Secure Software Development

~~Defending Against Denial of Service Attacks and~~ Current + trends

Objectives

- Explain the current trends in software security

Final Exam:

Next Week Thursday

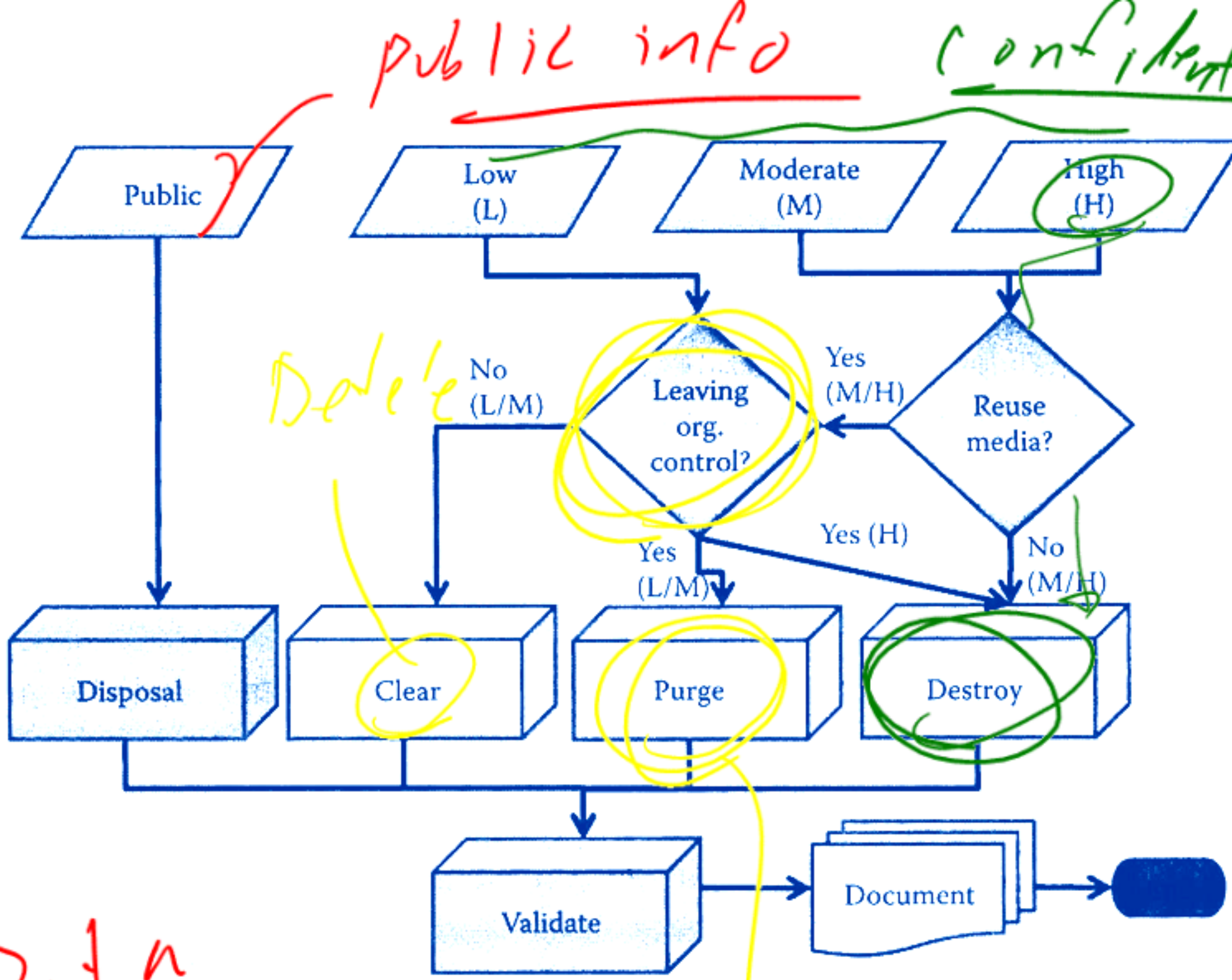
8:00 — 10:00 AM

Room?

Disposal

- Sunsetting criteria
  - When a specific hardware or software product must be disposed
- Reasons:
  - New threats against software are discovered
  - Contractual end of usage
  - Software has reached end of warranty period
  - Software has reached end of product support
  - Software is no longer compatible with hardware
  - Software which can provide same functionality in a more secure fashion is available

Information Disposal and Media Sanitization



Current trends in Software Security

- **Malicious Insiders** -
  - *Rising Threat*
- **Malware** -
  - *Steady Threat*
- **Exploited Vulnerabilities** -
  - *Weakening Threat*
- **Social Engineering** -
  - *Rising Threat*
- **Careless Employees**-
  - *Rising Threat*
- **Reduced Budgets** -
  - *Rising Threat*
- **Remote Workers** -
  - *Steady Threat*
- **Unstable Third Party Providers** -
  - *Strong Rising Threat*
- **Downloaded Software Including Open Source & P2P Files** -
  - *Steady Threat*

Figure 1: Incidents and Events by Category

QUARTERLY TRENDS AND ANALYSIS REPORT
June 16, 2009
Volume 4: Issue 1

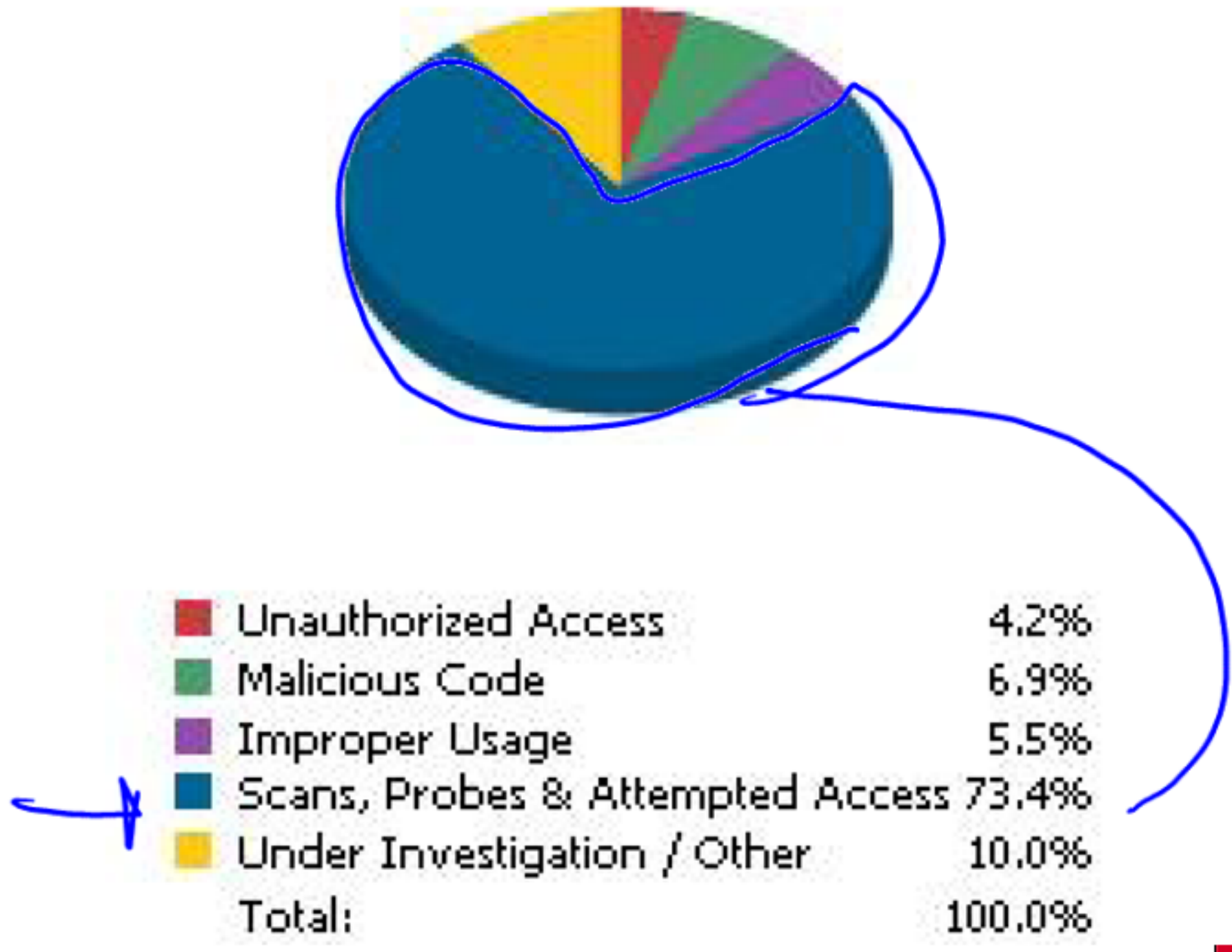
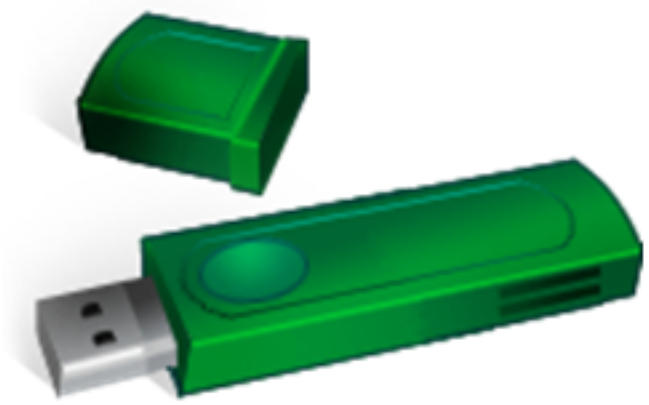


Figure 2: Top Five Incidents vs. All Others

Social Engineering

Proliferation of Malware via removable media



Windows.inf
⇒ Automatically runs programs when you insert media.

⇒ Compact Flash and cameras.

⇒ plug in your camera via USB

MSOE

Detection of spamming sites

More Emphasis on doing things right

More SW Engineering Training

More Security courses being Taught

Master's degree in Information Assurance.

More interest from companies

MSOE

- https://buildsecurityin.us-cert.gov/daisy/bsi/home.html

Build Security In

- Build Security In is a collaborative effort that provides practices, tools, guidelines, rules, principles, and other resources that software developers, architects, and security practitioners can use to build security into software in every phase of its development.

Ideas for labs came from

NIST

http://csrc.nist.gov/groups/SMA/fasp/

- Computer Security Resource Center
  - Created by The E-Government Act [Public Law 107-347] passed by the 107th Congress and signed into law by the President in December 2002
- Work to date includes:
  - ***Provide assistance in using NIST guides to comply with FISMA***
  - ***Provide a specification for minimum security requirements for Federal information and information systems using a standardized, risk-based approach***
  - ***Define minimum information security requirements (management, operational, and technical security controls) for information and information systems in each such category***
  - ***Identify methods for assessing effectiveness of security requirements***
  - ***Bring the security planning process up to date with key standards and guidelines developed by NIST***
  - ***Evaluate security policies and technologies from the private sector and national security systems for potential Federal agency use***
  - ***Solicit recommendations of the Information Security and Privacy Advisory Board on draft standards and guidelines***
  - ***Provide outreach, workshops, and briefings***
  - ***Satisfy annual NIST reporting requirement***

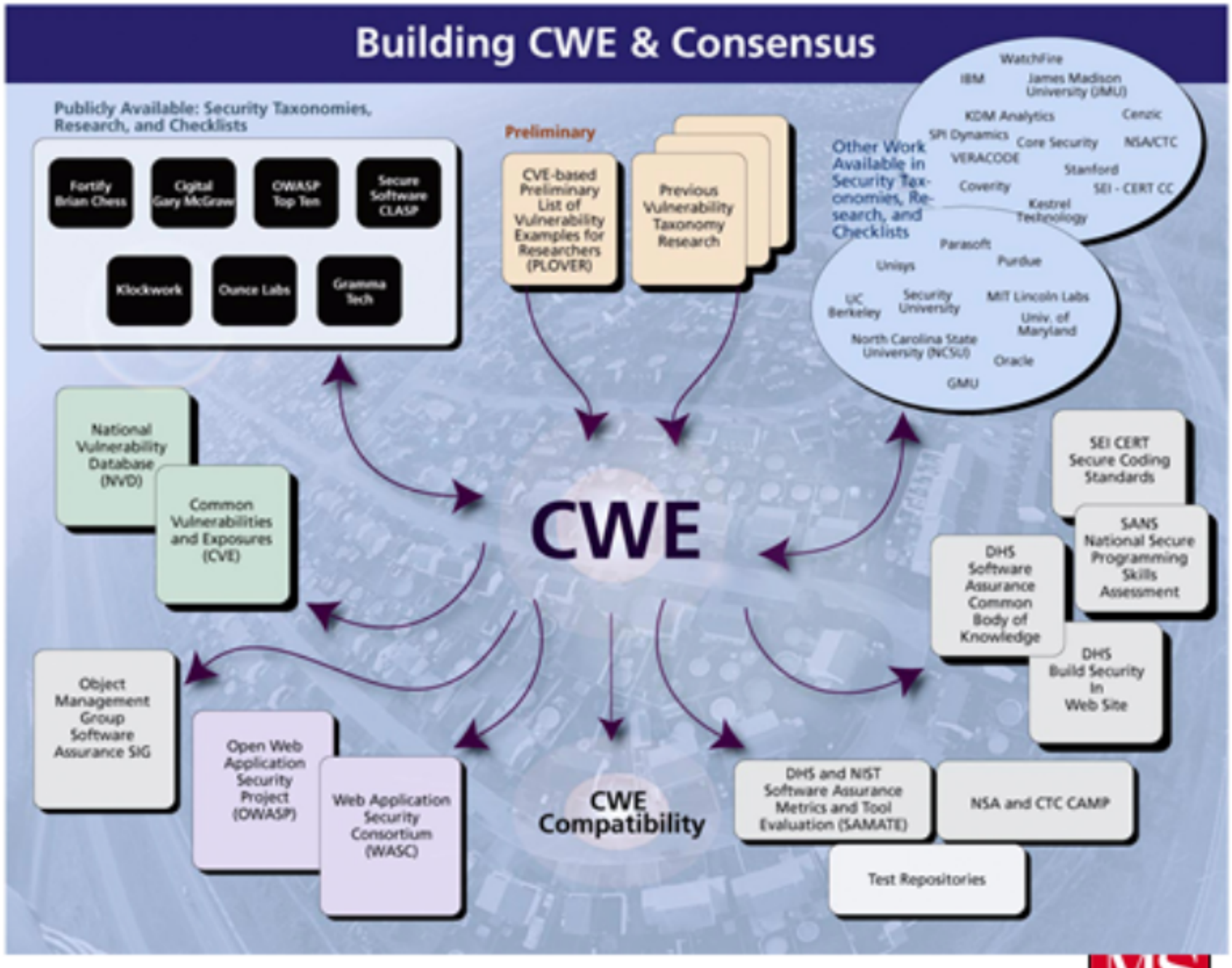
Common Vulnerability and Exposure Dictionary

- http://cve.mitre.org/about/

- Dictionary of common names (i.e., CVE Identifiers) for publicly known information security vulnerabilities,
- Common Configuration Enumeration (CCE™) provides identifiers for security configuration issues and exposures.

→ Taxonomy for Bugs / Flaws

Common Weakness Enumeration



Cloud Computing

Small companies
=> Distinct Advantages
=> Better Security
=> Better Reliability

Large companies
=> Verdict still out.

SaaS => Software as a Service

PaaS => Platforms as a Service