Building Trustworthy Systems

Overview

TRIAD

Stacy Cannady, TCG Board of Directors, Cisco Trustworthy Computing

February 2014

Agenda

Challenge

Defining Trustworthy Systems

Supply Chain Security

Trustworthy Systems Technologies

Challenge

Improve product security & integrity

AND

Reduce cost of development

AND

Reduce cost of ownership for the customer

Why are Trustworthy Systems Needed?

Infrastructure Attacks on Reputation, Revenue, and Intellectual Property

Hardware Tampering

Individual and Group Threats

Software Manipulation

Gray Market/ Counterfeit

Espionage

Disruption

Sony Pictures says LulzSec hacked 37,500 user accounts, not 1 million

June 9, 2011 | 3:02 pm

Swede Charged in Alleged Attacks on NASA, Cisco

abc NEWS

The Justice
Internet ha
universities

Security Industry

RSA SecurID authentication tokens hacked

Published: June 7, 2011 at 1:57 PM

SPIEGEL ONLINE INTERNATIONAL

Shopping for Spy Gear: Catalog Advertises NSA Toolbox

By Jacob Appelbaum, Judith Horchert and Christian Stöcker

After years of speculation that electronics can be accessed by intelligence agencies through a back door, an internal NSA catalog reveals that such methods already exist for numerous end-user devices.

The Washington Times NEWS OPINION VIDEO SPORTS LIFE MEDIA

TRENDING: NFL AL QAEDA CONGRESS FOOTBALL GREEN BAY PACKERS

EDITORS' PICKS: Pilot reports UFO around London's Heathrow Airport

HOME ▸ NEWS ▸ NATIONAL RADIO LOG IN WEE

TARGET credit card theft swells to 40 million victims

COMMENT(S) SIZE: + / - PRINT

By Anne D'Innocenzio and Bree Fowler - Associated Press Friday, December 20, 2013

Defining Trustworthy Systems

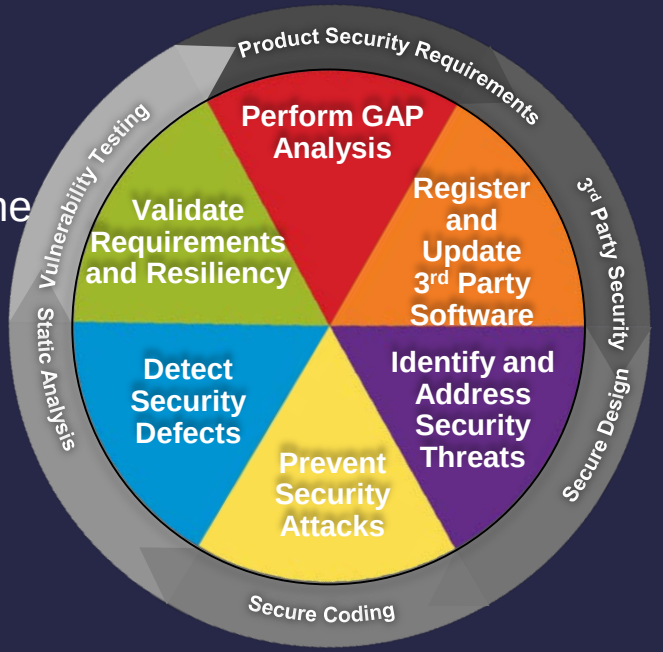
- Control the Supply Chain
- Secure Development Life Cycle
- Implementing Open Standard Security Architectures

Trustworthiness and Supply Chain Security

Secure Development Lifecycle (SDL)

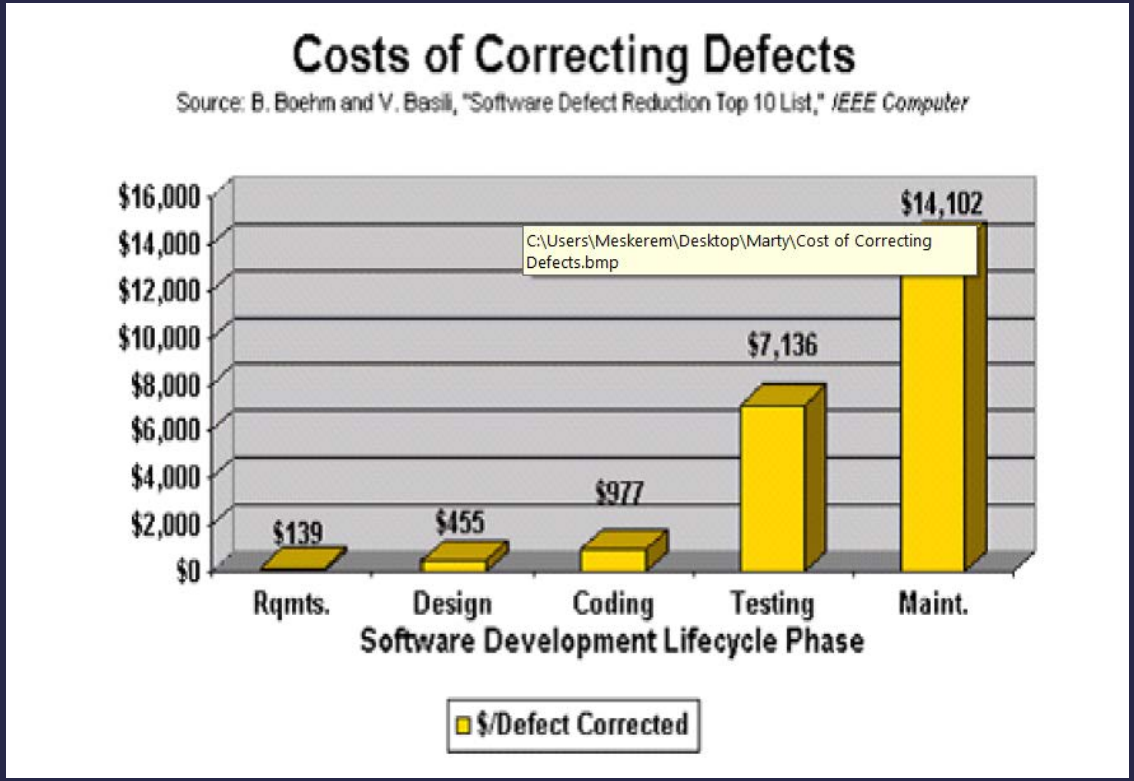
SDL reduces development costs and increases product security:

- Conforms with the guidelines of ISO 27034
- Incorporate security requirements in Product Security Baseline
- Identify security threats and mitigations during design phase with Threat Modeling
- Prevent security defects using Safe Libraries and Static Analysis tools with appropriate security rules
- Defend against exploits using Runtime Defense techniques, while Validating system through Security Testing

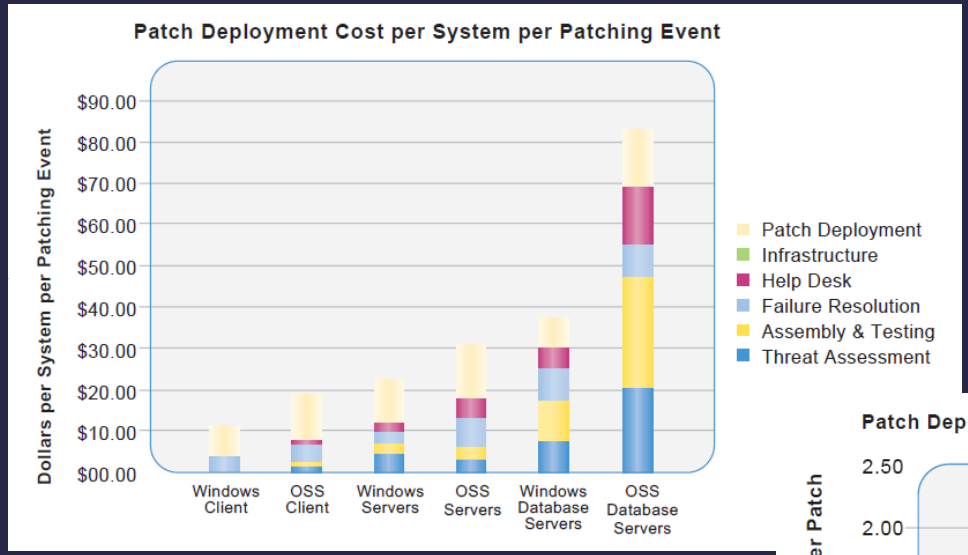


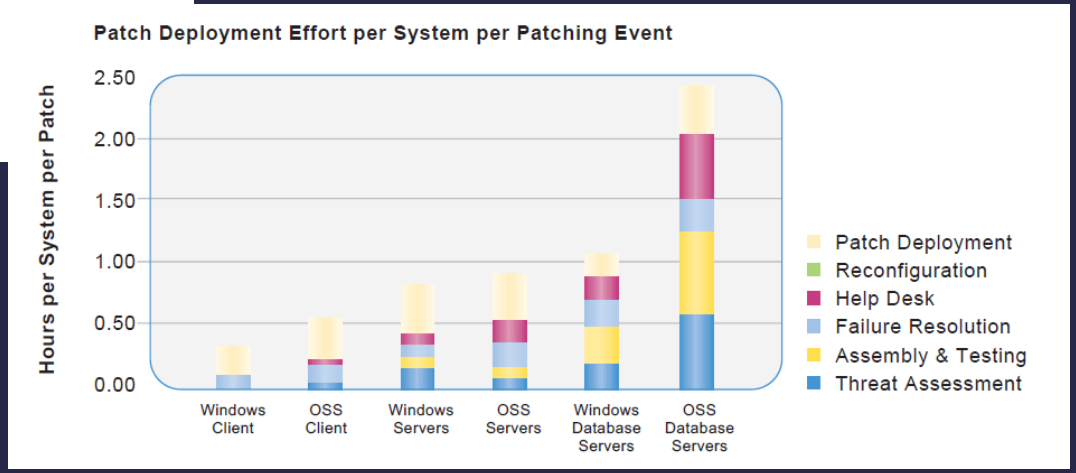
Value Statement: Ensures consistent product security through proven techniques and technologies, reducing the number and severity of vulnerabilities in software

Avoiding Defects Reduces Engineering Costs…….



Cost of Defect Correction for the Customer (patch management)

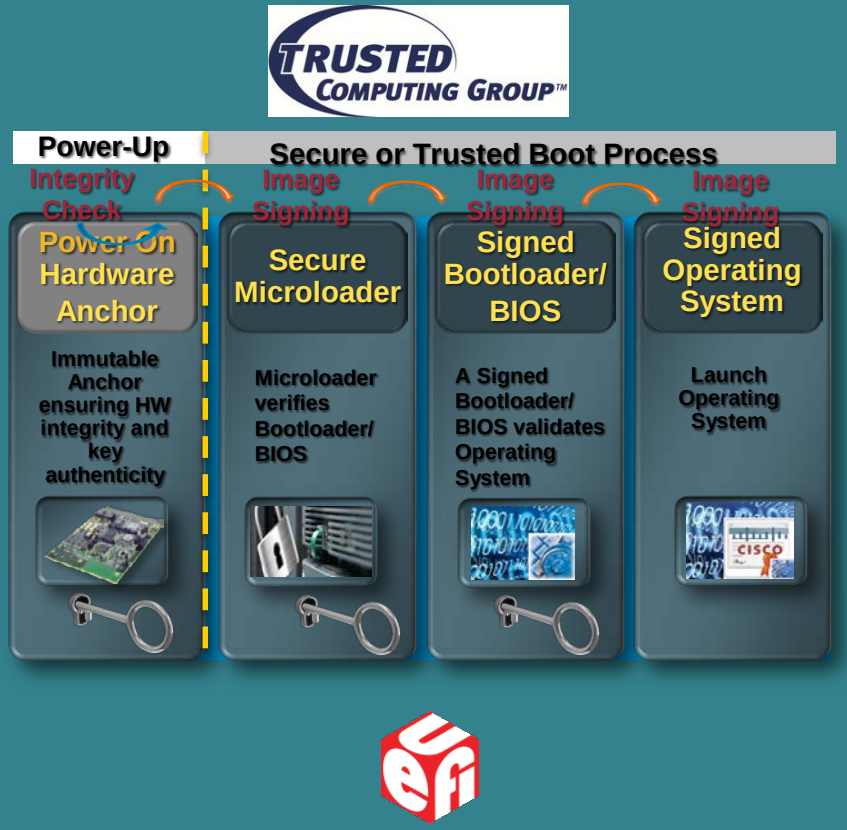




download.microsoft.com/download/1/7/b/17b54d06-1550-4011-9253-9484f769fe9f/TCO_SPM_Wipro.pdf

Secure Boot

- Ensures only authentic OEM boots up on a the OEM's Platform
- Anchored in hardware, as the image is created, the signature is installed & signed with a secure private key
- As the software boots, the system checks to ensure the installed digital certificate is valid
- Subsequent hash checks provides continuous monitoring with runtime integrity



Value Statement: Ensures that only authentic OEM software is being used while verifying the software has not been altered or tampered since it was signed

Hardware Root of Trust (HRoT)

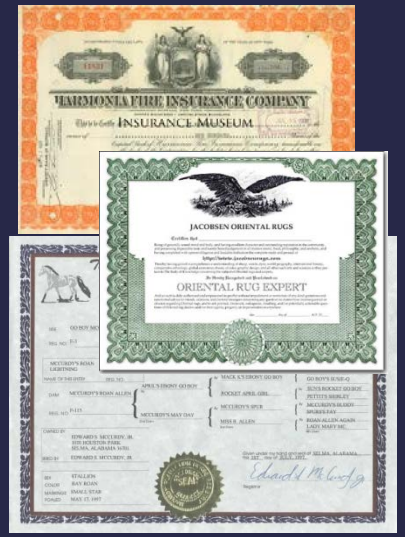
HRoTs, like Trusted Platform Modules

- Provide Immutable Identity
- Standard Identity- IEEE 802.1AR (SUDI- X.509 cert)
- Storage to Secure Credentials
- Anti-Theft & Anti-Tamper Chip Design
- HW Random No. Generator

Value Statement: Provides trustworthy OEM products, offering immutable identity, secure storage, random number generator, and encryption

Secure Identity

- Deployed in HRoT for immutable device identity (use a TPM, for example)
- A security credential installed on the device during manufacturing
- Provides a cryptographically secure unique identity for OEM products
- Communicate with the network, connection authenticated by the identity credential



Value Statement: Establishes a solution for device identity supporting authentication of the device's identity to the network

Next Generation Encryption (NGE) via Common Modules

Cryptographic Technologies

- New/upgraded algorithms (AES 128, 256 or greater, RSA 2048 or greater, ECC)
- Compatible with existing security architectures

Secure and Efficient

- Algorithm efficiency enabling increased security
- Scales well to high/low throughput

Compatible with Government Standards

- Suite B (US)
- FIPS-140 (US/Canada)
- NATO
- Germany, UK, AU
- HIPPA, PCI DSS

Authenticated Encryption

Key Establishment

Digital Signatures

Hashing

© 2012 Cisco and/or its affiliates. All rights reserved.

Standard Security Architectures

Don’t Confuse User-Facing Devices with IoT

User Facing: Android Phones	IoT Devices: Linux/Android Embedded
App writers for phones notorious for poor security practices	App writers can be trained to write secure code
App stores not policed well	No App stores
Phone users notorious for risky behavior	No users, or users can be constrained
Phone makers and carriers can’t control any of those problems	Device makers can control all of these problems

The software in an IoT device is often static

That means security can be built in by the OEM

…..

and not maintained by the customer

Access Control:
Isolate process from each other and from the OS

- SE Linux and SE Android –
  - "Security Enhanced" Linux and Android –
    - Kernel mods, tools and configuration files
    - Initial work done by the NSA, then open sourced
  - SE Android is built on top of SE Linux

- SE Security Model:
  - Mandatory Access Control – **nothing** happens unless it is allowed to happen
  - The basic security model: there are **Subjects / Actions / Objects**
    - Subjects are processes
    - Actions are anything a process might do to an object
    - Objects are anything a process might take action on
  - The Security Server process must permit a Subject to take Action on an Object -
    - **Subject="Stacy" Action=Write Object=Syslog ALLOW**

Virtualization Saves the OEM Money and Improves Platform Security

- Business value: Separate hardware from software
  - Saves software migration costs as HW evolves
  - Maximizes use of available resources
  - Virtualization saves the OEM **$$$$**

- Security value:
  - TPM (HRoT) attests integrity of hypervisor and guests
  - Process isolation
  - Ability to create a layered security model within the embedded device

Thank you.