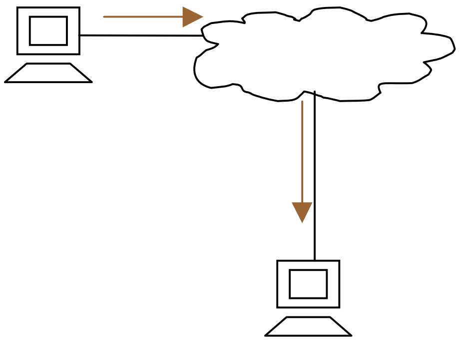
permutation



IP Address Scanning

worm	IP address scanning			
	random	host related	local subnet	
			probabilistic	non-probabilistic
Morris	v	v		v
Sadmind	v			v
Code Red v2	v			
Sircam		v		
Code Red II	v		v	
Nimda	v	v	v	
Slammer	v			
Code Red III	v		v	

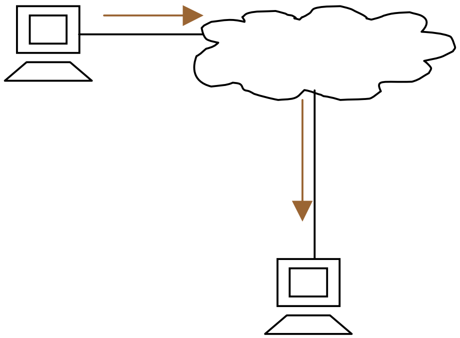
Propagation Nature



uniform payload
- *central*
- *back-chaining*
- *autonomous*

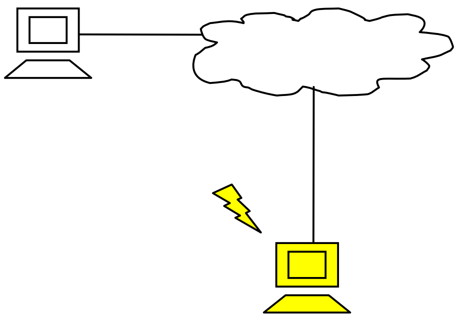
poly-morphic
- *central*
- *back-chaining*
- *autonomous*

Propagation Nature



worm	***propagation nature***		
	uniform payload		
	central	***back-chaining***	***auton-omous***
Morris		v	v
Sadmind		v	
Code Red v2			v
Sircam			v
Code Red II			v
Nimda	v	v	v
Slammer			v
Code Red III			v

Exploited Vulnerability



protocol

implementation

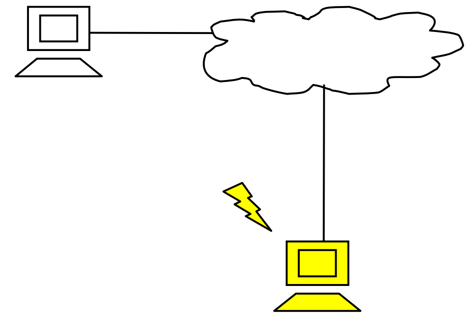
design

characteristics

misconfiguration/bad default setting

Carleton UNIVERSITY

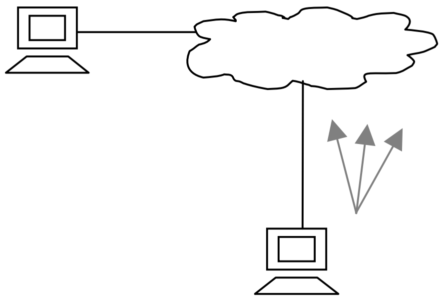
Exploited Vulnerability



worm	*exploited vulnerability*	
	implementation	*configuration/ bad default settings*
Morris	`sendmail`, `finger`	`.rhosts` / weak password policy
Sadmind	`sadmind`, IIS	
Code Red v2	IIS	
Sircam		network shares
Code Red II	IIS	
Nimda	IIS, Code Red II and Sadmind backdoors	java script
Slammer	SQL	
Code Red III	IIS	

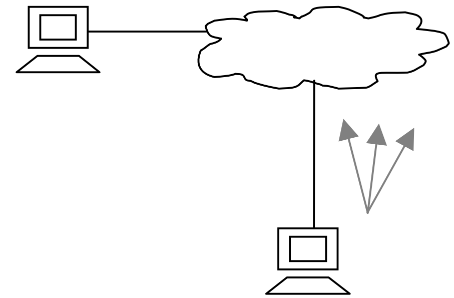
Carleton UNIVERSITY

Attack Rate Dynamics



continuous
- *latency-limited*
- *bandwidth-limited*

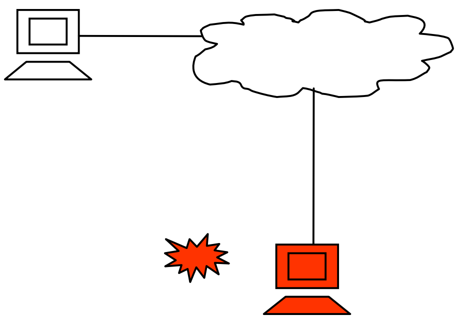
variable
- *fluctuating*
- *increasing*



Attack Rate Dynamics

worm	attack rate dynamics		
	continuous		variable
	latency-limited	bandwidth-limited	fluctuating
Morris	v		
Sadmind	v		
Code Red v2	v		v
Sircam			v
Code Red II	v		
Nimda	v		v
Slammer		v	
Code Red III	v		

Impact on Infected Host



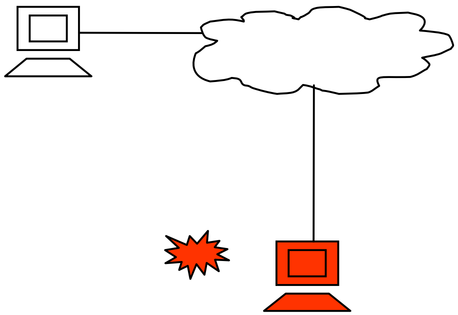
disruptive

- *delete/modify files*
- *subvert as DDoS zombie*
- *install backdoors*

degrading (bandwidth, processing power)

Carleton UNIVERSITY

Impact on Infected Host



worm	*impact on infected host*			
	disruptive			*degrading bandwidth/ processing power*
	file modifications /deletions	*DDoS zombie*	*back door*	
Morris				v
Sadmind	v		v	v
Code Red v2	v	v	v	v
Sircam	v			
Code Red II	v	v	v	v
Nimda	v		v	v
Slammer				v
Code Red III	v	v	v	v

Final Remarks

Worms are currently among the biggest threats to the Internet, and therefore understanding them better is one the most important things we can do.