

Research in Computer Viruses and Worms

Tom Chen

SMU

tchen@engr.smu.edu

Outline

- About Me and SMU
- Background on Viruses/Worms
- Research Activities
 - Virus research lab
 - Early detection
 - Epidemic modeling

About Me

- PhD in electrical engineering from U. California, Berkeley
- GTE (Verizon) Labs: research in ATM switching, traffic modeling/control, network operations
- 1997 joined EE Dept at SMU: traffic control, mobile agents, network security

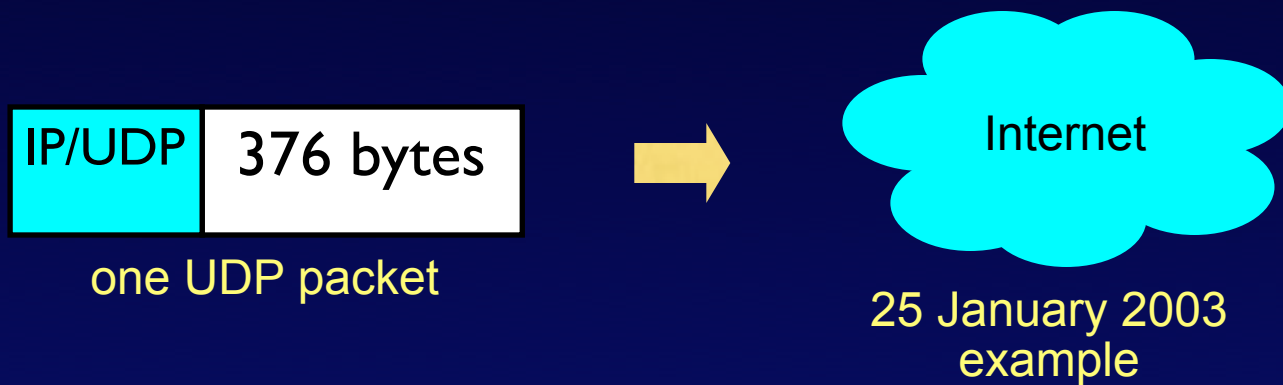
About SMU

- Small private university with 6 schools - engineering, sciences, arts, business, law, theology
- 6,300 undergrads, 3,600 grads, 1,200 professional (law, theology) students
- School of Engineering: 51 faculty in 5 departments
- Dept of EE: specialization in signal processing, communications, networking, optics

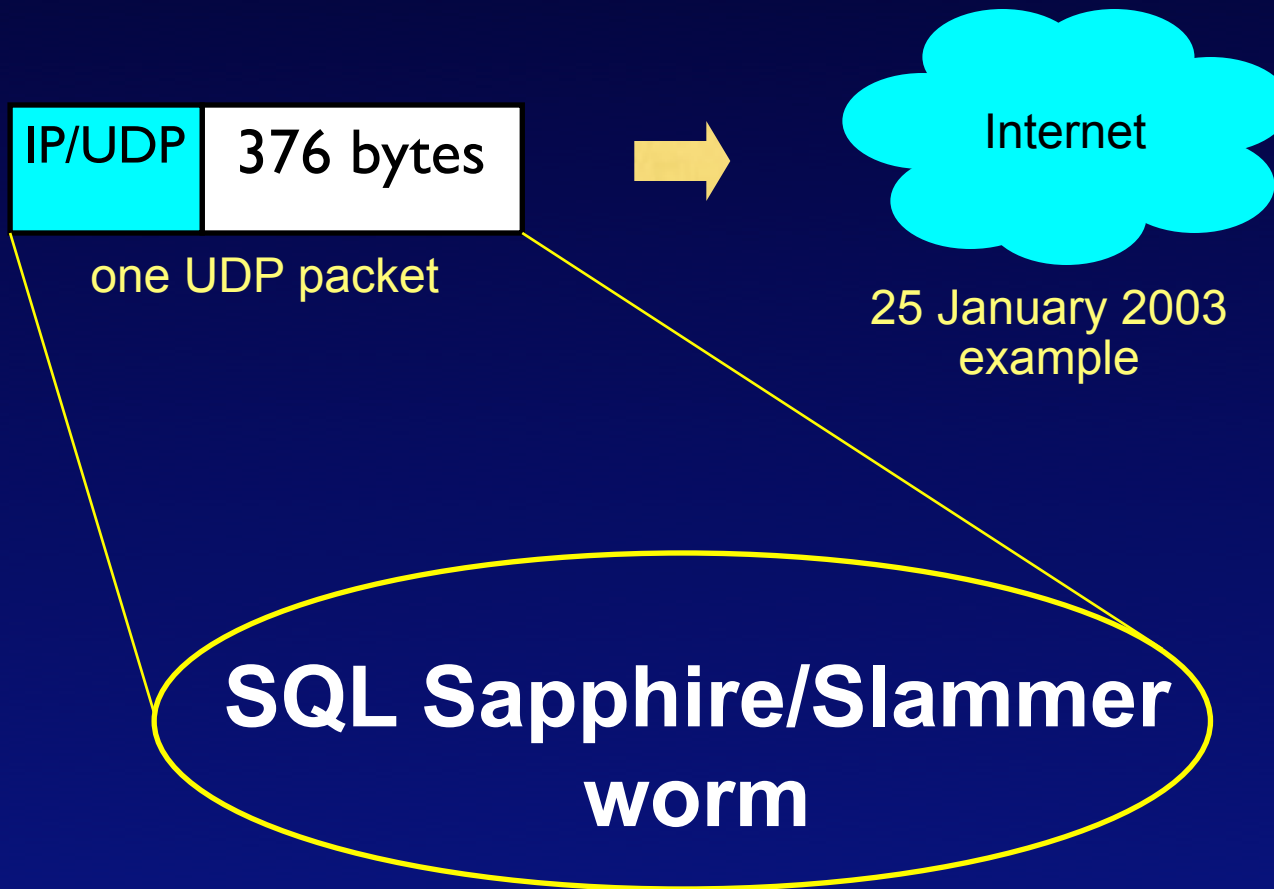
Background on Viruses and Worms

Motivations

Can one IP packet cripple the Internet within 10 minutes?

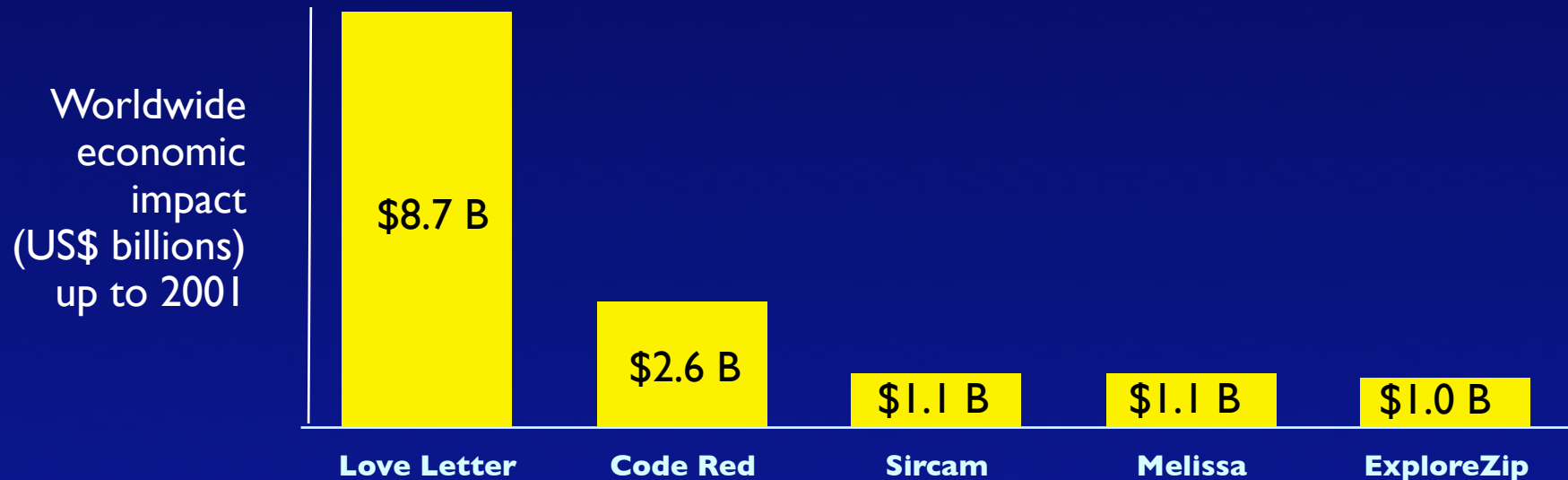


- More than 1.2 billion US dollars damage
- Widespread Internet congestion
- Attack peaked in 10 minutes
- 70% South Korea's network paralyzed
- 300,000 ISP subscribers in Portugal knocked off line
- 13,000 Bank of America machines shut down
- Continental Airline's ticketing system crippled



Top Viruses/Worms

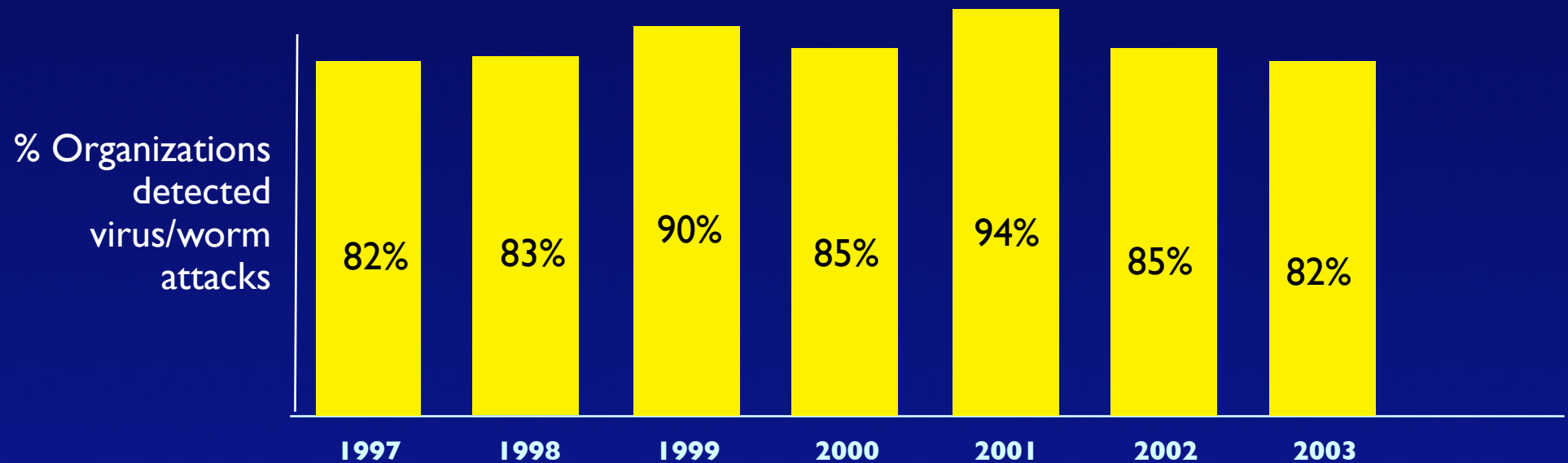
- 70,000+ viruses are known -- only hundreds “in the wild”
- A few viruses cause the most damage



*estimated by Computer Economics 2001

Prevalence

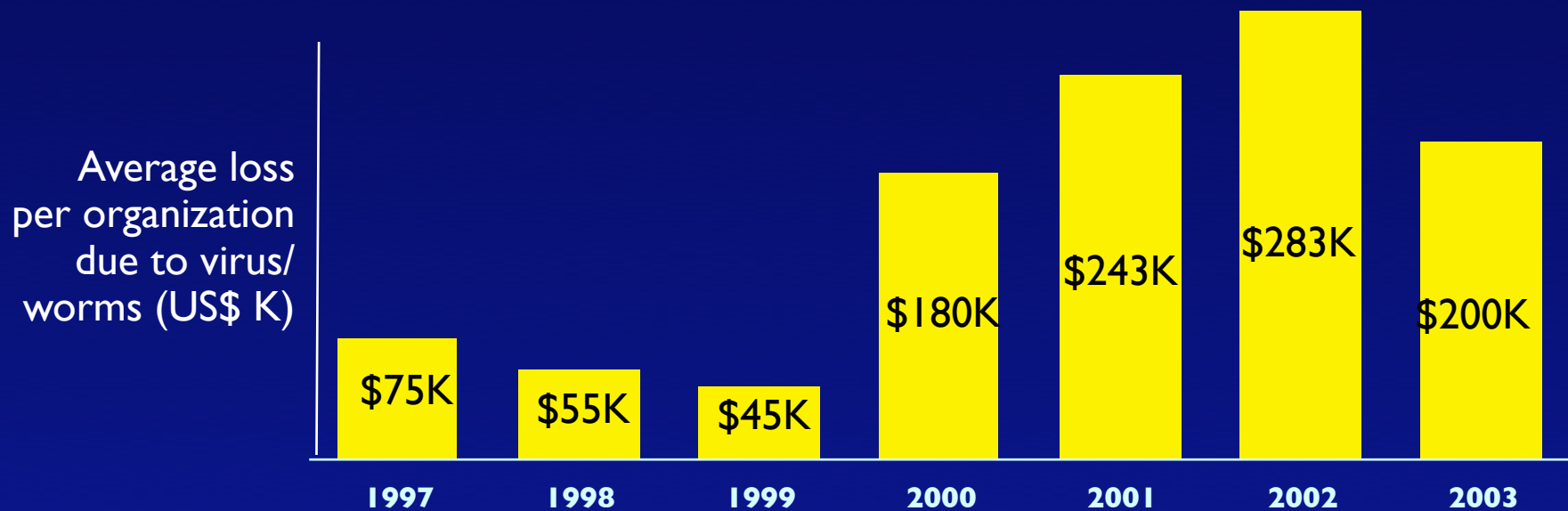
- Viruses/worms are consistently among most common attacks



*2003 CSI/FBI Computer Crime and Security Survey

Damages

- Third most costly security attack (after theft of proprietary info and DoS)



*2003 CSI/FBI Computer Crime and Security Survey

What are Viruses

- Key characteristic: ability to self-replicate by modifying (infecting) a normal program/file with a copy of itself
 - Execution of the host program/file results in execution of the virus (and replication)
 - Usually needs human action to execute infected program

Cohen's Viruses

- Nov. 1983 Fred Cohen (“father” of computer virus) thought of the idea of computer viruses as a graduate student at USC
 - “Virus” named after biological virus
- Cohen wrote the first documented virus and demonstrated on the USC campus network

Cohen's Viruses (cont)

Biological virus

Consists of DNA or RNA strand surrounded by protein shell to bond to host cell

No life outside of host cell

Replicates by taking over host's metabolic machinery with its own DNA/RNA

Copies infect other cells

Computer virus

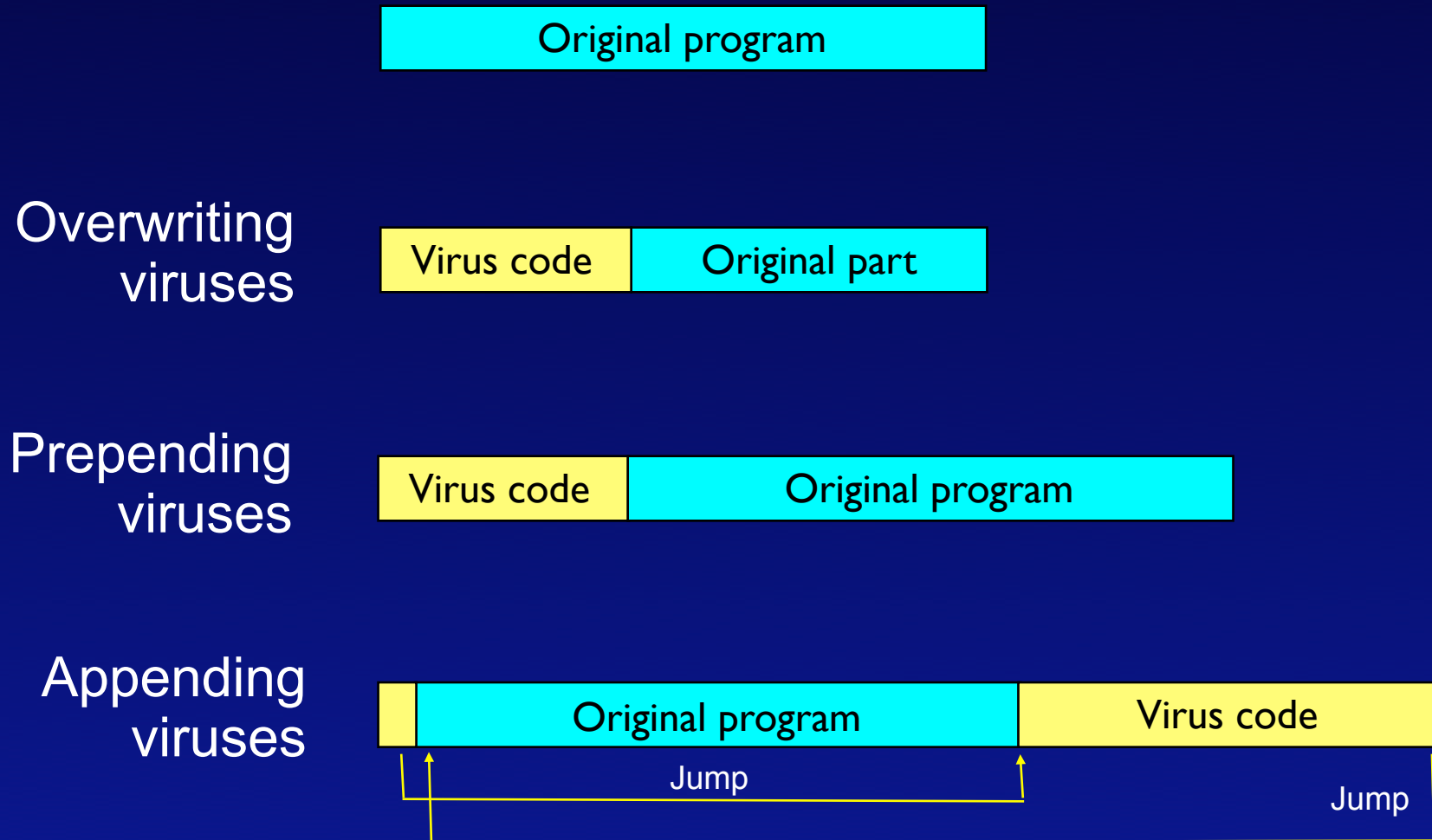
Consists of set of instructions stored in host program

Active only when host program executed

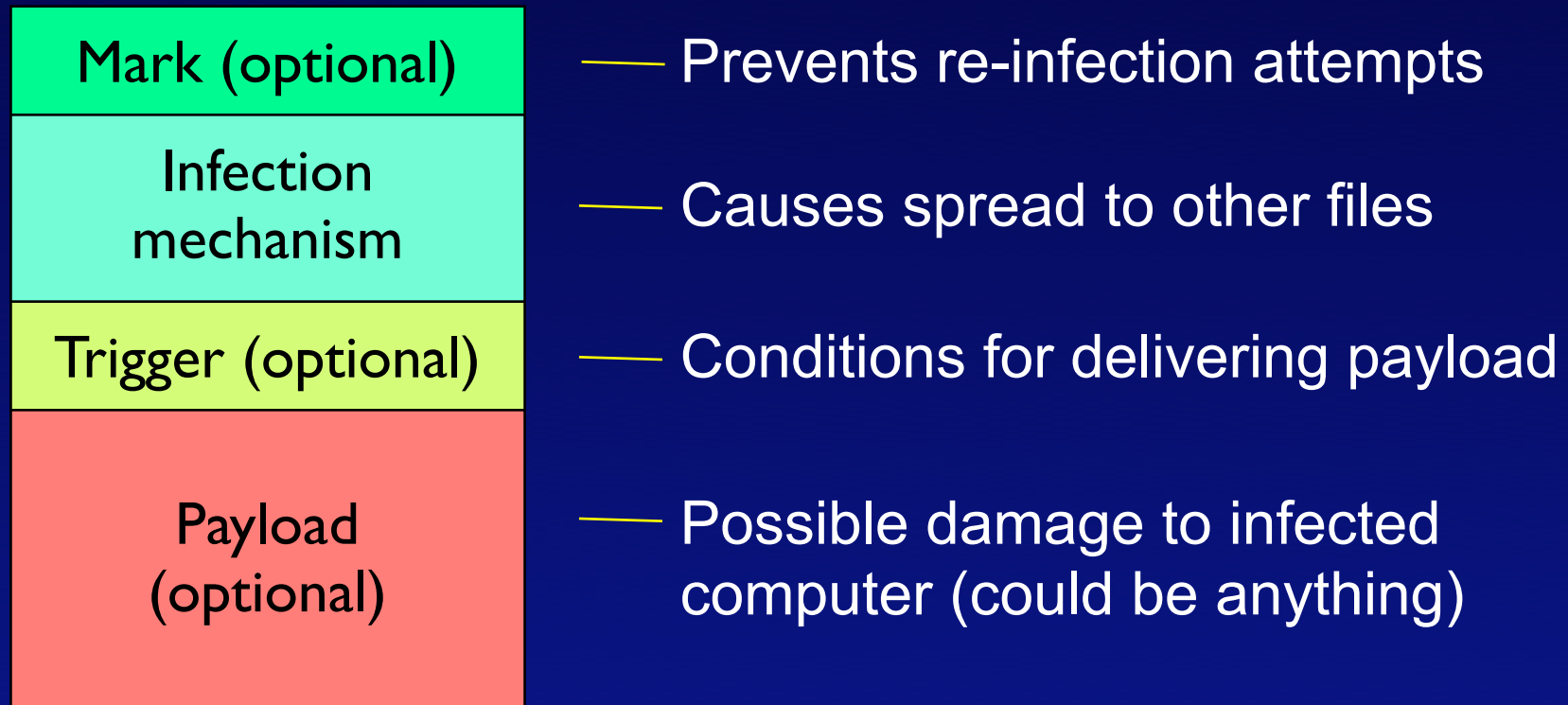
Replicates when host program is executed or host file is opened

Copies infect (attach to) other host programs

Virus Examples



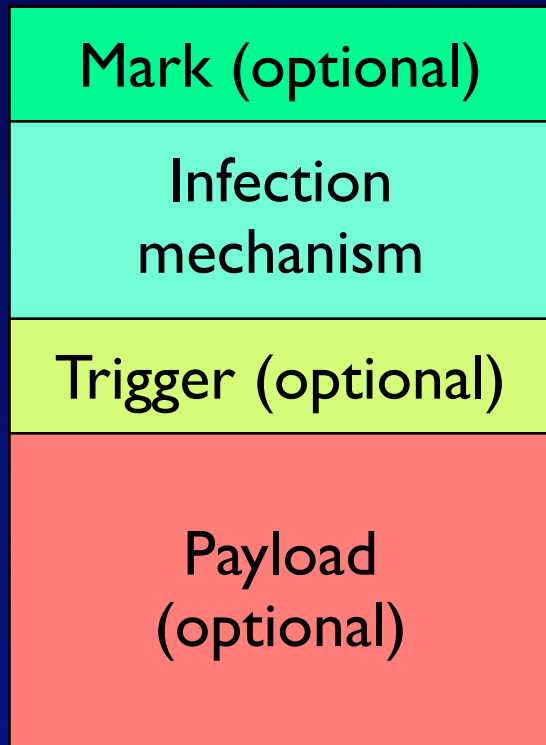
Virus Anatomy



What are Worms

- Worm is also self-replicating but a stand-alone program that exploits security holes to compromise other computers and spread copies of itself through the network
 - Unlike viruses, worms do not need to parasitically attach to other programs
 - Inherently network dependent
 - Do not need any human action to spread

Worm Anatomy

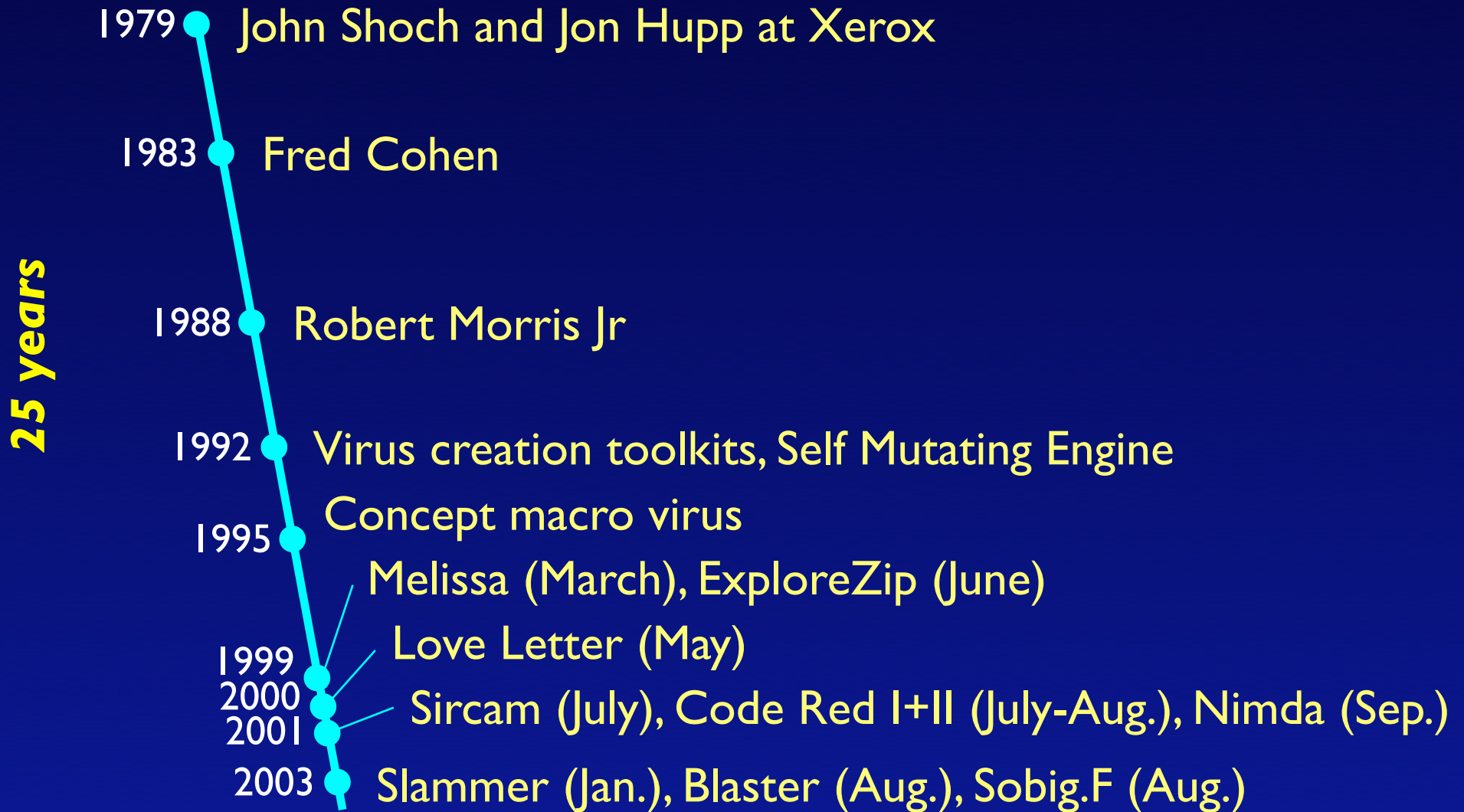


- Structurally similar to viruses, except a stand-alone program instead of program fragment
- Infection mechanism searches for weakly protected computers through a network (ie, worms are network-based)
- Payload might drop a Trojan horse or parasitically infect files, so worms can have Trojan horse or virus characteristics

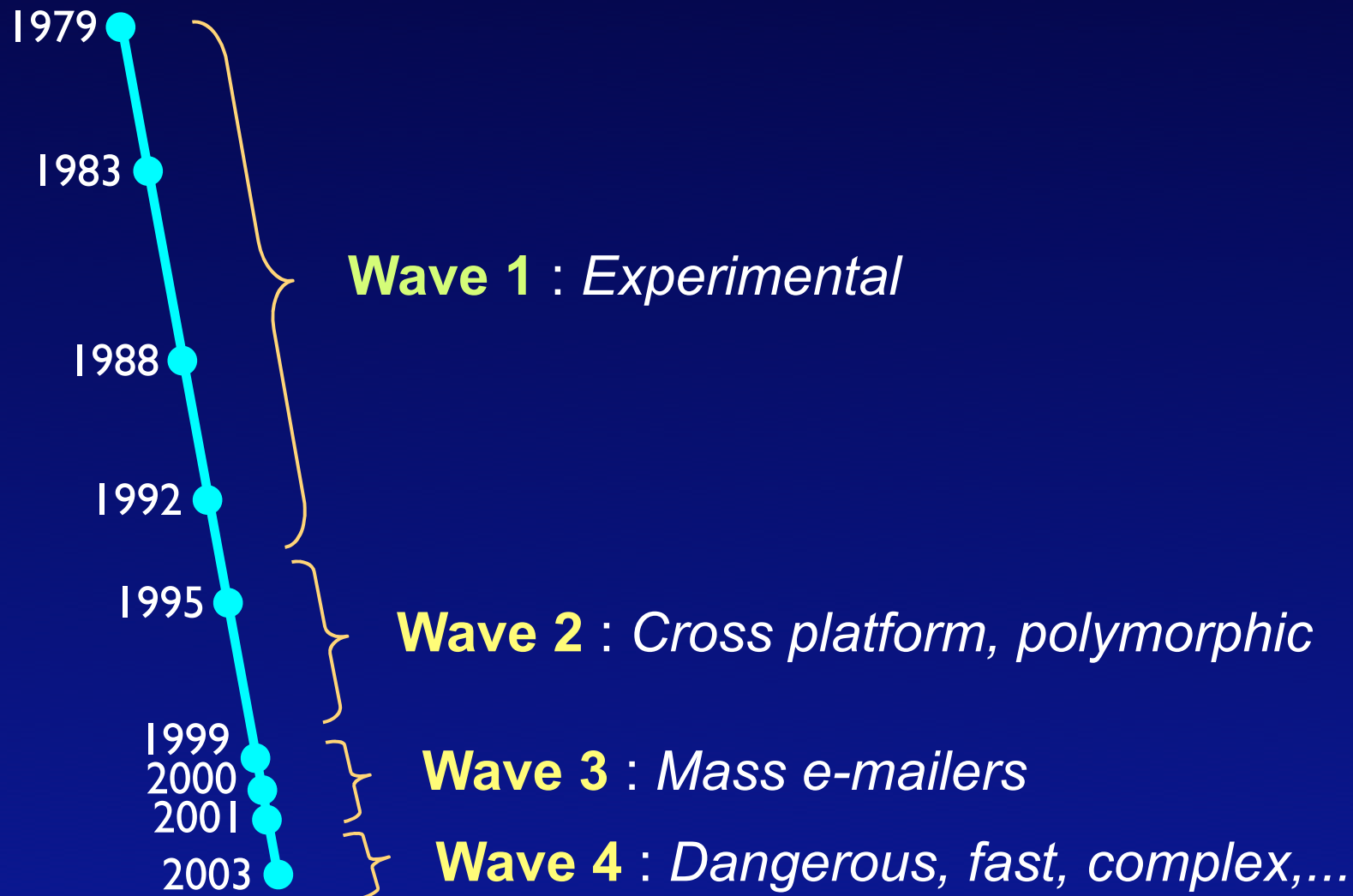
Worms (cont)

- Worms are more common and dangerous than viruses today
 - Virtually all computers are networked
 - Worms spread quickly through networks without need for human actions
 - People are more alert about viruses (disable MS Office macros, turn on antivirus software,...)

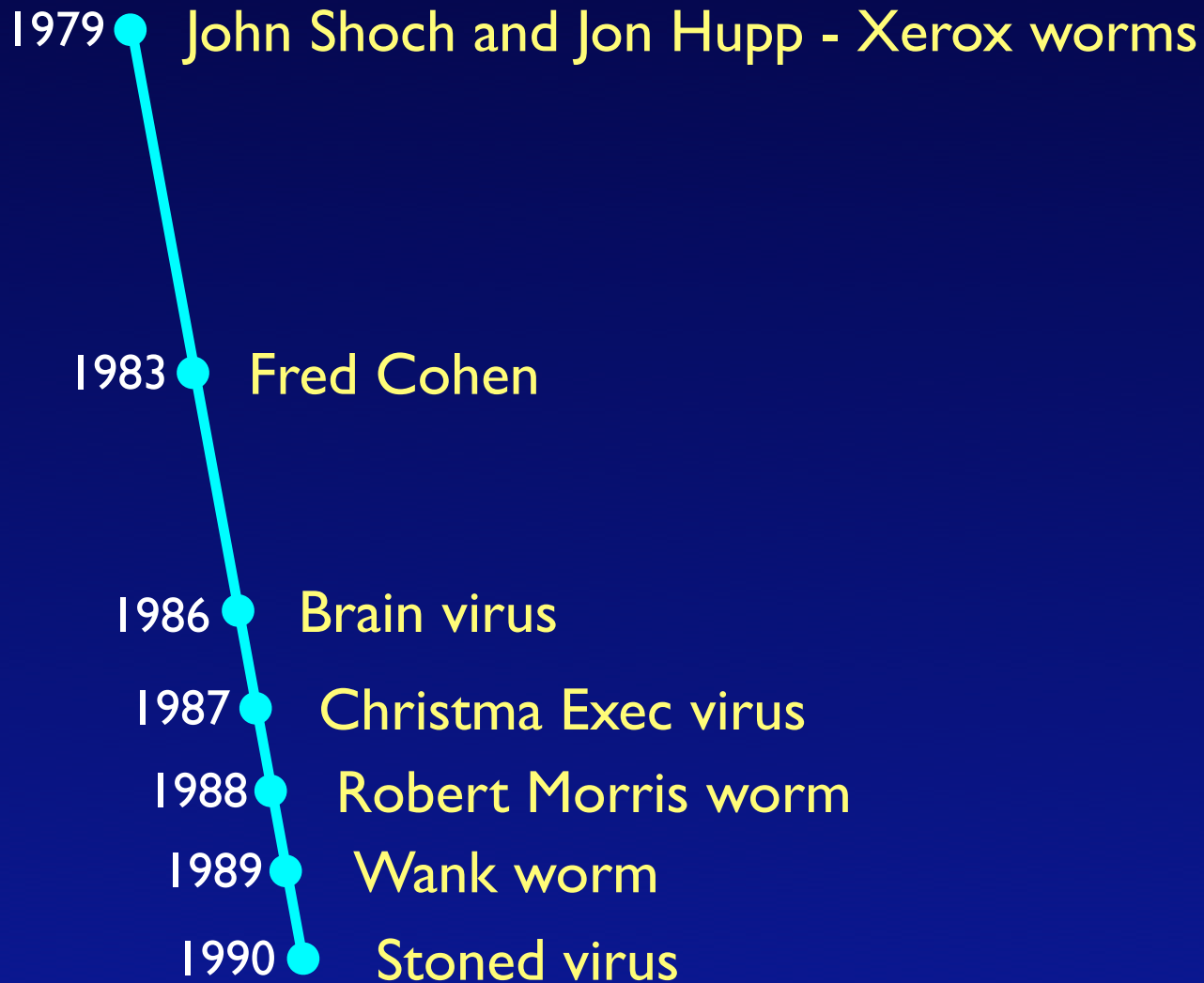
Virus/Worm Highlights



Past Trends: 4 Waves



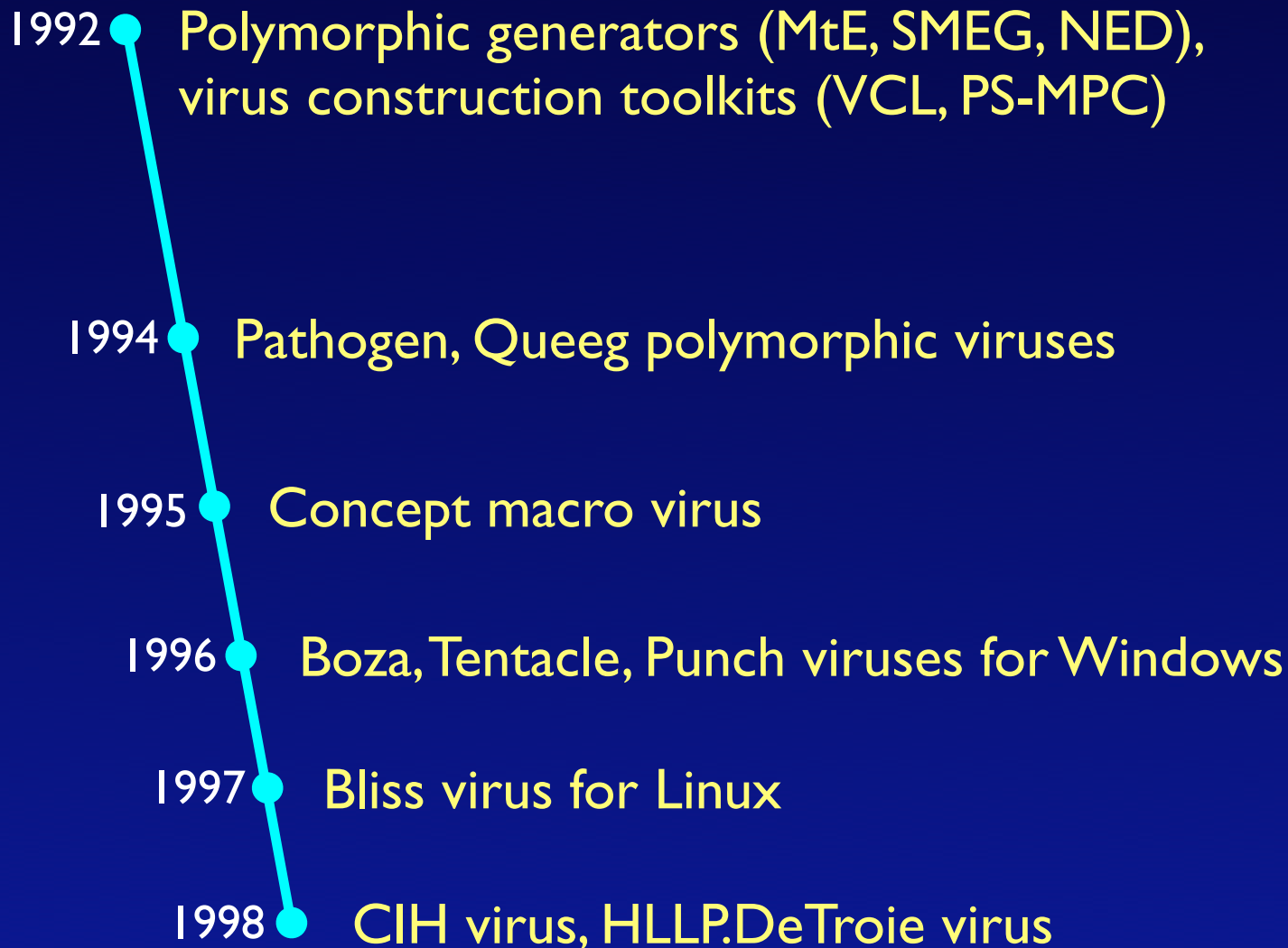
Wave 1



Wave 1 Highlights

- Most viruses limited to DOS and spread slowly by diskettes
- Experiments with worms (Xerox, Morris) got out of control
- Beginnings of stealth viruses and social engineering attacks

Wave 2



Wave 2 Highlights

- Easy-to-use virus toolkits allow large-scale automated creation of viruses
- Polymorphic generators allow easy creation of polymorphic viruses (appearance is scrambled) - challenges antivirus software
- Most viruses target Windows
- Macro viruses go cross-platform

Wave 3



Wave 3 Highlights

- Mass e-mailing viruses become most popular
 - Attacks increase in speed and scope
- Social engineering (tricking users into opening attachments) becomes common
- Worms start to become dangerous (data theft, dynamic plug-ins)

Wave 4



Wave 4 Highlights

- New infection vectors (Linux, peer-to-peer, IRC chat, instant messaging,...)
- Blended attacks (combined vectors)
- Dynamic code updates (via IRC, web,...)
- Dangerous payloads - backdoors, spyware
- Armored viruses try to disable antivirus software
- Sophisticated worms (Code Red, Nimda, Slammer, Blaster) spread very fast

Top 2004 Worms

- MyDoom spreads by e-mail to Windows PCs, searches for e-mail addresses in various files, opens backdoor for remote access
- Netsky spreads by e-mail, exploits Internet Explorer to automatically execute e-mail attachments, removes MyDoom and Bagle from PCs

Top 2004 Worms (cont)

- Bagle spreads by e-mail, tries to remove Netsky from PCs, opens backdoor for remote access, downloads code updates from Web, disables antivirus and firewall software

Current Defenses

- Antivirus software
- Operating system patching
- Firewalls
- Intrusion detection systems (IDS)
- Router access control lists

➤ **So why do worm outbreaks continue?**

Software Issues

- Antivirus software works by virus signatures combined with heuristics
 - Signatures are more accurate, but need time to develop for each new virus and constant updating
 - Heuristics can detect new viruses before signature is available, but not perfect detection
- Many people do not use antivirus software or keep it updated

Software Issues (cont)

- OS patches are announced regularly, but not always used
 - Constant patching takes time and effort
 - Patches can cause software conflicts
 - Patches are often available only for most critical vulnerabilities
- Missed patches leaves window of vulnerability for worms to exploit

Network Issues

- Firewalls are partially effective but
 - Need expert configuration of filter rules
 - May still allow viruses/worms to pass via allowed services
 - May allow new viruses/worms to pass
- Current IDS equipment are susceptible to high rates of false positives (false alarms)
 - Detection accuracy is major issue

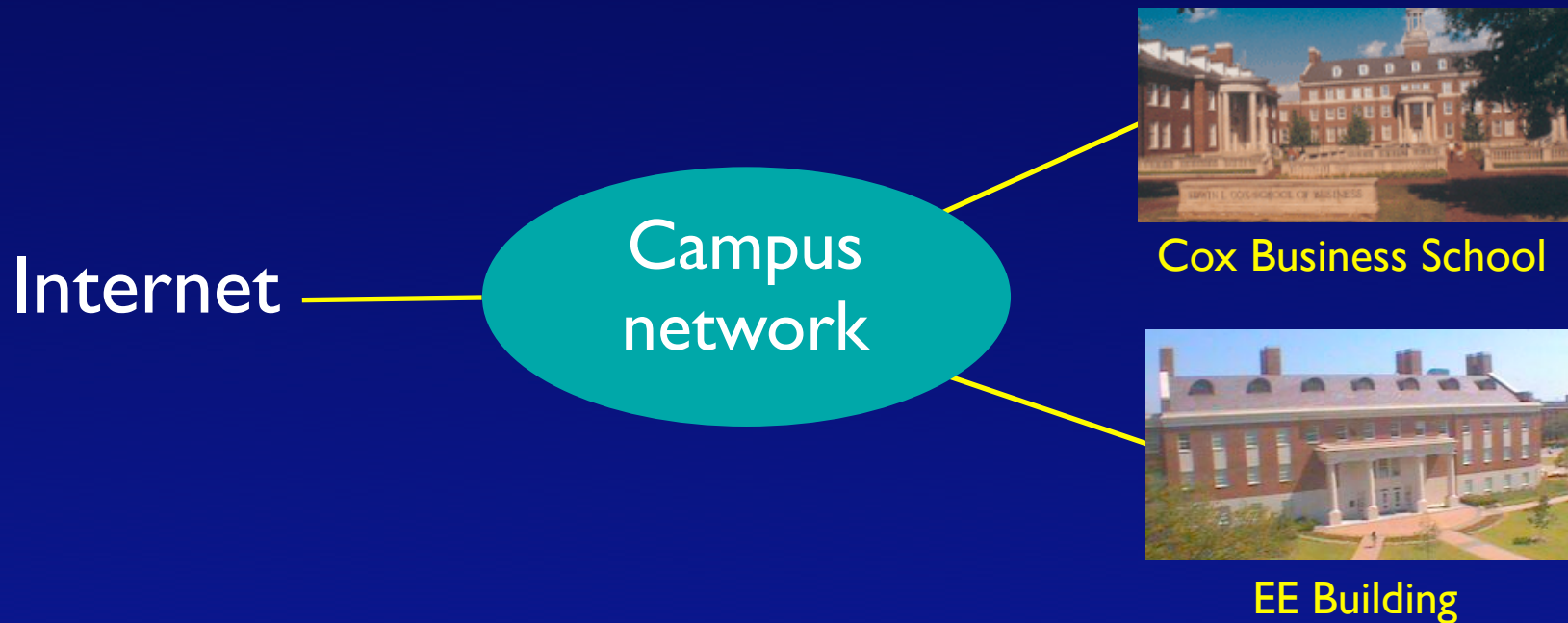
Research Activities

Research Activities

- Virus research lab
- Early detection of worms
- Epidemic modeling

Virus Research Lab

- Distributed computers in EE building and Business School



Virus Research Lab (cont)

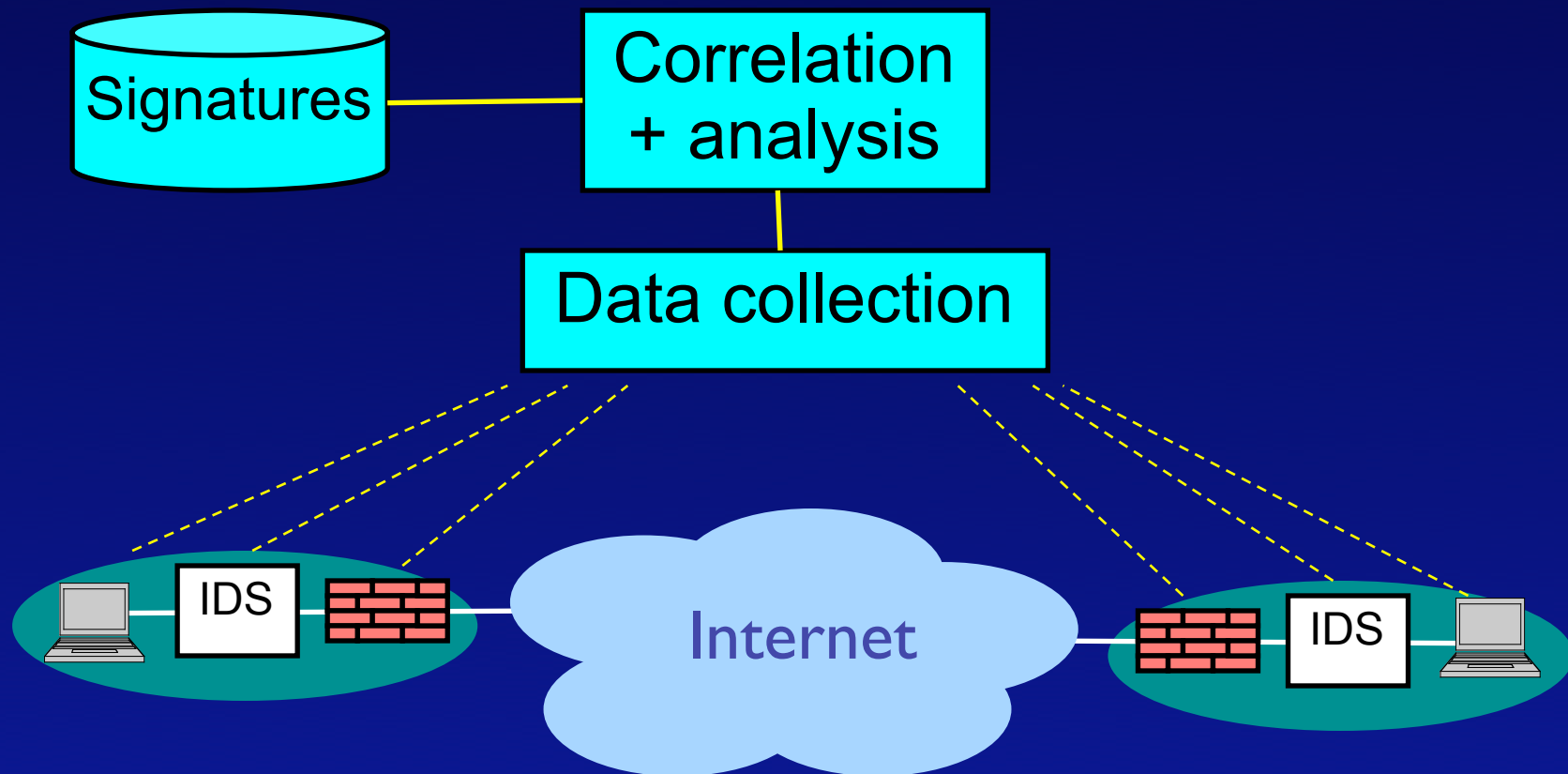
- Intrusion detection systems to monitor live traffic
 - Snort, Prelude, Samhain
- Honeypots to catch viruses
 - Honeyd, Logwatch, Nagios
- Network/virus simulator
 - To simulate virus behaviors in different network topologies

Early Detection of Worms

- Goal is global system for early warning of new worm outbreaks
- Jointly with Symantec to enhance their DeepSight Threat Management System
 - DeepSight collects log data from hosts, firewalls, IDSs from 20,000 organizations in 180 countries
 - Symantec correlates and analyzes traffic data to track attacks by type, source, time, targets

Early Detection (cont)

- Architecture of DeepSight



Early Detection (cont)

- Addition of honeypots to DeepSight
- Honeypots are “decoy” computers configured to appear vulnerable to attract attacks and collect data about attacker behavior
 - Can be used to capture worms
 - Carefully restricted from spreading any attacks to network

Epidemic Modeling

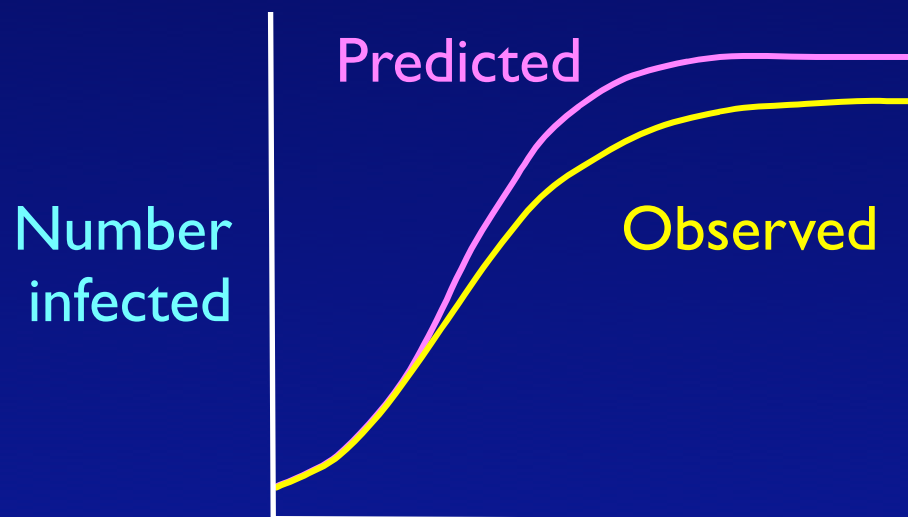
- Epidemic models predict spreading of diseases through populations
 - Deterministic and stochastic models developed over 250 years
 - Helped devise vaccination strategies, eg, smallpox
- Our goal is to adapt epidemic models to computer viruses and worms
 - Take into account different behavior of computer viruses and effect of network congestion

Basic Epidemic Model

- Assumes all hosts are initially Susceptible, can become Infected after contact with an Infected
 - Assumes fixed population and random contacts
- Number of Infected hosts shows logistic growth

Basic Epidemic (cont)

- Logistic equation predicts “S” growth
- Observed worm outbreaks (eg, Code Red) tend to slow down more quickly than predicted



Basic Epidemic (cont)

- Initial rate is exponential: random scanning is efficient when susceptible hosts are many
- Later rate slow downs: random scanning is inefficient when susceptible hosts are few
- Spreading rate also slows due to network congestion caused by heavy worm traffic

Dynamic Quarantine

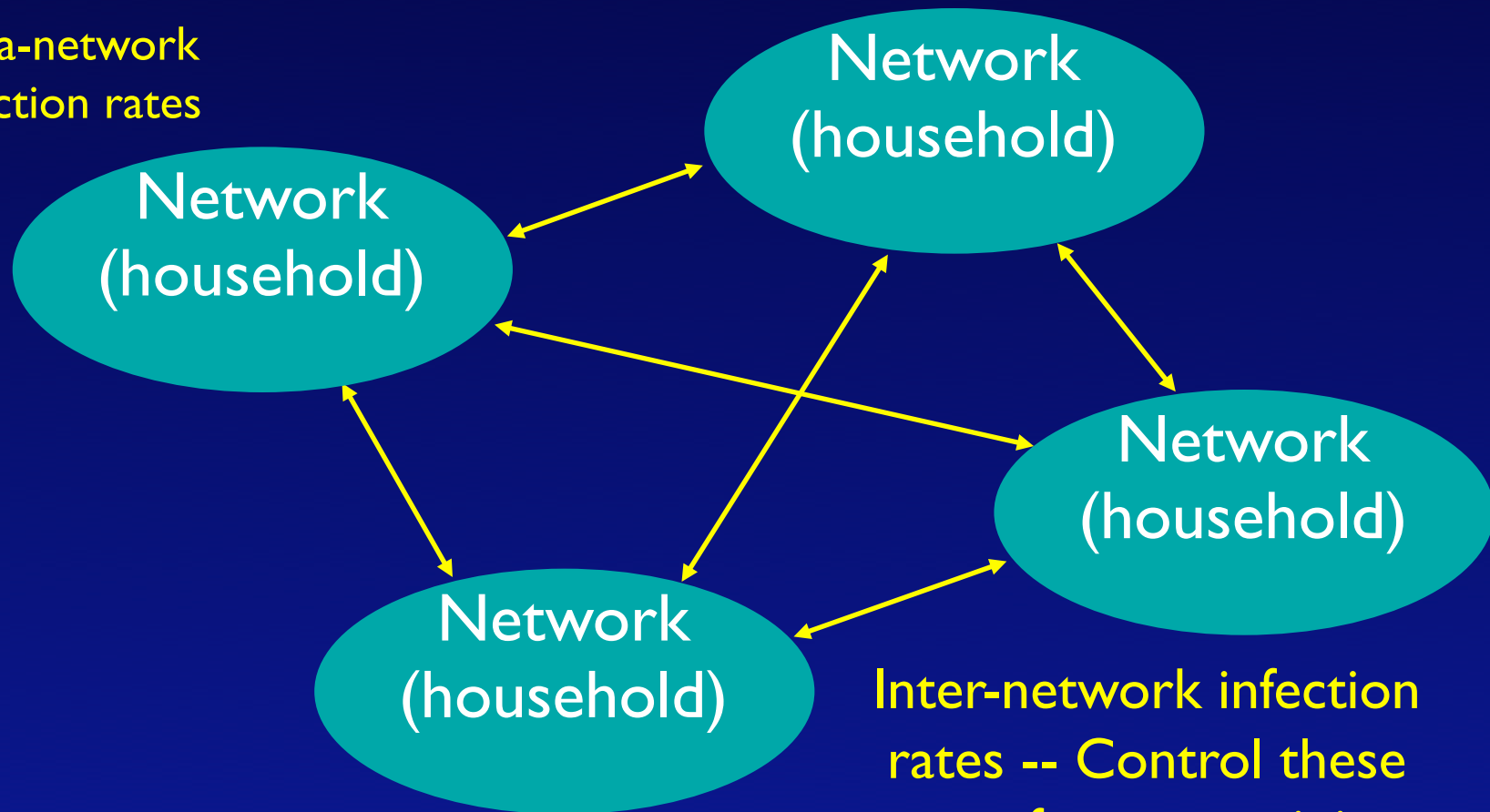
- Recent worms spread too quickly for manual response
- Dynamic quarantine tries to isolate worm outbreak from spreading to other parts of Internet
 - Cisco and Microsoft proposals
- Epidemic model?

Quarantining (cont)

- “Community of households” epidemic model assumes
 - Population is divided into households
 - Infection rates within households can be different than between households
- Similar to structure of Internet as “network of networks”

Quarantining (cont)

Intra-network
infection rates



Inter-network infection
rates -- Control these
rates for quarantining

Conclusions

- Viruses and worms will continue to be an enormous network security problem
- New technologies are needed in
 - Early detection
 - Dynamic quarantining
 - Intrusion-tolerant networks