

The Security of Cyber-Infrastructure

Anita Jones
University of Virginia

Viet Nam Education Foundation
August, 2004

Information Infrastructures

Processes of society & business
are integrally supported by information systems

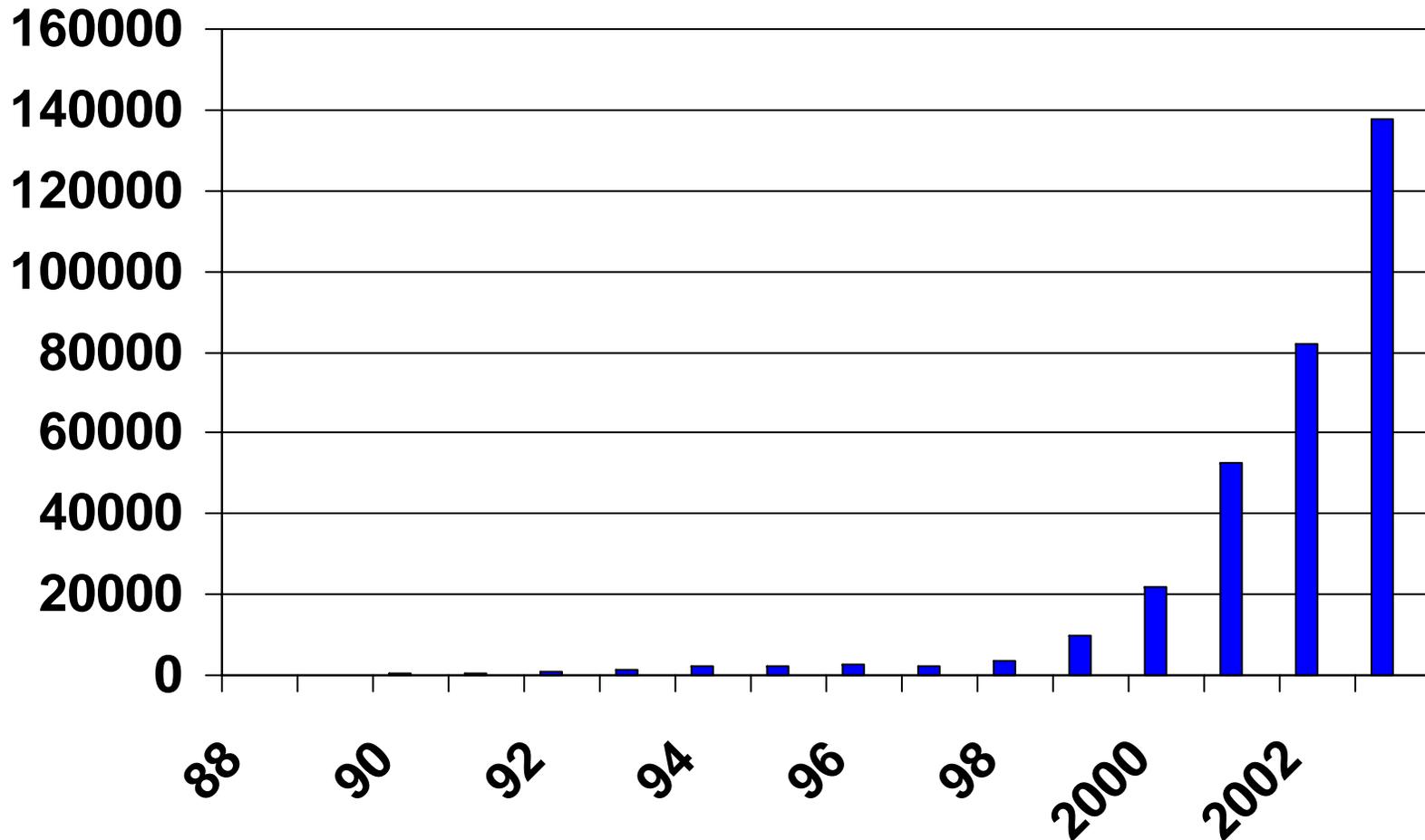
Weak link: they are not secure!

- How did we get here?
- What are the shortfalls?
- How can we improve security?

Just how Vulnerable???

- We don't know!
 - Cyber attacks can "kill" infrastructure
 - Societal processes integrally depend on cyber infrastructure
 - Cyber attacks can debilitate - e.g. military or emergency responders
- Can a cataclysmic attack hurt society?
- Basically, we don't know how vulnerable we are!

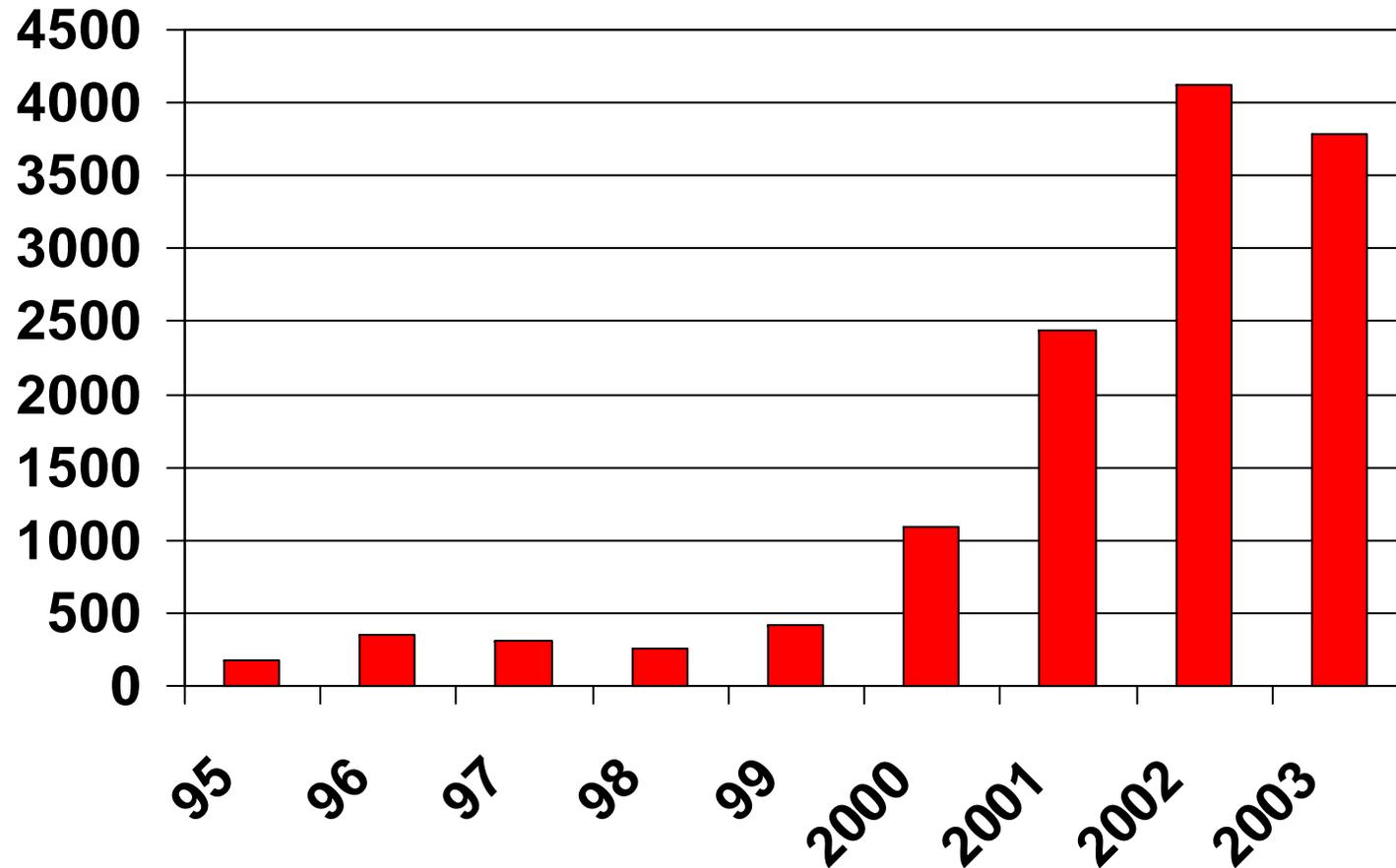
Reported Internet Security Incidents



Number of incidents growing dramatically with net size

Source: CERT, 2004

Different Internet Vulnerabilities



New vulnerabilities introduced annually - too large

Source: CERT, 2004

Sequence of Worms & Viruses

Date	Worm/Virus
1999	Melissa virus, trinoo, Tribe Flood Network Stacheldraht DDOS tool – on net
2000	yahoo, ebay, etc high profile site attacks Loveletter – email attachment attack
2001	Anna Kournikova, Code Red, Code Red II, Nimda
2002	Slapper
2003	SoBig
2004	MyDoom

... and buffer overflow vulnerabilities “everywhere”

Who are the Perpetrators?

- U. S. FBI study of security incidents
 - 643 organizations
 - Attacks by 30 outsiders – average loss of \$35,000
 - Attacks by 60 insiders – average loss of \$1.8M
- **Attacks come from the inside:** 70%, on average; not the viruses & worms that you hear about
- **Inside attacks are more costly**
- Trend: Authorized outsiders being given access to internal nets: subcontractors, customers, international partners

Let's analyze more carefully ...
and ask how got here

What is Cyber Security?

Enforcement of **policies** of how information is treated:

- **confidentiality** - protect against wrongful access
- **authentication** - assured identification of accessor
- **integrity** - only authorized creation or modification of information
- **non-repudiation** - action (i.e. use of digital signature) cannot be denied
- **availability** - ensure information access

Tailor policies to organizational needs

Kinds of Attacks

- **fabrication** - destroys authenticity of source
- **modification** - destroys integrity of information
- **interception** - of information (traffic), breaches confidentiality
- **interruption** - of service
 - Computer time, bandwidth on network, and memory available to store information

We don't distinguish between attack on one computer, or on network

Prevailing Model of Security

Perimeter Defense

- Designed in the 1960s when
 - Mainframes were locked in a machine room, and
 - Users hand-carried jobs to the computer room
- Kernel in the operating system controls “all”
- Kernel is a gatekeeper, adjudicating between users
- Once the perimeter is breached.....

Perimeter defense* is the “state of the practice”

* Analogous to castle walls and the Maginot Line

Prevailing Language of Security

- Password, key
- Insider --- outsider
- Firewall, gateway, DMZ
- Intruder, penetrator
- Intrusion detection systems
- Access control

The language we use “**assumes**”
the notion of a perimeter

Implications - Current State

- Perimeter defense model - dominant paradigm
- Security policies are generic; not tailored to application
- Fails to address "insider" threat
- Monoculture - IBM compatibles' software; one successful attack can affect many systems
- Software development methodology weak
 - Hacker needs one bug; defender protects against all
 - NRL study of security flaws - half (22 of 50) exploited specifications for correct behavior

State of Practice: Monitor & Patch

System administrators.....

- Define generic security policies
- Exercise continual configuration control (hardware & software)
- Use available tools: firewalls & intrusion detection software
- Assure authentication, e.g. enforce password quality/freshness
- Track vulnerabilities; make software fixes as they are published
- Monitor & log continually; audit procedures periodically
- Red team occasionally

Poor Engineering Practice!



**Always
Work on
Important
Problems**

-Thomas Jefferson

**Founder, University
of Virginia**

How?

Are there alternatives to
“perimeter defense”?

New models?

One Bright Spot - Cryptography

- Two types:
 - **Symmetric (secret) key crypto** - for block data
 - **Public key crypto** - to exchange keys in secret
- End to end - **empowers**:
 - Individual
 - Application - not the network, or the "system"

NOT a perimeter mechanism!

1 - Immune System Analog

Detect when an application goes awry

- **Imbue software with an “immune system”**
 - **Detect problems locally - in application**
 - **No perimeter; anti-bodies throughout**
 - **Do something about it, if only to sound an alert**

2 - Active Defense of Networks

- **Definition:** Active Defense - “employ limited, offensive counter actions to deny contested position to the attacker”
- Today, network defense is passive
- All costs accrue to the victim!
- Make the sender pay - i.e. “compute a value” as “payment” for message delivery
 - Costly to compute, but cheap to verify - e.g. factor a number

3 - Use Physical Properties

- If the information system is integrated into its physical environment, use corroborating physical state information to detect attacks
- Physical infrastructures
- Embedded sensor/actuator networks
 - Building
 - Perimeter of military air base
 - Assembly line
- E.g. Use sensors to check health of assembly line

Possible New Approaches

1. Mimic the human immune systems in software
2. Actively defend networks
3. Use physical properties - embedded
 - network can rely on known physical states

New alternatives to perimeter defense.

Computer science researchers need to create new security solutions.

Thank you

Questions?