Secure Software Development Introduction

Objectives

- Comprehend the magnitude of the security problem
- Compare and Contrast Secure Software Development, Network Security, and Data Security
- Compare and contrast bugs and flaws
- Explain the trinity of trouble
- Justify why more code leads to more security bugs

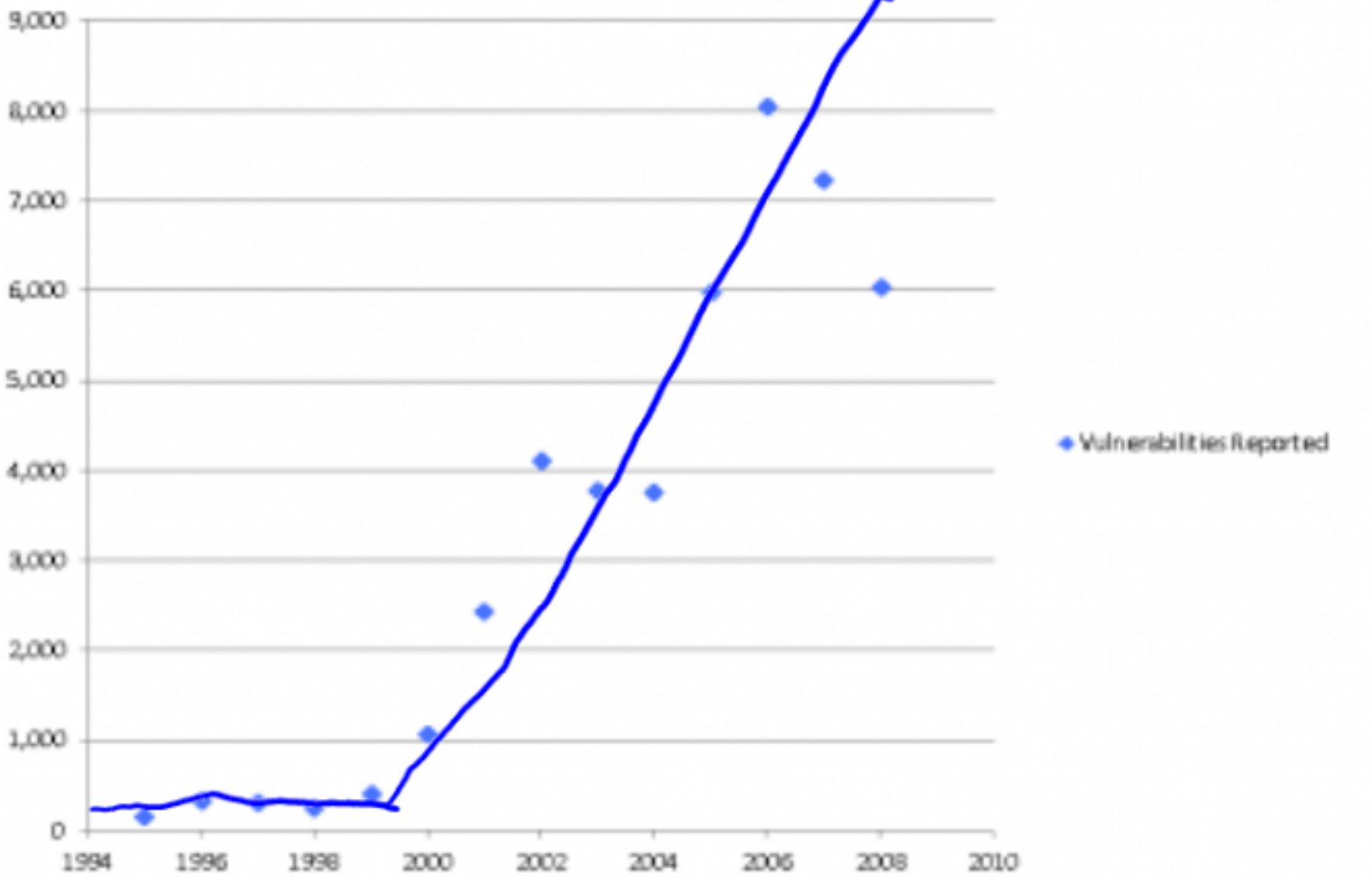
Introduction

- Software Security: Big business
  - $45 billion / year
- 532% growth in incidents, 2000-2003
- 43% of companies indicate a growth in cyber crime attacks against their sites

Attack from outside

MSOE

CERT Vulnerabilities: 1995-2008



Areas of exposure

Security watchdog

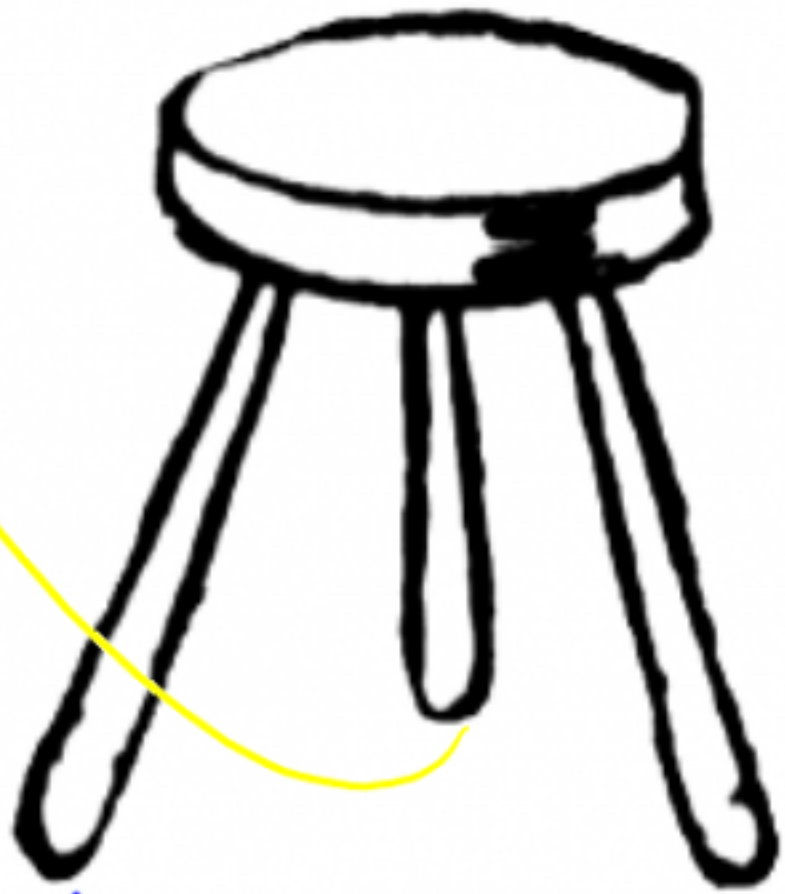
Types of security

21st Century Childhood Pranks.

We do not need physical access to attack a machine.

Types of security

SW Development



Network Security

Information Security
⇒ Encryption

↳ keeping our network up and running

Bugs versus flaws

- Two categories of software security defects
  - Bugs → Simple mistakes made in implementation
    ⇒ Static analysis helps
  - Flaws
    Complex architectural mistakes made when designing the system → reviews & inspections

Microsoft Bob

Microsoft Bob

Microsoft Bob

Microsoft Bob

Microsoft Bob

The trinity of trouble

- Connectivity
- Extensibility
- Complexity

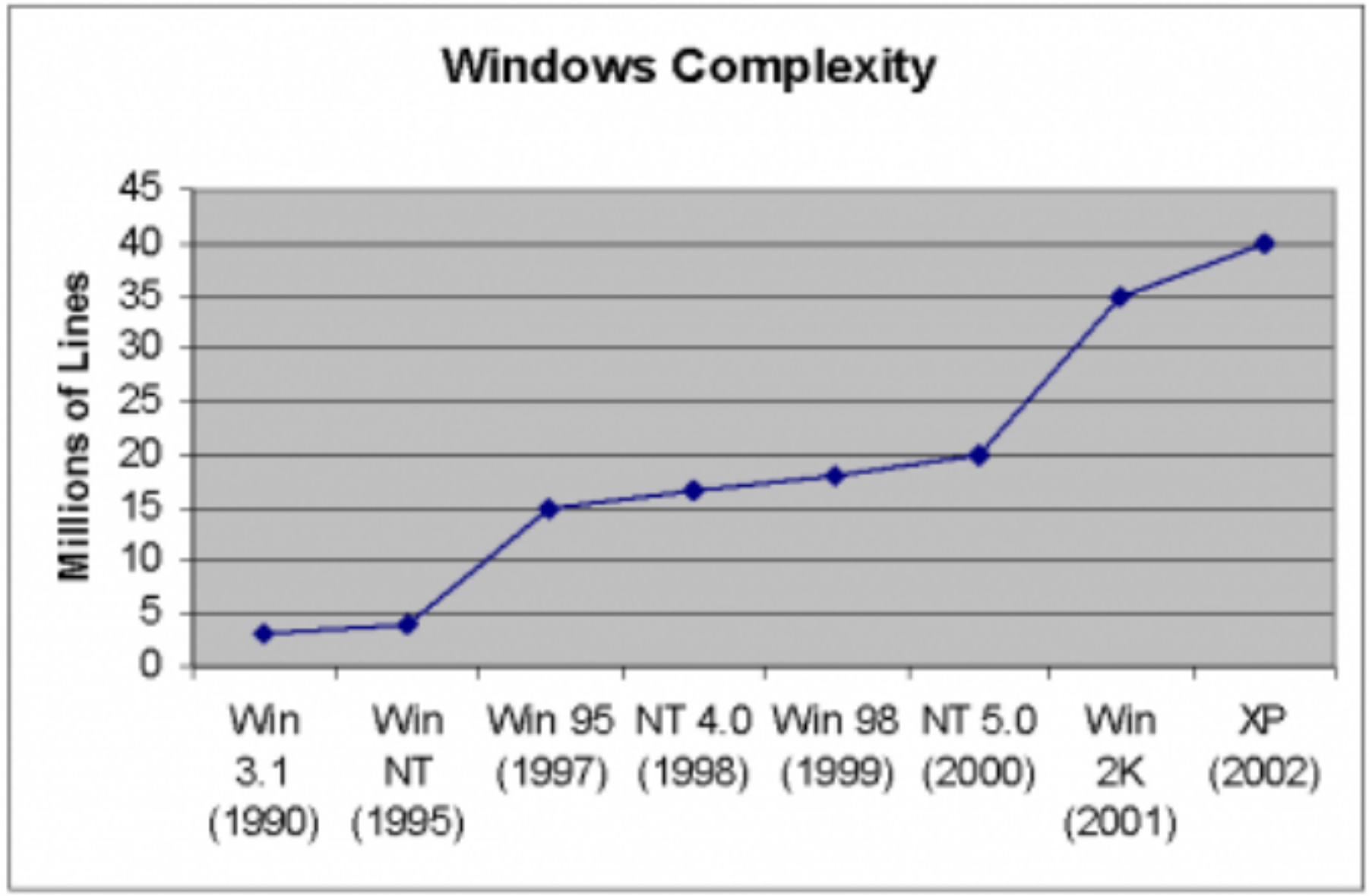
Software Complexity

5-50 bugs per/kloc[8]

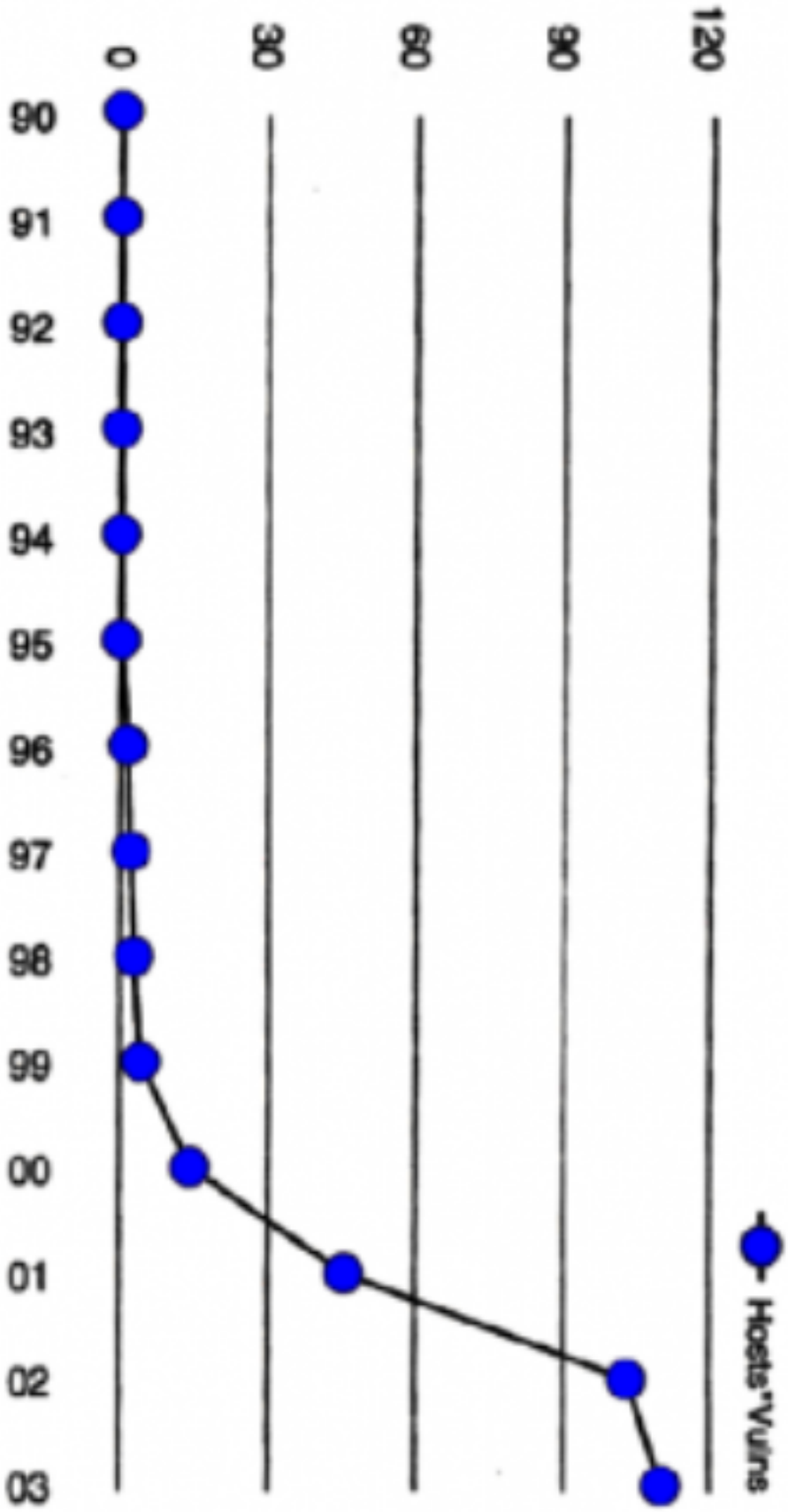
- 5/kloc: rigorous quality assurance testing (QA)
- 50/kloc: typical feature testing

System	Lines of Code
MS Word 95	2 million
MS Windows 3.1	3 million
Boeing 777	7 million
Space Shuttle	10 million
Netscape	17 million
MS Windows XP	40 million
Vista	50 million
Red Hat Fedora	6.7 million (Core) 204.5 million (Entire Distro)

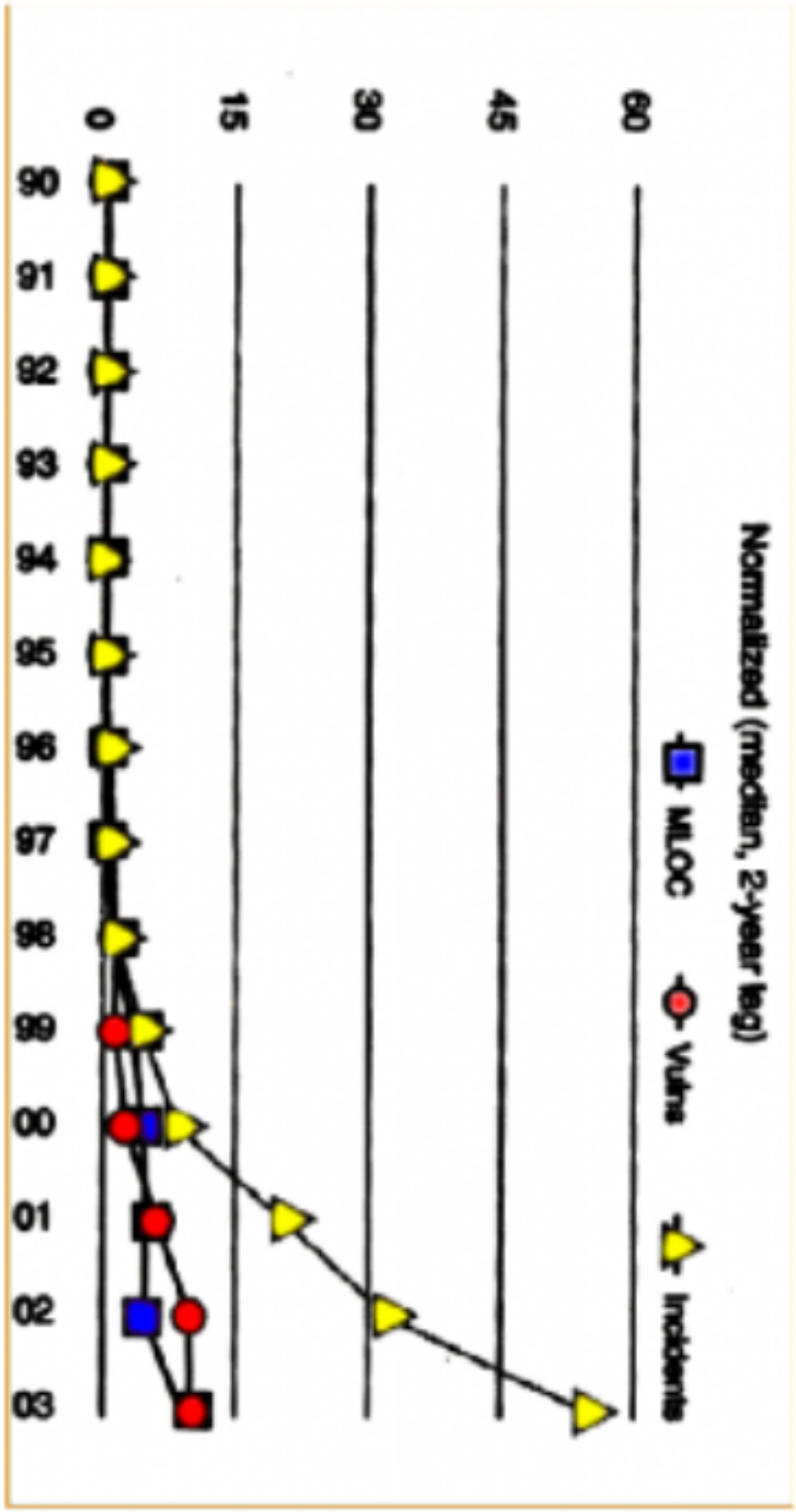
Software Complexity: Windows



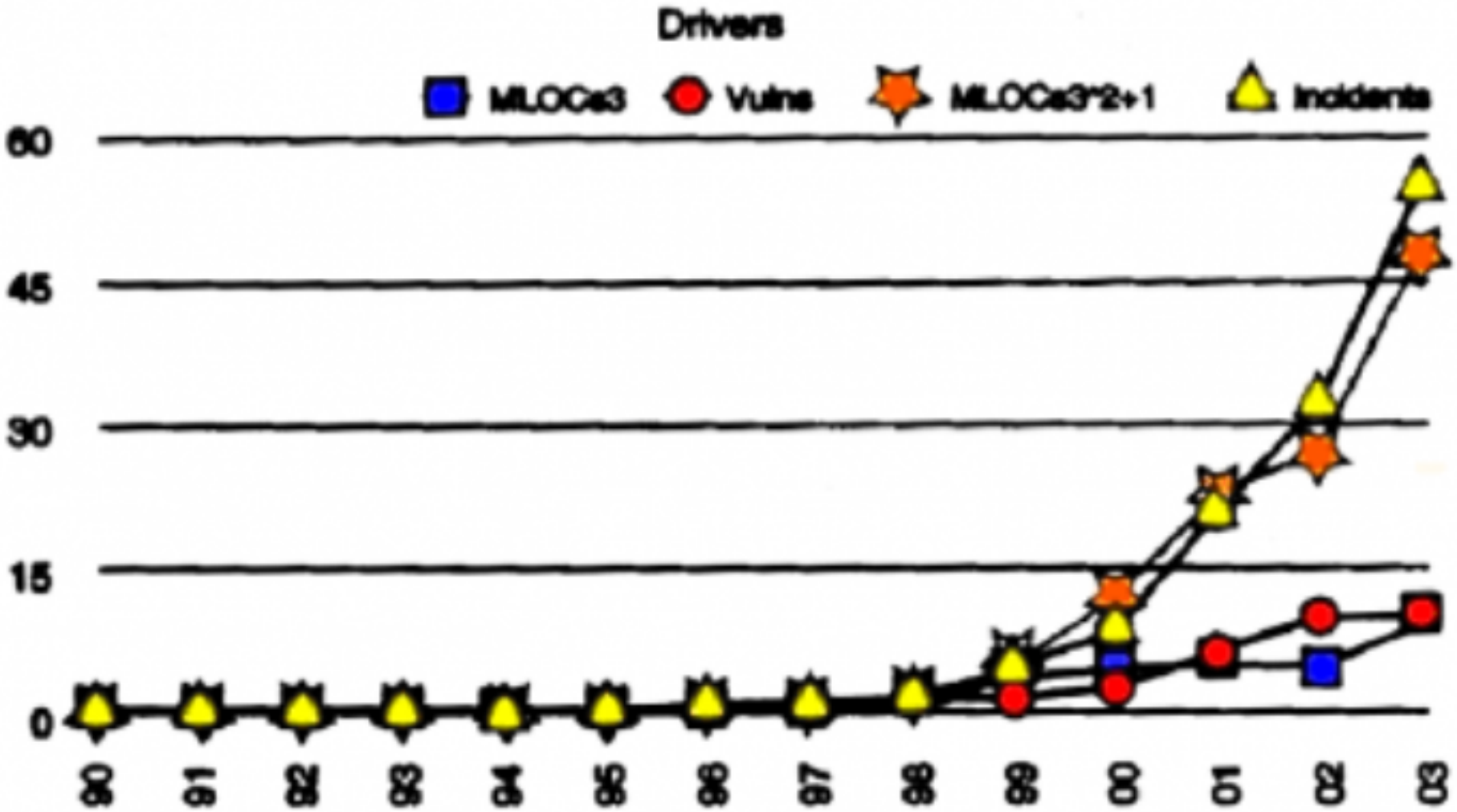
Normalized Number of security vulnerabilities



Normalized MLOC, Vulnerabilities, and incidents



Don't believe me?



Bugs versus flaws again

Bugs	Flaws
Buffer overflow: stack smashing	Method over-riding problems (subclass issues)
Buffer overflow: one-stage attacks	Compartmentalization problems in design
Buffer overflow: string format attacks	Privileged block protection failure (DoPrivilege())
Race conditions: TOCTOU	Error-handling problems (fails open)
Unsafe environment variables	Type safety confusion error
Unsafe system calls (fork(), exec(), system())	Insecure audit log design
Incorrect input validation (black list vs. white list)	Broken or illogical access control (role-based access control [RBAC] over tiers)
	Signing too much code