SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

*3/4/5 November 2009*

# Achieving Software Assurance in a Global Marketplace

## Panel Briefing

Facilitator: Dan Wolf

Panel Member: **John Weinschenk, CEO of Cenzic**

Homeland Security


- **NOT network security** & **NOT SSL** – hackers get into Websites just like end users – ports 80 and 443 are open
- Website Security **IS** … protecting:
  - Web servers
  - Application servers
  - Web database servers
  - Web based front-ends to legacy applications
  - Web services applications
  - New Web-based technologies
    - AJAX, JAVA, ActiveX, Web 2.0


Homeland Security


80
443


- 75% of cyber attacks & Internet security violations are generated through Internet applications

  Source: Gartner Group

- 87% of Websites are vulnerable to attack

  Source: SearchSecurity – January 2009

- Malware on legitimate Websites has doubled in 6 months

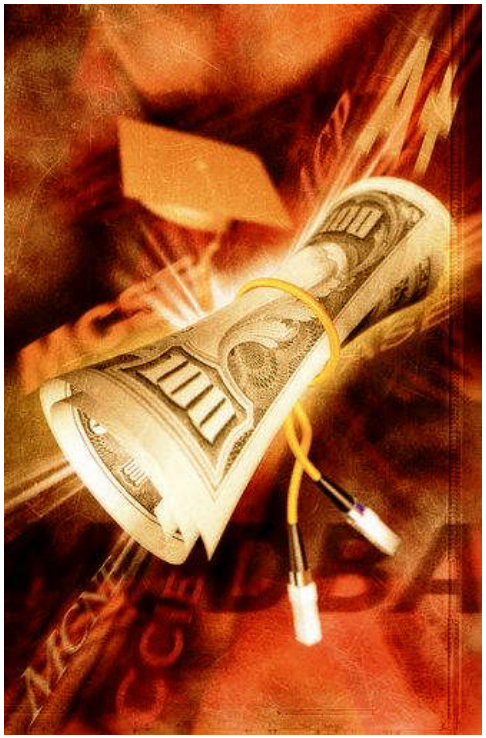
  Source: IT PRO – 2008

- $6.6 Million is the average cost of a data breach

  Source: Ponemon Institute – January 2009

**400+ New Vulnerabilities a Month and Growing**


- **Industry Average is $150-$200/card**
- Cost of Investigation / Inquiries
- Cost of Disclosure
- Cost of Fines and Penalties
- Cost of Increased Fees
- Cost of Litigation
- Cost of Remediation
- Cost to company brand?



Homeland Security



VS

- Does your Website contain as much valuable data as a **7-11** does in cash?

- Or does your Website contain as much valuable data as **Ft. Knox** does in cash?

Homeland Security


# SOFTWARE ASSURANCE FORUM

## BUILDING SECURITY IN

## *Website Security Levels*

| Levels | Types of Testing | Testing Freq | Best Suited For |
|---|---|---|---|
| **Bronze**  | **Basic Testing** (most common 5-10 attacks) | Test once or twice | Anyone with a Website |
| **Silver**  | **More Comprehensive Testing** (Intrusive & non-intrusive attacks) | Test every 6 months | Small e-commerce; Hi Tech; higher risk tolerance |
| **Gold**  | **Most Comprehensive Testing** (Intrusive & Non-intrusive & Application Logic) | Test every 3 - 6 months | Finance; ecommerce sites; low risk tolerance |


SOFTWARE ASSURANCE FORUM

BUILDING SECURITY IN

# *Who Is Cenzic?*

- Cenzic provides software and SaaS products to protect Websites against hacker attacks
- Products
  - **Software** (Cenzic Hailstorm Enterprise ARC & Professional)
  - **SaaS / Cloud delivered** (Cenzic ClickToSecure)
  - **Services** (training courses and assessment methodology)
- Awards
  - **2009 Tomorrow's Technology Today & Top Hot Companies Awards**
  - **2008 SC Magazine's Best Buy Award**

Tomorrow's Technology Today 2009 Info Security Products Guide

Network Products Guide HOT Companies 2009

SC Magazine Best Buy

**"Cenzic emulates a hacker and looks for real-time responses at the browser level. This approach has helped Cenzic provide a very accurate solution with less than 1% false positives."**

**Charles J Kolodgy**

**IDC**


# DoD-DHS-NIST Software Assurance (SwA) Forum

## Achieving SwA in a Global Marketplace

## Panel Briefing - Industry Aspects of SwA

Panelist: C. Warren Axelrod, Ph.D.

Executive Advisor, FSTC

Homeland Security


- Where are we in software assurance?
- Where are we going?
- What challenges do we have in achieving SwA?

Homeland Security


- Significant progress in defining problems for Web apps
- Little being done for legacy systems … biggest slice
- Increasing grasp of threats, exploits and vulnerabilities
- Better understanding of good practices (BSIMM)
- No worthwhile application security metrics
- Inadequate testing, monitoring and reporting of application weaknesses
- Few decision-worthy return-on-investment analyses
- Focus on large organizations - inadequate SMB attention

Homeland Security


- FSTC Software Assurance Initiative
- "Preferred" policy and practices …
  - Security architecture and design
  - Secure System Development Lifecycle
  - Threat modeling
  - Metrics, ROI and risk assessment and management
  - Objective testing lab for financial services industry
- Collaboration among public and private sectors, financial services firms, academic institutions, government, software makers, security products and services vendors

Homeland Security


- Need for greater collaboration among different constituencies
- Need for easier-to-implement approaches - automation
- Need for standards and enforcement - governance
- Need for more convincing justifications for approval by management - metrics, ROI, risk management
- Need for top-down support of software assurance - legal and regulatory compliance, management policy

Homeland Security


- An environment where security trumps features
- A culture that supports secure policy and practices for software development and operational support
- Assignment of responsibility, liability and means of enforcement to appropriate entities
  - Software manufacturers
  - Customer with buying power (government, critical sectors)
  - Infrastructure managers (ISPs, telecoms)
- A measure of assurance that one can trust software implicitly - recognized, practical, meaningful certification

Homeland Security


# Trusted Operational Availability

- DoD requirement for software assurance lifecycle management
- Consistent international standards
- Integration of government/contractor plans early in acquisition lifecycle
- Agility to proactively adapt and enforce policies

L


# Areas of Vulnerability

- Embedded software on LM platforms
- LM enterprise business systems
- End-to-end supply chain systems
- Customer enterprise systems

L


## Increasing Importance

- 2.5M SLOC in F-22
- 2.9M SLOC in H-60 Romeo
- 3.6M SLOC in Littoral Combat Ship
- 8.5M SLOC in F-35, 9 partner nations

L


# Assuring Warfighter Outcomes

- Exploit existing modeling & simulation architecture to provide warfighter training for cyber attacks
- 2010 USMC Mobile Provider Wargame
- Intrusive attack simulation
- NexGen Cyber Innovation & Technology Center

SAFECode
Software Assurance Forum for Excellence in Code
Driving Security and Integrity

# From Controls to Confidence:

## *Software Supply Chain Integrity*

Patrick Arnold
CTO, Trustworthy Computing
Microsoft
3 NOV 2009

# SAFECode Overview

- The Software Assurance Forum for Excellence in Code (SAFECode) was announced on October 2007
- 7 Global members Adobe, EMC, Juniper, Nokia, Microsoft, SAP, and Symantec
- Established SAFECode International Advisory Board in October 2008

**SAFECode Lines of Work**

| Assurance | Integrity | Education | Measurability |
|---|---|---|---|
| **October 2008** *Fundamental Practices for Secure Software Development: A Guide to the Most Effective Secure Development Practices* | ***July 2009*** *The Software Supply Chain Integrity Framework: Defining Risks and Responsibilities for Securing Software in the Global Supply Chain* | **April 2008** *Security Engineering Training: A Framework for Corporate Training Programs on the Principles of Secure Software Development* | *In progress* |

Phase 2 is now under way

# Supply Chain Context

- Commercial software **underpins** the information technology infrastructure that businesses, governments and critical infrastructures rely upon for their most vital operations
- Enterprise customers are rightfully concerned about the **security of commercial software** and the potential for its **exploitation** by those seeking to maliciously disrupt, influence or take advantage of their operations
- **Historically**, commercial software was **developed** at a **central** location
- However, as market demands for **innovation** and **competitiveness** have increased, a more **distributed approach** to software development is evolving as commercial software vendors expand to serve **international markets** and seek engineering skills and numbers wherever they reside globally
- **Limiting** the use of **global resources** for **software development** is **not practical** in today's market environment, the increased distribution of development activities globally does raise questions about what additional product security and commercial brand risks are introduced, how these risks should be assessed, and what proactive measures can minimize their occurrence

# What is Supply Chain Security?

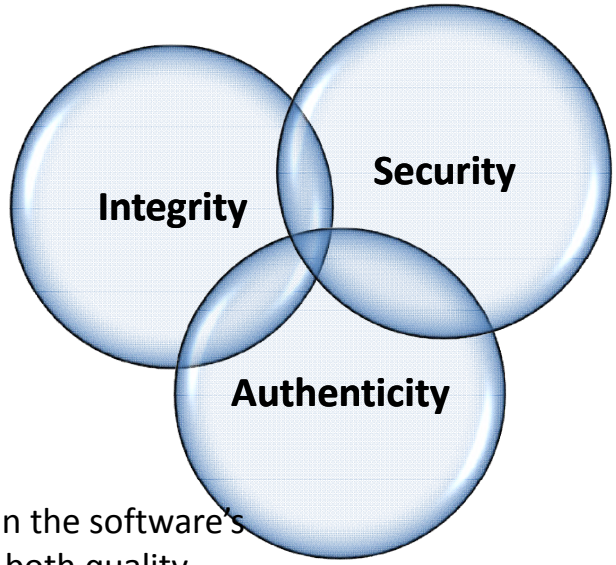
- Customers want *assurance* that their vendors' software supply chain is secure, doesn't have malware, and is not counterfeit
- The concept of software supply chain integrity and its key components of "software integrity" and "software supply chain" are not clearly defined
  - How do you identify, compare, communicate and evaluate software integrity best practices?
- SAFECode launched a two part initiative to bring clarity and focus to software supply chain integrity from a *software engineering perspective*
- As part of this effort SAFECode will
  - identify the threats and assess the risks
  - share its members' current practices for mitigating those corresponding risks, and
  - develop process guidelines that other software companies can leverage to protect the integrity of the software they produce through the global supply chain.

- **Phase 1: Released paper July 21, 2009**
- **Phase 2: Developing a detailed list of controls to be released in late 2009 or early 2010.**

# Software Integrity an Element of Software Assurance

- **Software assurance is most frequently discussed in the context of ensuring that code itself is more secure through the repeatable application of secure software development practices**

- **Another key consideration is the security of the processes used to handle software components during their sourcing, development and distribution since a variety of potential attack vectors exist throughout the software lifecycle**




## Assurance

- **Security: Security threats are anticipated** and addressed in the software's design, development and testing. This requires a focus on both quality aspects (e.g., "free from buffer overflows") and functional requirements (e.g., "passport numbers must be encrypted in the database")
- **Authenticity: The software is not counterfeit** and customers are able to confirm that they have the real thing
- **Integrity: The processes for sourcing,** creating and delivering software contain controls to enhance confidence that the software functions as the supplier intended

# Supply Chain Context

- A supply chain attack can be directed at any category of software, including custom software, software delivering a cloud service, a software product, or software embedded in a hardware device
- Software in any of these categories is often packaged as a collection of files
- To be successful, a software supply chain attack must result in either:
  - the modification of an existing software file(s); or,
  - the insertion of an additional file(s) into the collection of software files.

SAFECode Focus

# Describing the Supply Chain


1. ***Supplier Sourcing:*** Select the suppliers**,** establish the specification for the supplier's deliverables, and receive software/hardware deliverables from the suppliers;

2. ***Product Development and Testing:*** Build, assemble, integrate and test components and finalize for delivery; and,

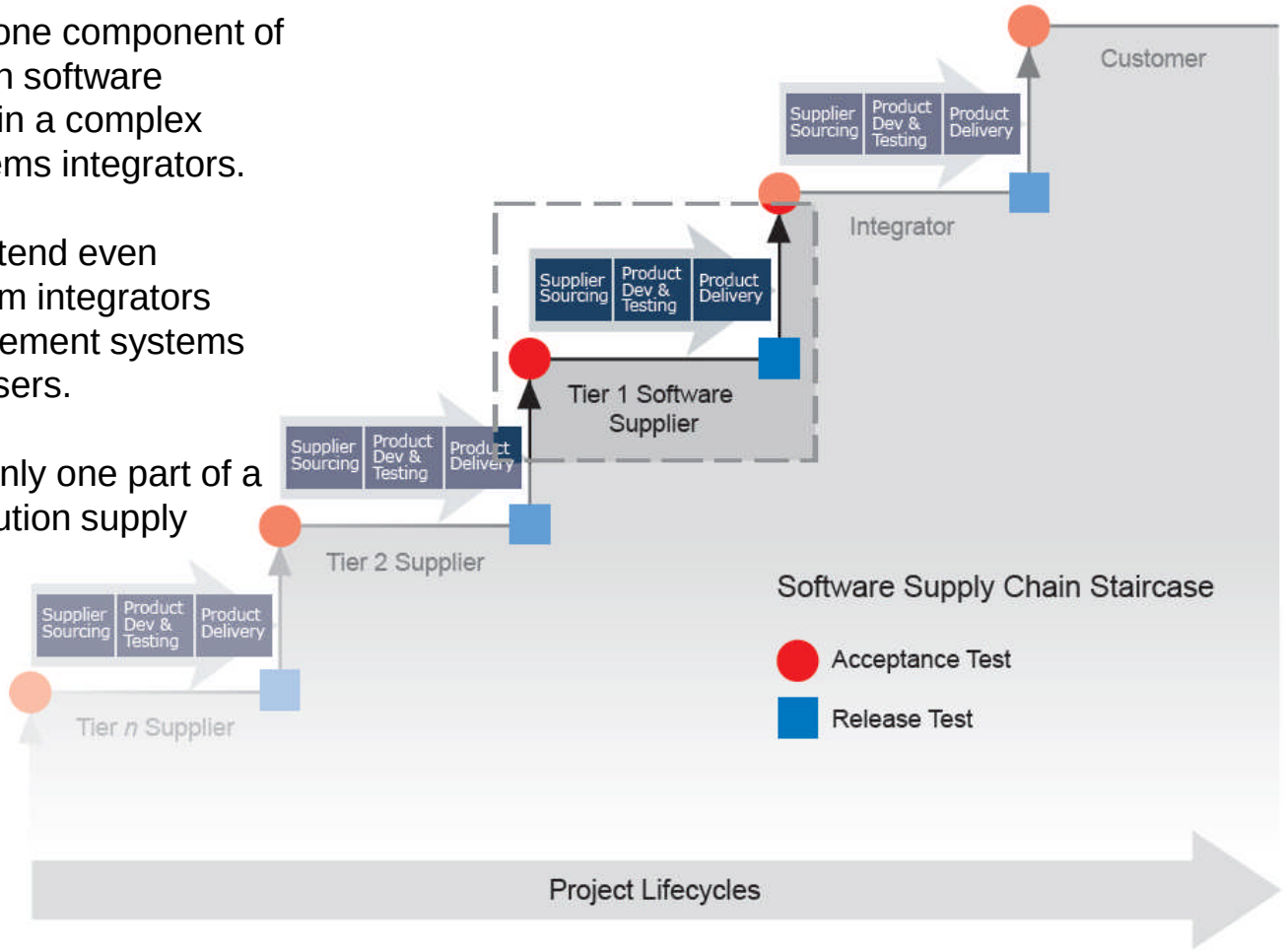
3. ***Product Delivery:*** Deliver and maintain product components to the customer.

# Software Supply Chain Staircase

- Delivered software is just one component of a larger IT solution and each software supplier is only one vendor in a complex chain of suppliers and systems integrators.

- Customer relationships extend even beyond the traditional system integrators since some “acquirers” implement systems as solutions for other end users.

- Software supply chain is only one part of a larger, more complex IT solution supply chain.



# Principles for Designing Software Integrity Controls

## Chain of Custody

**Each handoff during source code lifetime is authorized, transparent and verifiable**

## Least Privilege Access

**Personnel can access critical data with only the privileges necessary to perform their jobs**

## Separation of Duties

**Personnel cannot unilaterally change data, nor unilaterally control the development process**

## Tamper Resistance and Evidence

**Attempts to tamper are obstructed and when they do occur they are evident and reversible**

## Persistent Protection

**Critical is protected even if removed from the development environment**

## Compliance Management

The success of protections can be continually and independently confirmed

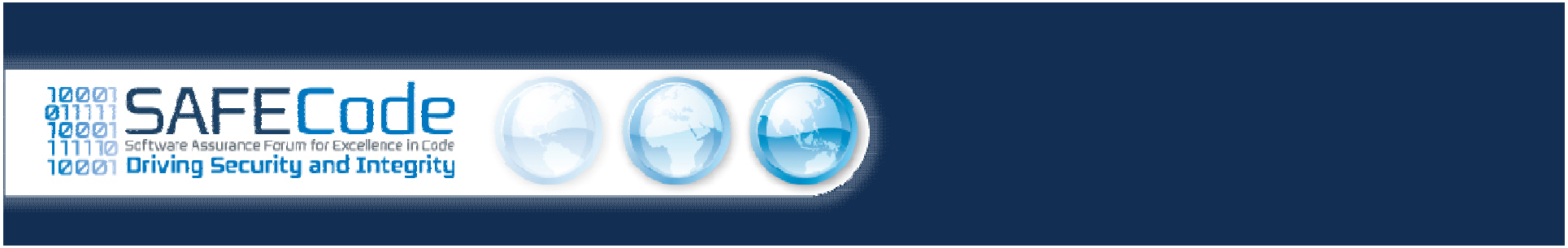
## Code Testing and Verification

**Methods for code inspection are applied and suspicious code is detected**

# What's Next for Supply Chain?

To meet this important industry need:

- SAFECode will build upon this framework for software supply chain integrity with a focused effort to identify and analyze the most effective software integrity practices that its member companies use to help assure the integrity of their software
- We will publish our findings later this year to extend these practices across the industry and provide customers with additional insight into how to view and evaluate the processes by which software integrity is achieved




For further Information on SAFECode
please contact
stacy@safecode.org
or one of the seven global member companies

patar@microsoft.com