



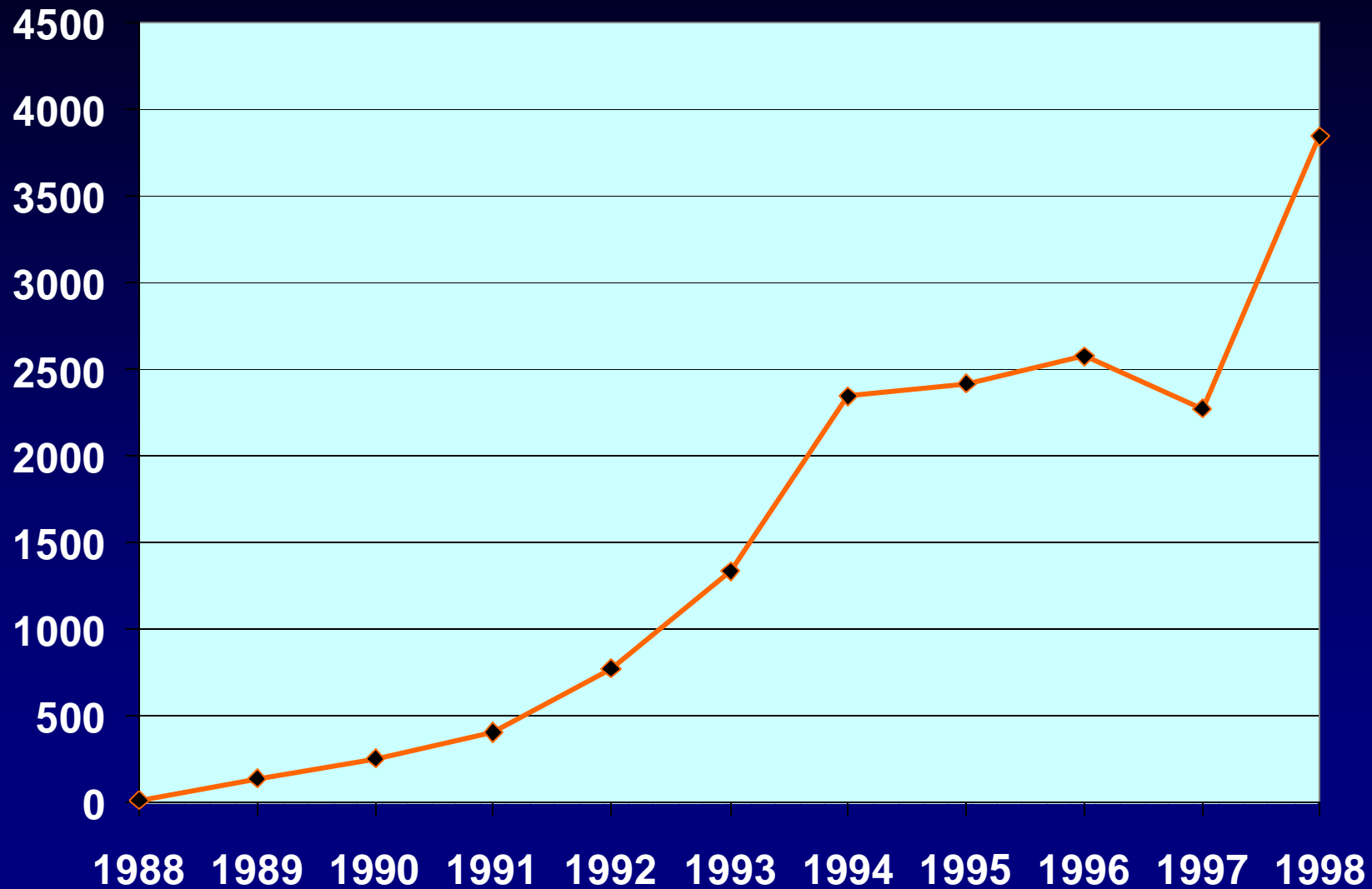
Computer Security Incident and Vulnerability Trends

Barbara Y. Fraser byf@cert.org

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

Sponsored by the U.S. Department of Defense
© 1999 by Carnegie Mellon University

CERT Incidents 1988-1998



Current Incident Reports

Average of 40 new incidents reported each day

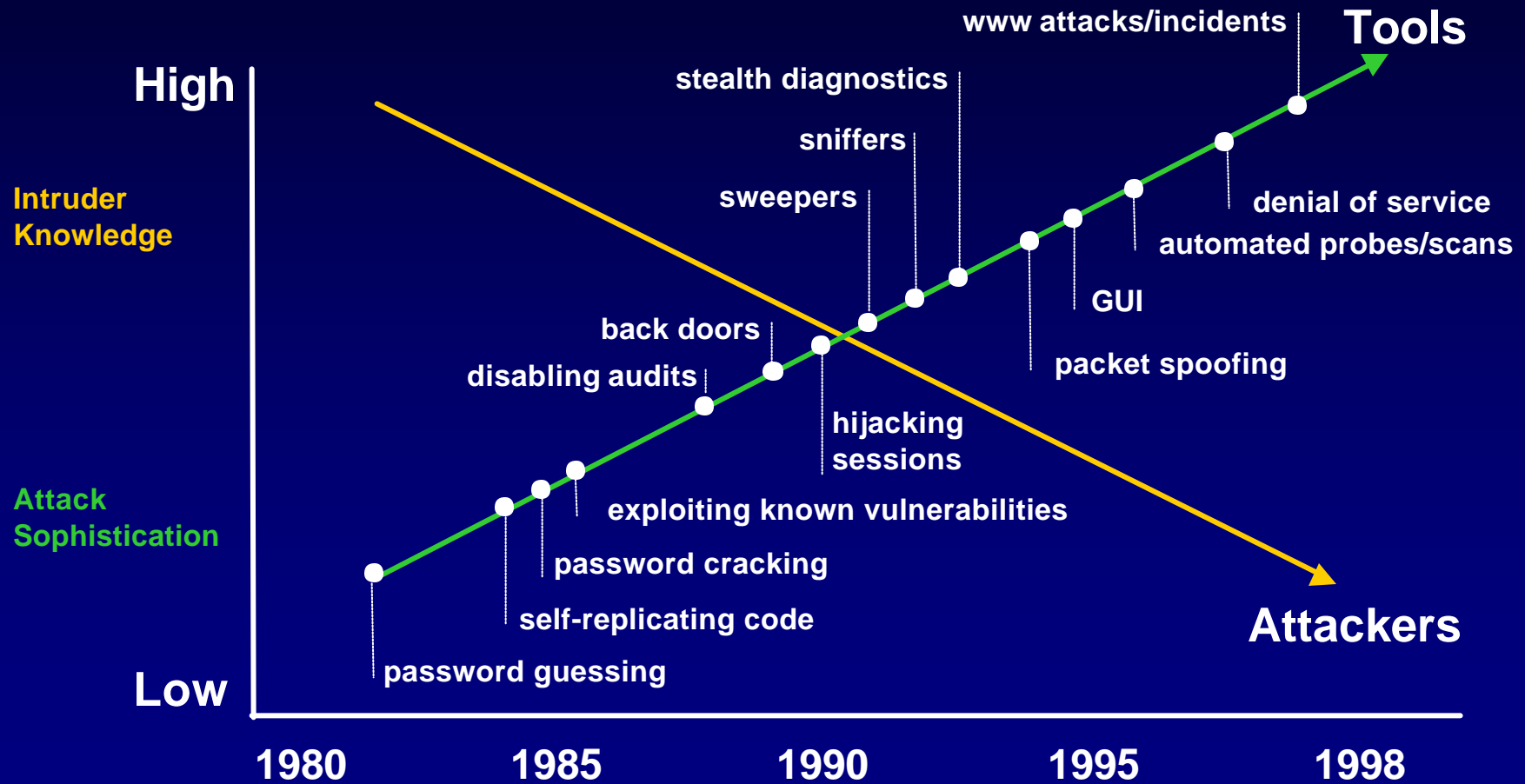
Increased number of reports from individuals

Increased number of virus reports

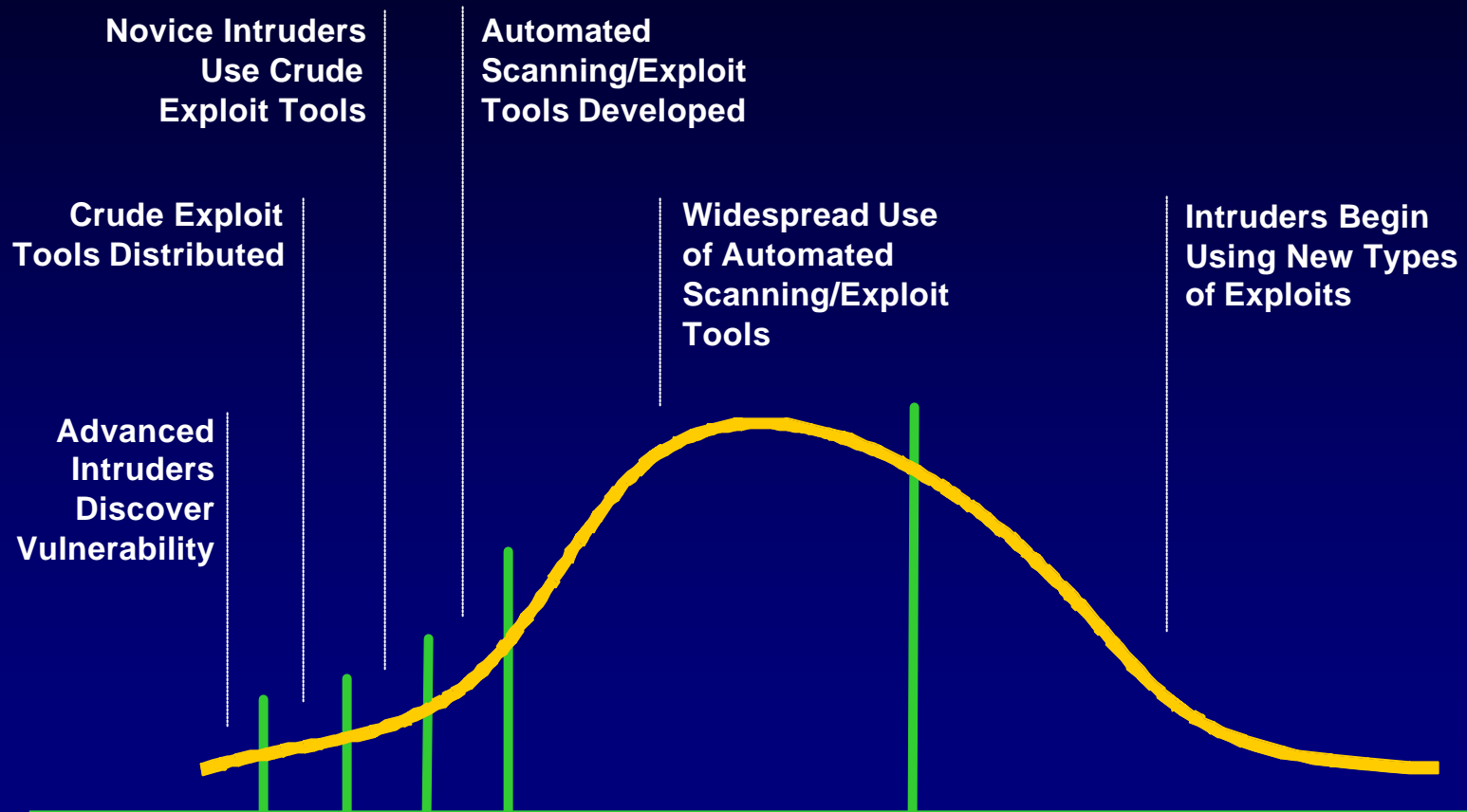
Impacts of intrusions at universities:

- **researchers' data compromised**
- **theses are deleted**
- **web pages are changed**
- **student and administrative data altered**

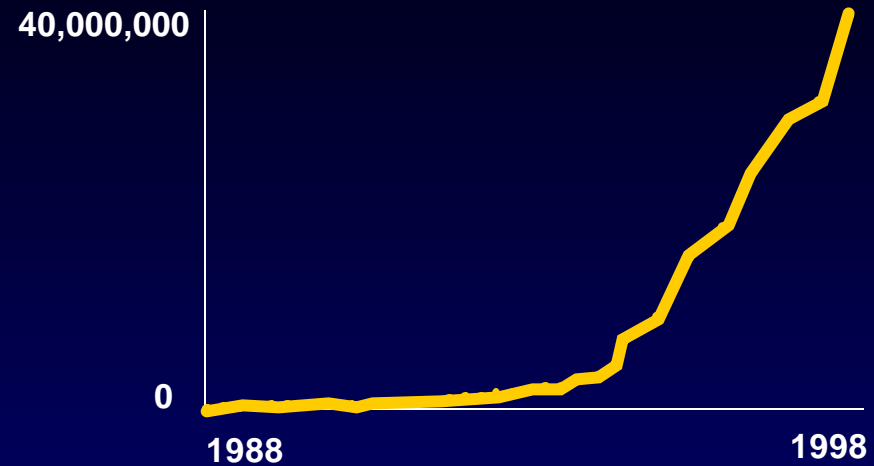
Attack Sophistication vs. Intruder Technical Knowledge



Vulnerability Exploit Cycle

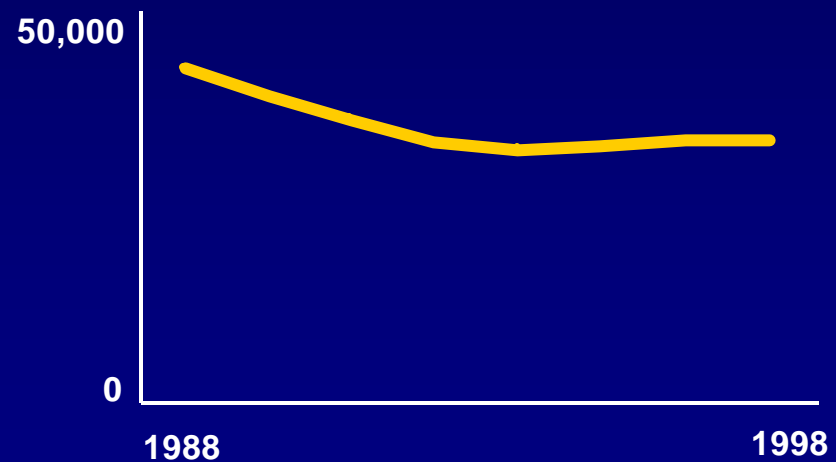


Internet Growth 1988-1998



Source: Internet Domain Survey by Network Wizards, WWW.ww.com/zone

BS and MS Degrees in Computer and Information Sciences 1988-1998



Source: Digest of Education Statistics 1997, US Office of Educational Research and Improvement, Washington DC, publisher: US Superintendent of Document, 1997

Intruder Trends

Leveraging use of currently available technologies

Creating easy-to-use exploitation scripts

Developing increasingly sophisticated toolkits

Transferring expertise to novices

Scanning large blocks of addresses

Increasing impact by targeting the infrastructure

Melissa and the Future

CERT/CC handled over 300 reported incidents affecting well over 100,000 computers

Estimates of tens of millions of hosts affected world-wide

It easily could have been worse

Office2000 makes it unnecessary to have the user open an attachment

- **Outlook 98 supports viewing HTML which could include Vbscript or other languages**

All the components are available to launch a really nasty Internet-wide attack

Vulnerability Trends

Flaws can be found without source

- **common: system call trace**
- **new: subroutine call trace**
- **protocols can be examined for vulnerabilities**
- **program instabilities (buffer overflow, etc.)**

Patches now being released via Internet

Still untested — product liability

Competitive pressures resulting in decrease in vendor product development and testing time

Good news — the public & vendors becoming more security conscious

Recurring Software Development Problems

Not applying lessons learned

Old bugs still present in new versions

Known problems are not getting fixed

Programmers not aware of proper use of algorithms and tools

- **buffer overflows**
- **timing windows**
- **trusting untrustworthy information**
- **principle of least privilege**

The Community Must:

Assume hostile environment

Identify security risks

Design with security in mind

Budget for increased cost of “Defensive Programming”

Strain on System Administrators

Engineering for ease of use has not been matched by engineering for ease of secure administration

- **ease of use and increased utility are driving a dramatic explosion in use**
- **system administration and security administration are more difficult than a decade ago**
- **this growing gap brings increased vulnerability**

The demand for skilled system administrators far exceeds the supply

System and Network Administrators are Unprepared

Behind in the installation of patches and work-arounds

Too many services supported by common host

Insufficient training

Poor perimeter security

Poor infrastructure management

Low use of encryption

Reliance on standard plain text passwords

Incomplete security policies

No incident response team or procedures

What Can You Do?

Improve security at your site:

- **reduce use of clear text passwords**
- **shutdown students' easy access to network traffic**
- **configure network connectivity to provide accountability**
- **protect proprietary data on your systems, such as vendor source code**
- **provide sufficient resources so that infrastructures can be developed with security in mind**
- **maintain infrastructures through timely application of patches and other security fixes**

What Can You Do?

Ensure coordination between various departments

Plan in advance for security incidents

- **identify technical resources**
- **address PR, legal, and law enforcement roles**

Share solutions such as the tools for automatic installation of patches

Issues Heard during Earlier Presentations

Where does the security group live?

Staffing for fixing security problems

Reducing use of clear text passwords

Installing security patches

Private campus networks

Communications with other locations

New applications being developed that still use clear text passwords

Improving security practices of IT staff

CERT Contact Information

24-hour hotline:



+1 412 268 7090

CERT personnel answer 8:30 a.m. — 5:00 p.m. EST(GMT-5) / EDT(GMT-4), and are on call for emergencies during other hours.

Fax:



+1 412 268 6989

Anonymous FTP archive:
Web site:

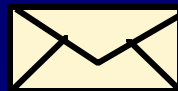
<ftp://info.cert.org/pub/>
<http://www.cert.org/>

Electronic mail:



cert@cert.org

US mail:



CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh PA 15213-3890
USA