Introduction to Software Security

Laurie Williams
lawilli3@ncsu.edu

John Slankas
jbslanka@ncsu.edu

http://www.isdecisions.com/products/userlock/benefits.htm

HBO hackers release Game of Thrones leak and ransom note

A hacking group claim to have 1.5 terabytes of data from HBO, including scripts, unaired episodes of top shows an

MASSIVE BUG MAY HAVE LEAKED USER DATA FROM MILLIONS OF SITES. SO … CHANGE YOUR PASSWORDS

WannaCry Ransomware

Agenda

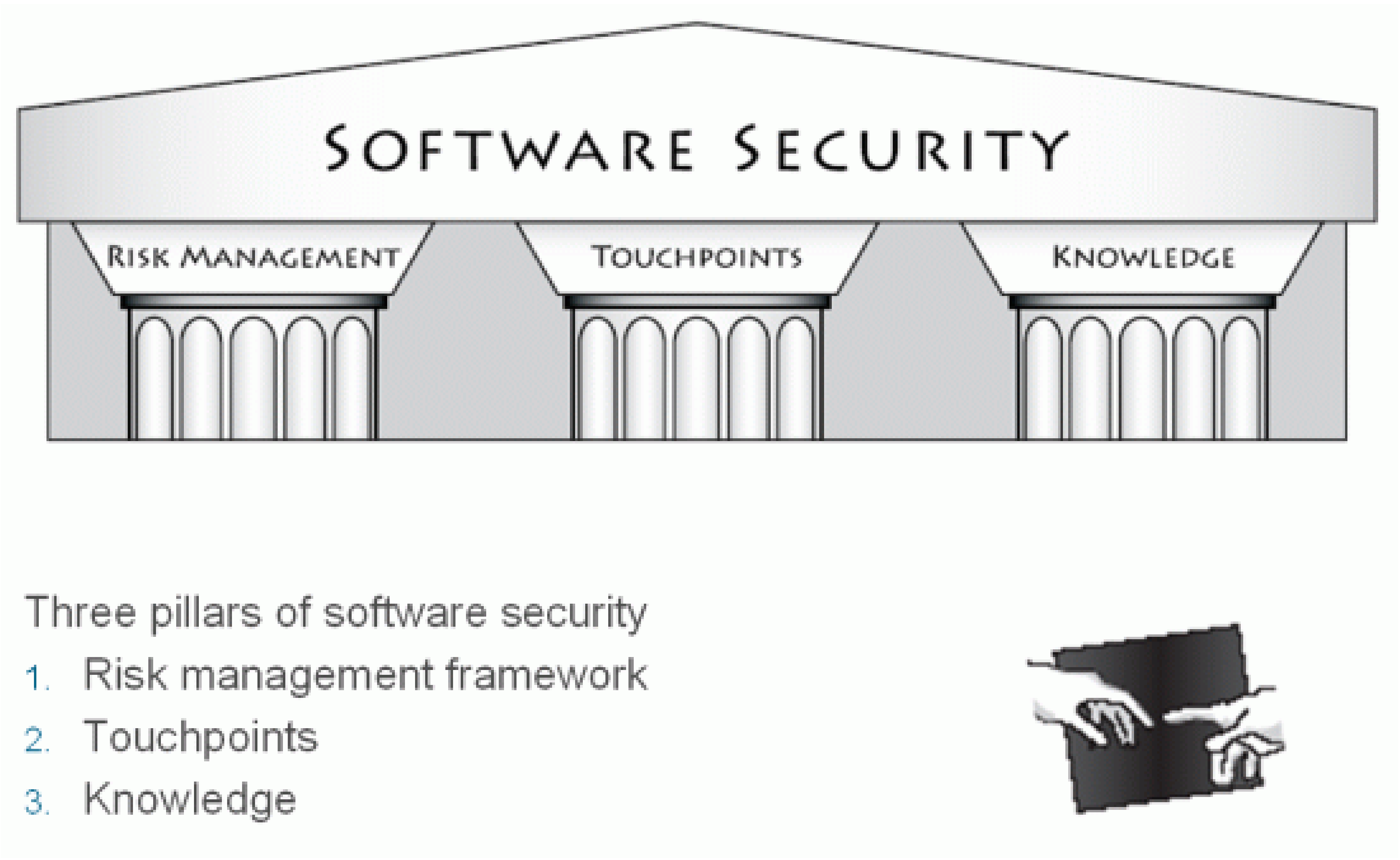
- What’s the course about
- Syllabus

Security Concepts

Confidentiality	Degree to which the "data is disclosed only as intended"
Integrity	Degree to which a system or component guards against improper modification or destruction of computer programs or data."
Availability	Degree to which a system or component is operational and accessible when required for use."
Identification & Authentication	Need to establish that "a claimed identity is valid" for a user, process or device.
Accountability	Degree to which actions affecting software assets "can be traced to the actor responsible for the action"
Privacy	Degree to which an actor can understand and control how their information is used.

Software Security

- The idea of engineering software so that it continues to function correctly under malicious attack
  - Not firewalling vulnerabilities
  - Not reacting through "penetrate and patch"
- Understand and manage software-induced security risks

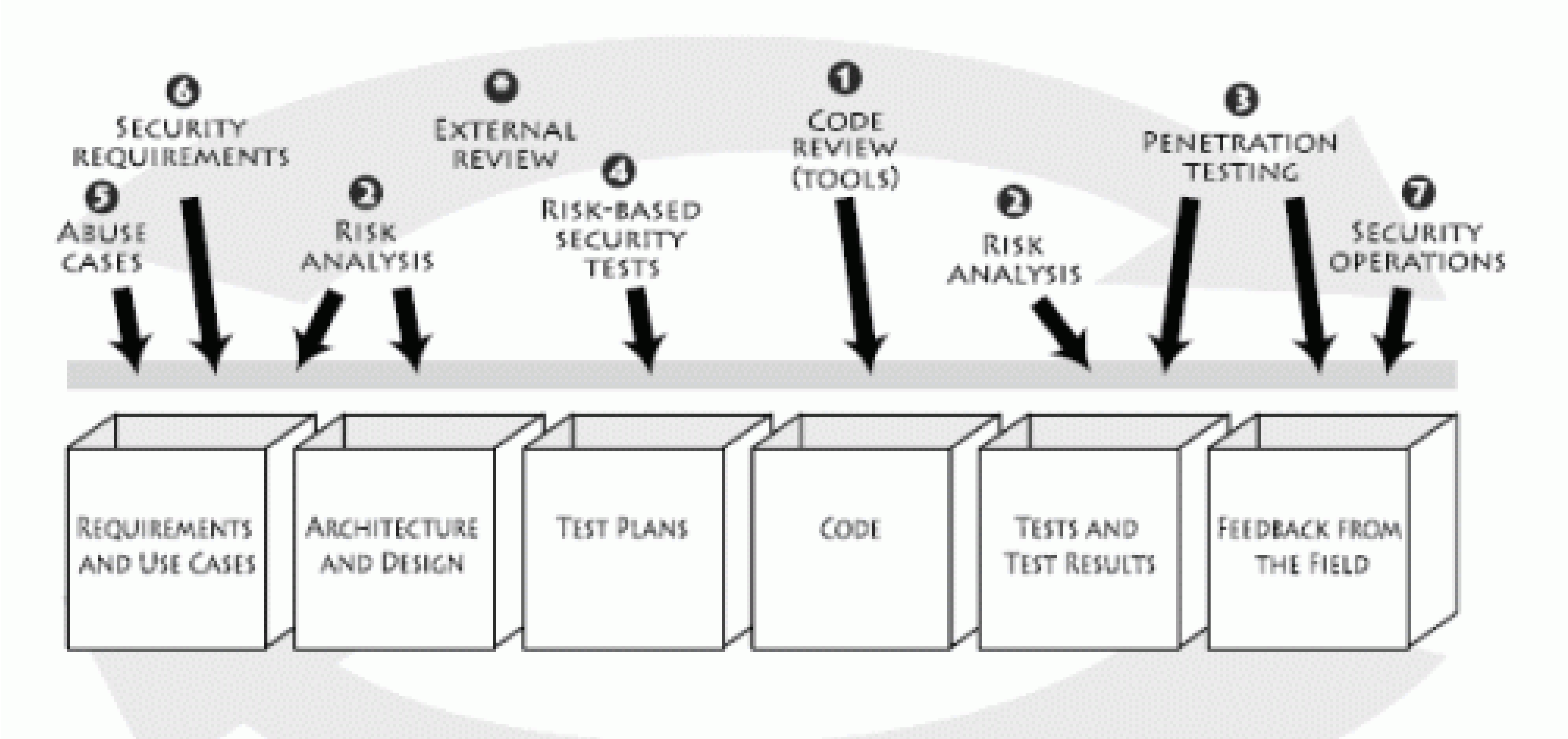


Three pillars of software security

1. Risk management framework
2. Touchpoints
3. Knowledge

http://www.buildsecurityin.com/images/pillars.gif

Software Security Touchpoints



Numbered according to effectiveness and importance or their “natural utility” per Gary McGraw in “Software Security”

http://www.cigital.com/justiceleague/wp-content/uploads/2007/07/touchpoints.gif

Vulnerability

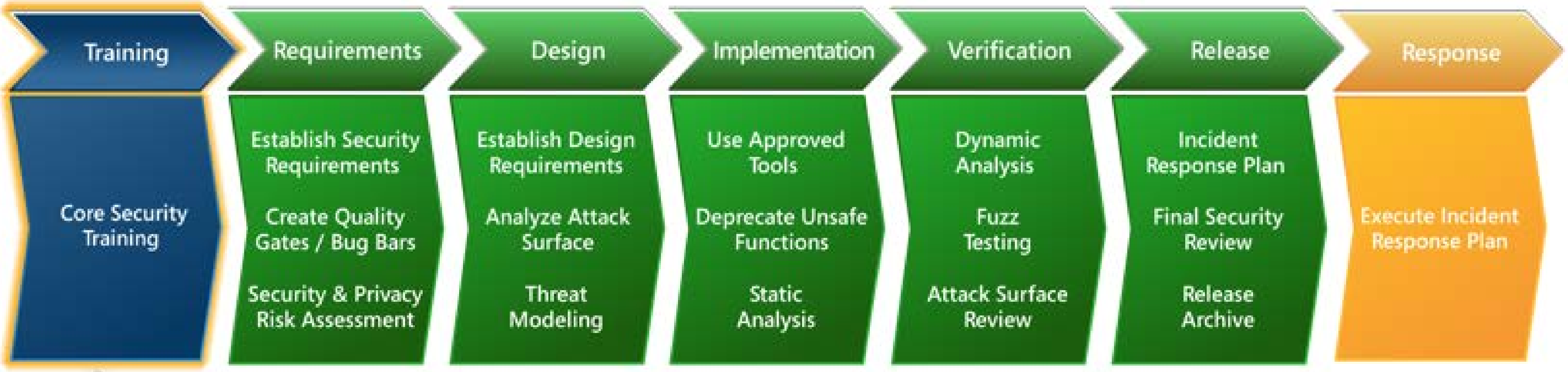
- Informally, a bug with security consequences

- A design flaw or poor coding that may allow an attacker to exploit software for a malicious purpose
  - Non-software equivalent to "lack of shoe-examining at the airport"
  - e.g. allowing easily-guessed passwords (poor coding)
  - e.g. complete lack of passwords when needed (design flaw)

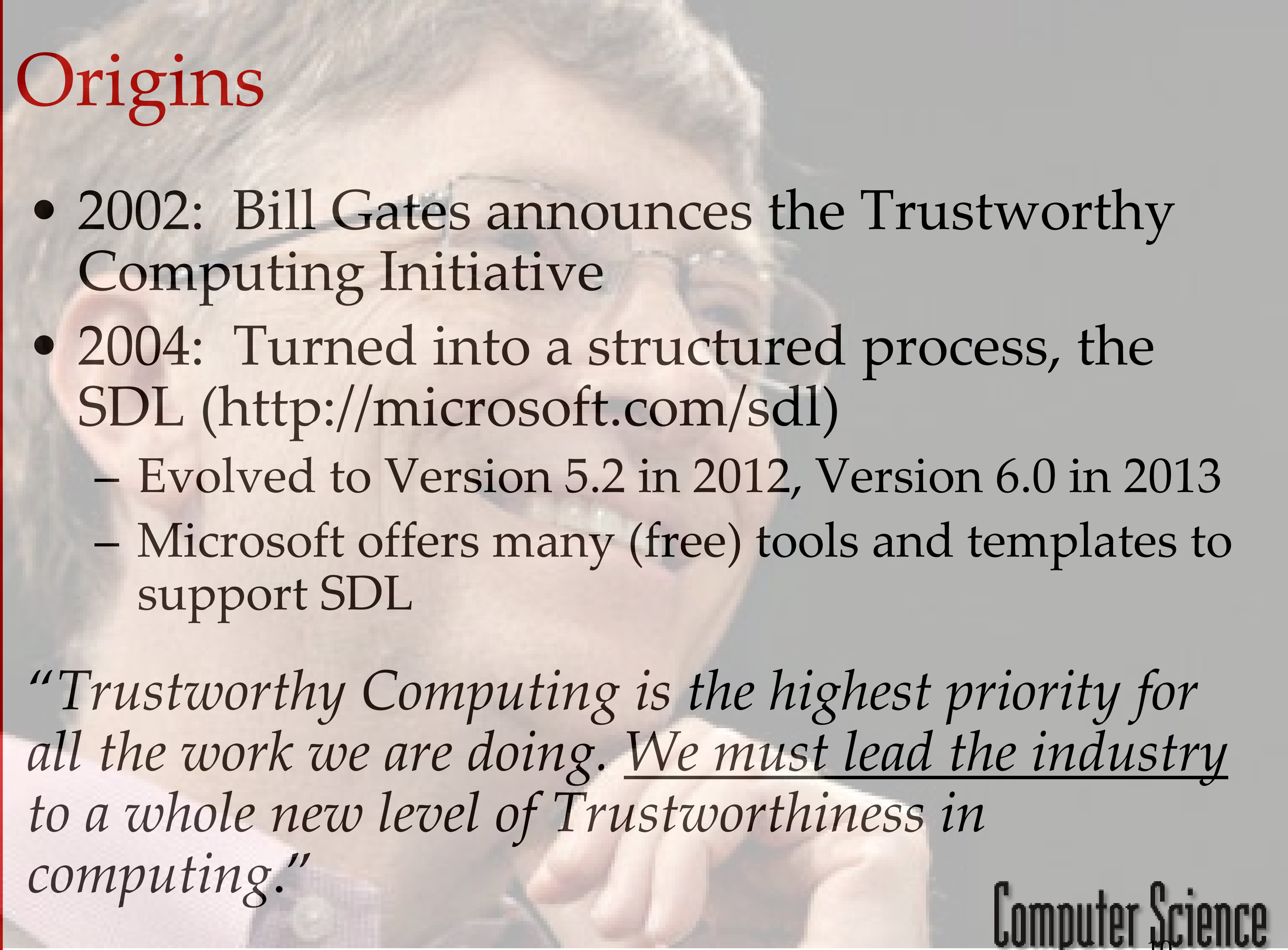
- More formal definition (NIST): "a weakness in … an implementation that could be exploited by a threat source"

Microsoft Security Development Lifecycle (SDL): What is it?

- A software development security assurance process consisting of security practices
- Affects all steps in the lifecycle and the development culture
- Simplified SDL has 17 practices (see figure below)
- Uses a build-security-in/secure-by-design-philosophy



Origins

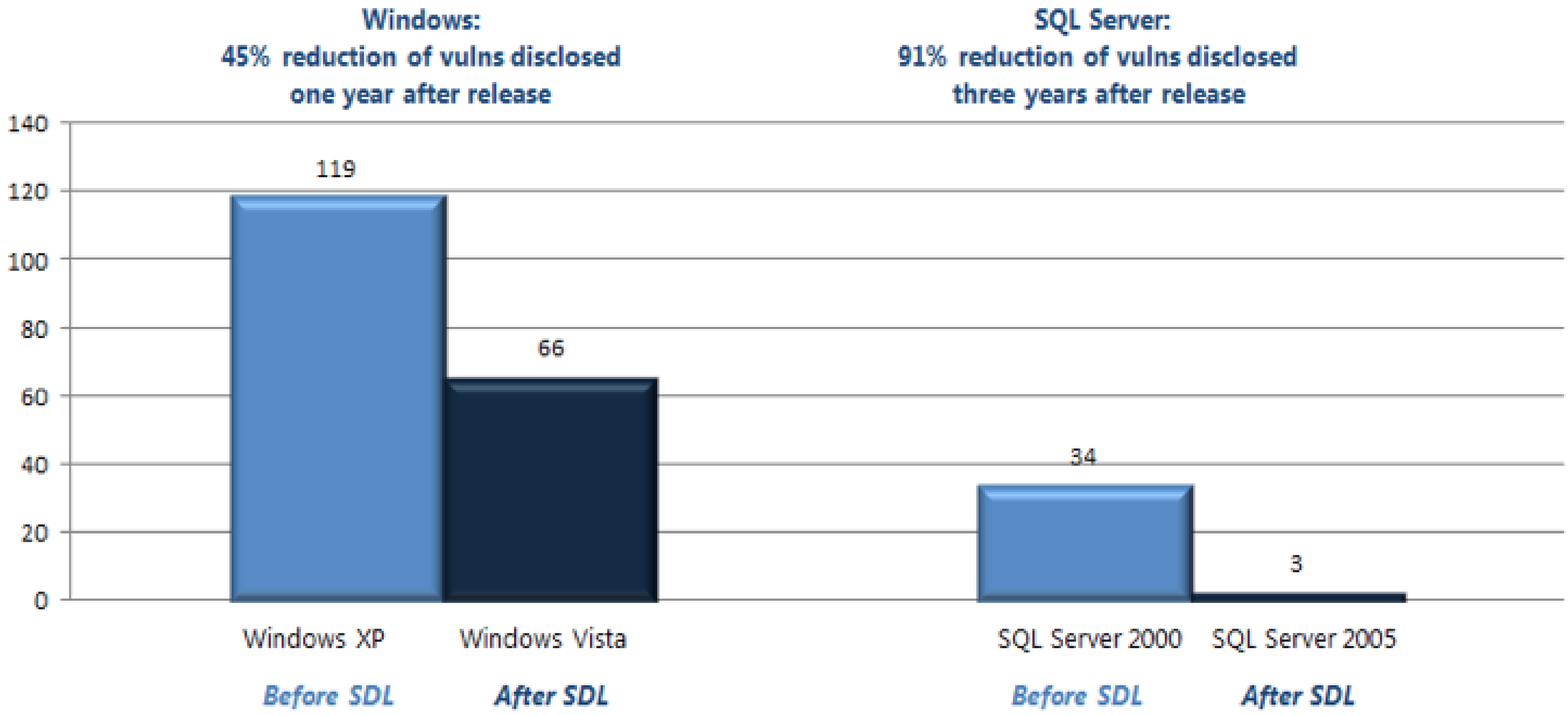


- 2002: Bill Gates announces the Trustworthy Computing Initiative
- 2004: Turned into a structured process, the SDL (http://microsoft.com/sdl)
  - Evolved to Version 5.2 in 2012, Version 6.0 in 2013
  - Microsoft offers many (free) tools and templates to support SDL

"Trustworthy Computing is the highest priority for all the work we are doing. We must lead the industry to a whole new level of Trustworthiness in computing."

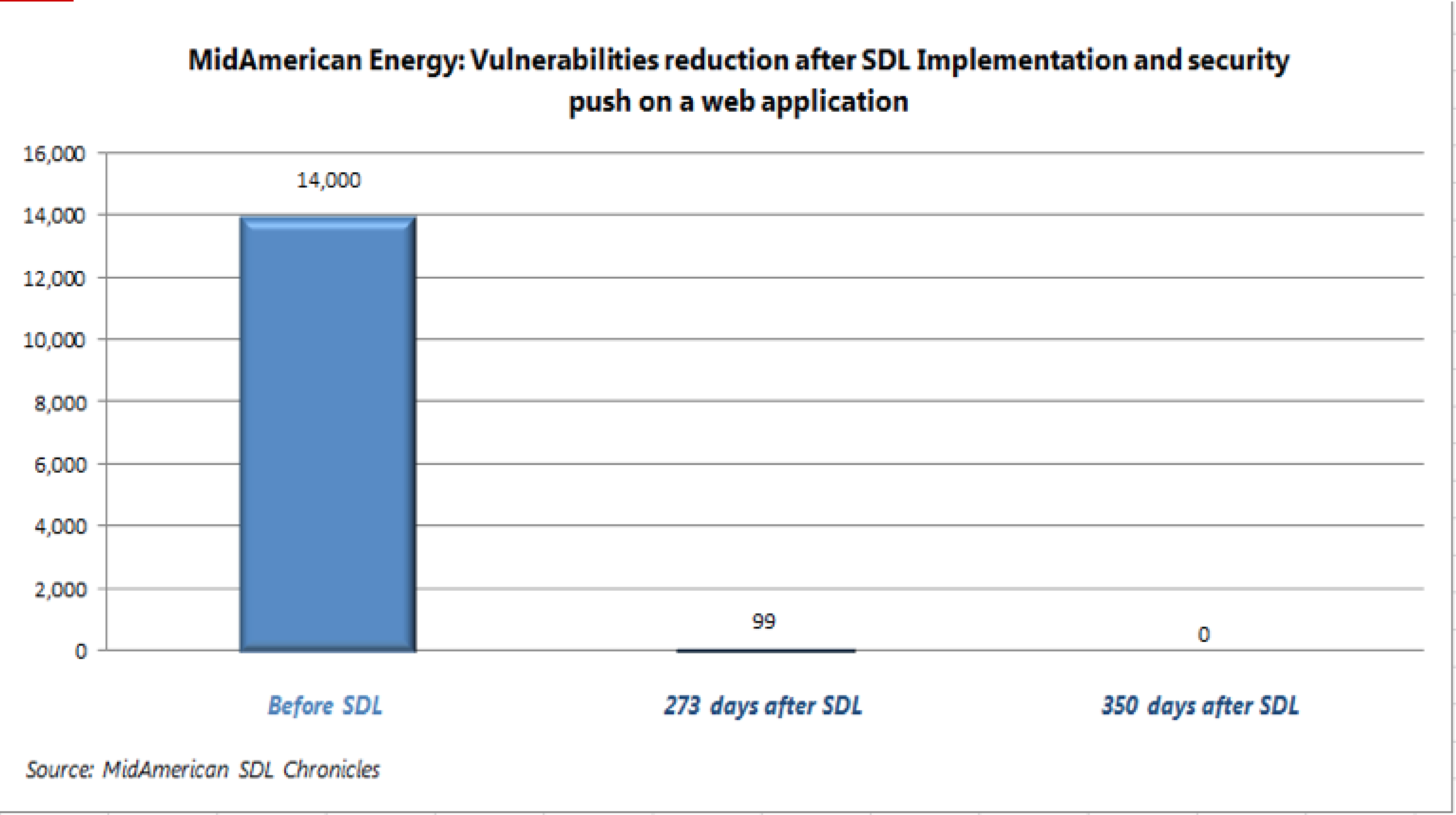
http://www.greatpriceshere.com/2008/06/30/bill-gates-dethroned/

Microsoft products: Vulnerabilities reduction after SDL implemention



Sources: Microsoft Security Blog and Microsoft TechNet Security Blog

http://www.microsoft.com/security/sdl/learn/measurable.aspx



Source: MidAmerican SDL Chronicles

http://www.microsoft.com/security/sdl/learn/measurable.aspx

Agenda

- What's the course about
- Syllabus

Teaching Assistants

Shudi Shao
sshao@ncsu.edu

Shaown Sarker
ssarker@ncsu.edu

Course Progression

- Introduction
- Implementation bugs
- Design Flaws
- Finding vulnerabilities
- Preventing vulnerabilities
- Risk analysis/management

Course content

- Lectures
- In-class Exercises
- Project: Security Review of OpenMRS
- Midterm 1: 18 October
- Midterm 2: 29 November

Grading Distribution

- 25% Project
- 25% Midterm 1 (no unexcused)
- 25% Midterm 2 (no unexcused)
- 10% Attendance & Participation
- 15% Class Exercises, Worksheets, & Quizzes

Group Activity

- Get in groups with at least one laptop
- Search for ZDNet Breaches 2017
- Find one interesting breach
- Search for and find more information:
  - How was the breach done (aka black box … from the attacker's point of view)
  - How much damage (dollars, reputation)
  - Any information of what underlying vulnerabilities were exploited.