Software Assurance

Session 15
INFM 603

Bug hunting vs. vulnerability spotting

- Bugs are your code not behaving as you designed it.
  - Many can be found by testing for expected behaviour
  - Users report, workaround bugs
  - Maximum damage is normally loss of functionality
- Security vulnerabilities are someone smart making your system doing something unanticipated
  - Difficult to test for in routine way
  - Valuable knowledge to others; may not be reported!
  - Maximum damage: ???

Strategic Thinking

- Decide what to protect
- Analyze vulnerabilities
- Adopt layered defenses

Risks

- Denial of service
- Malicious code
  - Trojan horse
  - Virus
  - Spyware
  - Botnet
- Impersonation
- Interception
  - Man-in-the-middle attack
- Physical compromise
  - Insider threat

Risk Assessment

- Likelihood
  - Preconditions
  - Event

- Severity
  - Direct Costs
  - Reputation
  - Compliance

Scenarios

- Your bank account
- VA laptop
- Zero-day exploit

Mitigation

- Develop knowledge of possible types of security vulnerability (buffer overflow, SQL injection, etc.)
- Brainstorm possible vulnerabilities
- Act as or employ white-hat hacker (“red team”)
- Monitor security updates for packages you use
- Reduce attack surface area
- Learn from the mistakes of others!

Models for software quality assurance

- Models and standards developed for software assurance, after pattern of other quality assurance standards (e.g. ISO 9000)
- Models don't tell you how to write good software
- … and they don't tell you what process to use to build good software
- They provide a yardstick for measuring the quality of your process management
- They measure whether **you** can measure your process

CMMI Maturity Levels

CMMI has five levels of process maturity (with process areas to verify at each level):

1. Initial
2. Managed (e.g. Measurement and Analysis)
3. Defined (e.g. Organizational Process Focus)
4. Quantitatively Managed (e.g. Quantitative Project Management)
5. Optimizing (e.g. Causal Analysis and Resolution)

ISO 15504

ISO 15504 has six capability levels (each practice develops through these levels):

1. Not performed
2. Performed informally
3. Planned and tracked
4. Well-defined
5. Quantitatively controlled
6. Continuously improved

Qualitative, Quantitative, Improved

Both CMMI and ISO 15504 embed the same sequence:

1. Qualitative management (e.g. process for code reviews, testing, etc.)
2. Quantitative management (metrics of performance)
3. Improvement (change process, check with metrics that improvement in quality results)

Example: MS SDL process

Process: Security Development Lifecycle (SDL)

Metric: Bug count (critical and serious, within year of release), on product versions before and after adoption of SDL.

Result:

Product	Pre-SDL	Post-SDL
Windows 2000/2003	62	24
SQL Server 2000	16	3
Exchange Server 2000	8	2