InformationWeek
WEBCAST

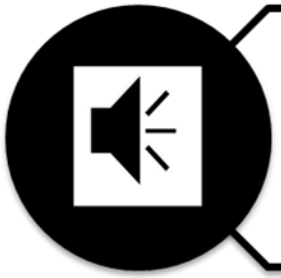
Securing the Internet of Things: New Ways to Deploy Trust in Enterprise Computing Beyond the PC

An InformationWeek Webcast

Sponsored by

UBM
TechWeb

Webcast Logistics



No Sound?

This is a streaming audio event. Make sure the sound on your PC is turned on.

Questions?

Type your questions using the Ask a Question Text Box

Technical problems?

Click the “Help” link below the media player.

Today's Presenters

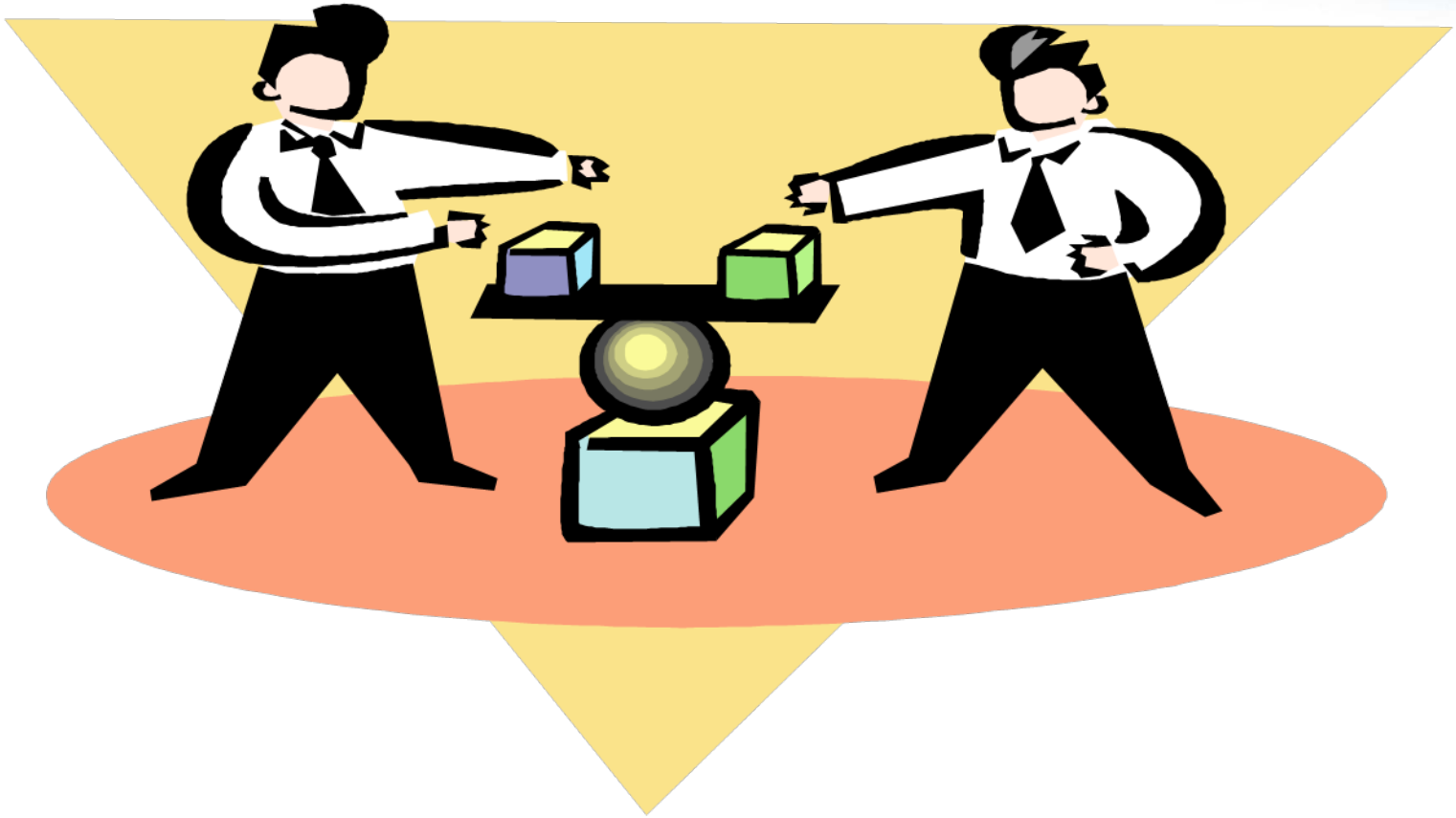
Moderator: Paul Korzeniowski,
Contributing Editor, Information Week

Chris Daly,
Business Development Director for Cybersecurity,
General Dynamics C4 Systems

Michael Donovan,
Technology Consultant, New Services Development,
Hewlett-Packard Company

Sung Lee,
Sr. Research Scientist, Wave Systems Corp.

Security: A Delicate Balancing Act



Paul Korzeniowski
Information Week

The Changing Workplace

- Employees becoming more mobile
  - Work at home
  - Work on the road
- More end user devices
  - Smartphones
  - Tablets

The Rise of Cloud Computing

- Widely accepted application development platform
- Broad definition, different segments
  - SaaS
  - IaaS
  - PaaS
- Dramatic growth

More Flexibility, Less Security

- Data is more dispersed, more chances for intrusion emerge
- Security on mobile devices is now just emerging
- Organized Crime's role
- Cost of data theft is very high

More Visibility and Control Needed

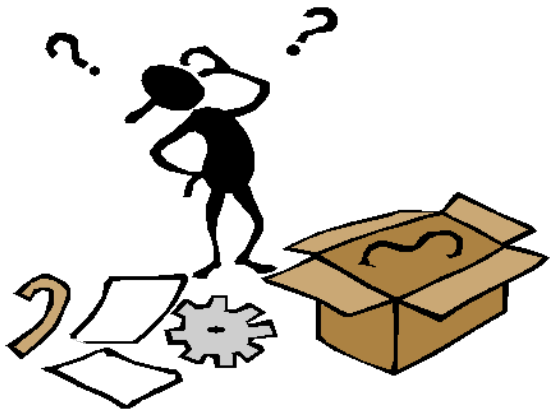
- Who is entering your network?
- What data are they accessing? What are they doing with it?
- What is happening at the end point?

Current Security Constraints

- Increased complexity
- Lower budgets
- End result: balance security risks versus security investments

Network Security Needs

- Inexpensive
- Comprehensive
- Easy to deploy
- Works with a broad range of ever changing devices



Introduction to TCG Trusted Mobility Solutions (TMS) Work Group

Chris Daly

General Dynamics C4 Systems, TMS Co-Chair

Problems and Challenges

BUSTED! Secret app on millions of phones logs key taps: An Android app developer has published what he says is conclusive proof that millions of smartphones are secretly monitoring the key presses, geographic locations, and received messages of its users. Posted by Security, 30 November 2011

Malicious apps that look like legitimate apps: A malicious Android application that looked exactly like the virtual-steam app has fooled users into purchasing the malicious app by mistake. An SMS Trojan, designed to deceive the user and surreptitiously run up charges on her mobile bill, was included with the malicious app. Posted in ThreatPost.com, 28 November 2011

Smartphone users vulnerable: The majority of Android smartphone users are walking around with insecure devices running out-of-date OS builds, leaving personal and business data at greater risk of attack. A study found that the sheer complexity of the Android ecosystem has meant security has taken a back seat, leaving smartphone users more vulnerable. Posted by Mobile, 22 November 2011

The evolution of mobile malware seems to be accelerating, especially as it applies to Android malware. The newest example of this acceleration is "GingerMaster," which sports a root exploit for Android 2.3 and gives the attacker complete control of the infected device. Posted by ThreatPost, 18 August 2011

More Problems and Challenges

Man-in-the-middle (MITM) attack was successfully launched against all 4G and CDMA transmissions in and around DEFCON 19 hacking conference. This MITM attack enabled hackers to gain permanent root access in some Android devices. Whoever launched this attack was able to steal data and monitor conversations. Posted by Extremetech.com, 10 August 2011

Bring Your Own Device to Work: Employees enjoy using work-related mobile apps, especially on smartphones and tablets that they choose themselves, according to a survey from mobile software maker Sybase. The online survey of found that half would rather choose the mobile device that they use at work. Posted by Computerworld.com, 27 July 2011

Zeus Banking Trojan Comes to Android Phones: The Zeus banking Trojan has jumped to the growing ecosystem of mobile Android devices. Researchers say a Zeus variant, dubbed "Zitmo," has the ability to intercept one time pass codes sent to mobile phones as an added, "two factor" security measure. Posted by Threatpost.com, 12 July 2011

Smartphones - The New Lost And Stolen Laptops Of Data Breaches: Enterprises have enacted full-disk encryption to protect themselves from their data being exposed through careless laptop users. And now companies must deal with mobile devices that are smaller, always-on, unmanaged, and need to be plugged into the corporate network. Posted by DarkReading, 7 October 2011

Why TMS WG?

- The Need: Mobile devices and network infrastructure must be secure, trustworthy, AND the user experience must be simple
  - A Root of Trust to enable:
    - Trusted User Identity
    - Trusted Platform Execution and Integrity
    - Secure and Trusted Communications
    - Secure Data Storage
  - A trusted way to provide Dual Use (Enterprise and Personal)
  - A secure way to handle Multiple Stakeholders for Manageability and Situational Awareness
- The Opportunity: Extending Trustworthy Protections and Manageability E2E from Ecosystem Providers to Mobile Endpoints
- The Solution: TCG Can Provide Trustworthy and Secure Capabilities That Are Cost-Effective and Practical for Current and Future Mobile Ecosystem Providers and Users

TMS WG Approach

Deliverables

Threat Matrix

Use Cases

Reference Architecture

Solution Requirements

Reference Implementation

Compliance Matrix

Demonstrations of E2E Capabilities

Outreach

TCG Work Groups

Mobey Forum

Global Platform

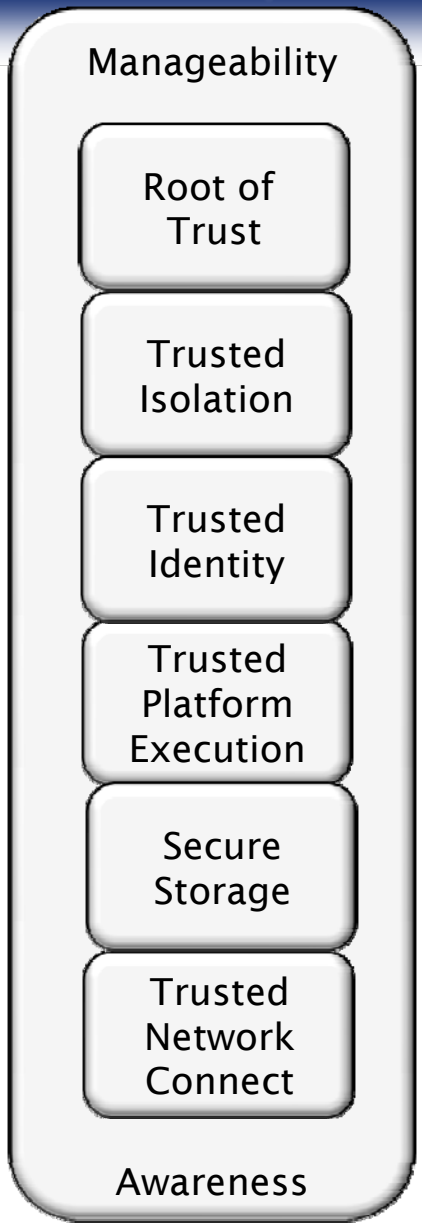
Government Mobile Applications Group

Desktop Management Task Force

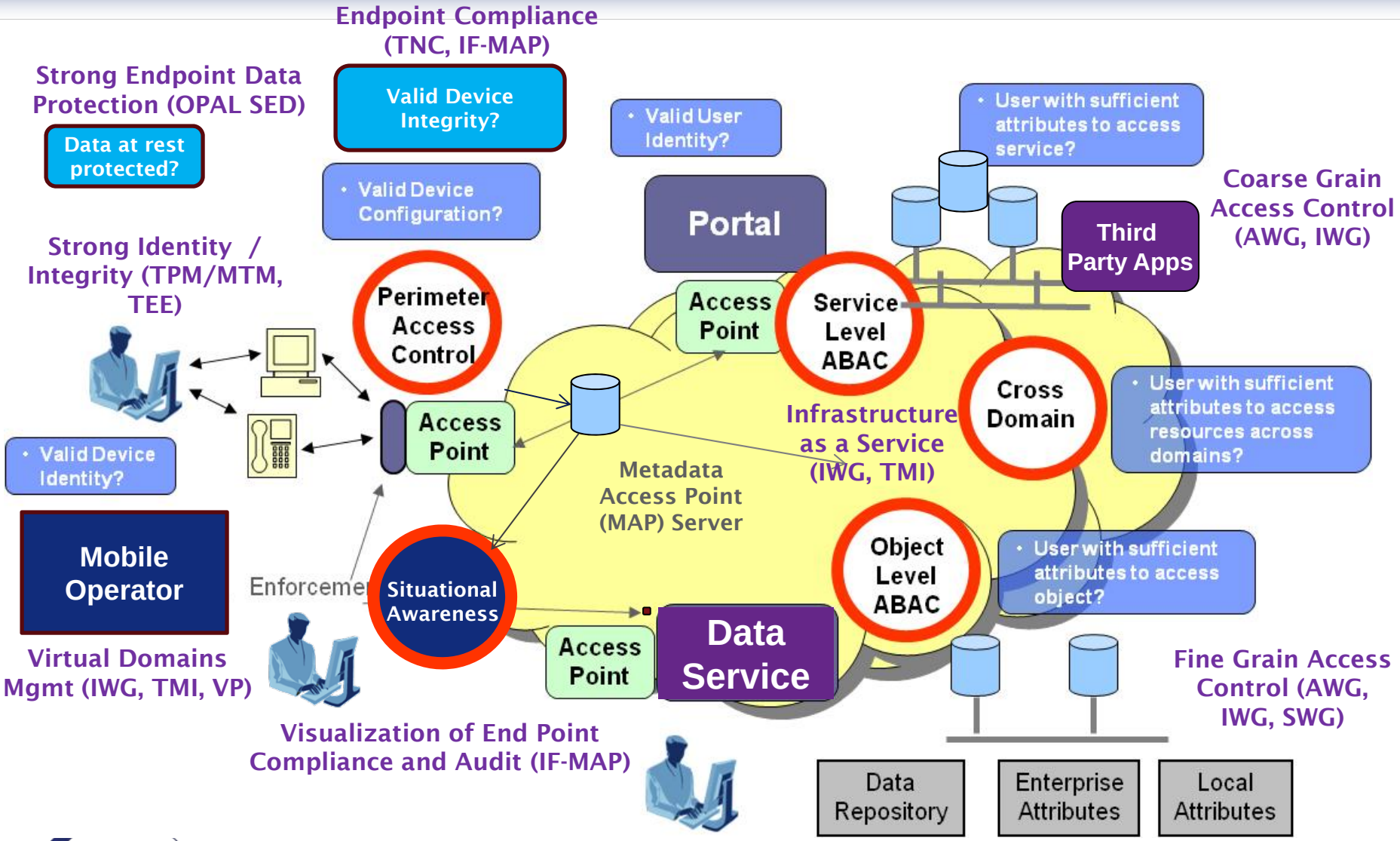
Providers

Adopters

Others



Notional E2E Mobile Work Scenario



Trusted Multi-Tenant Infrastructure?

A new approach to cloud security

Michael Donovan

Hewlett-Packard, TMI WG Co-Chair

Trusted Computing and Cloud

So what is the root problem of cloud security?

TRUST

- In cloud you can't directly verify the Trusted Computing Base

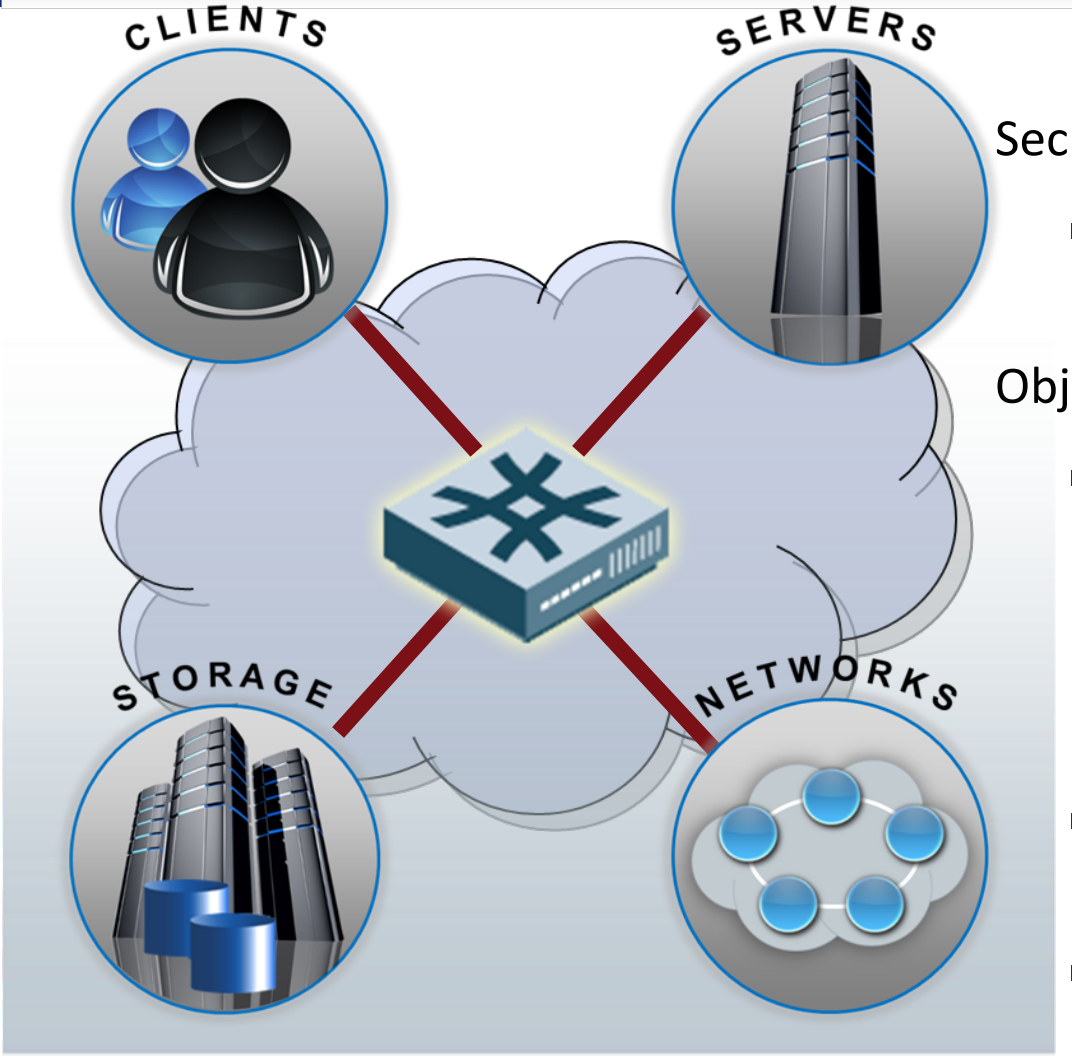
Market Observations

- Multi-Tenant security is an end-to-end configuration requirement, while most of the products and standards address specific devices or functionality within the overall end-to-end scope
- Many standards and products contribute to the ability to solve parts of the problem
- No comprehensive framework exists to describe the business/mission needs and validate compliance of the entire solution set against open standards
- There is a need for solutions that address trust and security across solutions derived from combining dedicated and shared infrastructures

Market Demand

- Cost reduction and consolidation of IT resources and staffing
- Green Initiatives to better manage power usage and waste
- To support shared infrastructure for critical infrastructure:
  - Financial (PCI), Healthcare (HIPAA), Energy (NERC/CIP)
  - Global Government and Industrial Base
  - Defense including joint service or coalition operations (HAP)
  - Shared services within public, private, community and hybrid “clouds”

Trusted Platform Framework



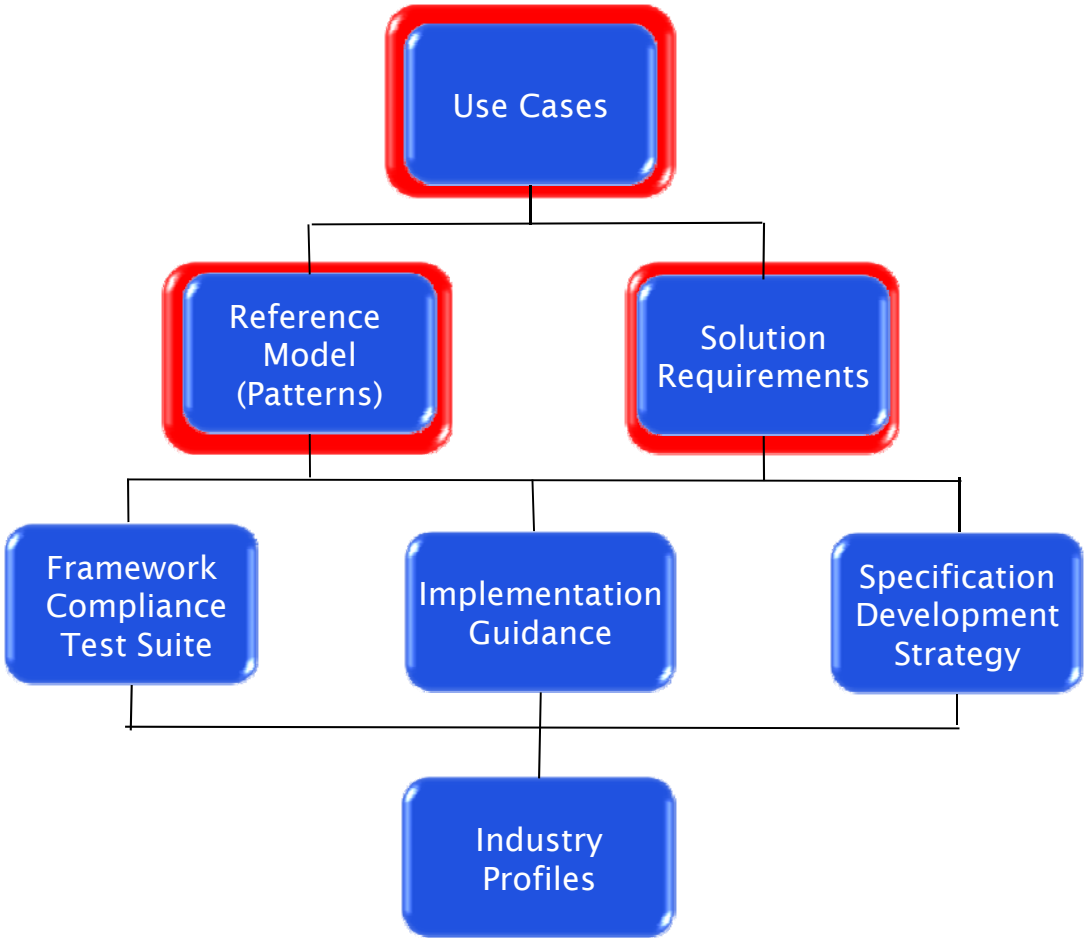
Security Built In & Coordinated

- **Trusted Multi-Tenant Infrastructure (TMI)**

Objectives

- Standards framework for implementing:
  - Shared Infrastructures
  - Multi-Provider Infrastructures
- Reference Models and Implementation Guidance
- Identify and address gaps in existing standards

Trusted Multi-Tenant Infrastructure Deliverables



TMI Reference Framework: Phase 1: Use Cases

- Most use cases can be derived from a small set of core primitive capabilities:
  - Establish Trust
    - Establish a level of trust (including the degree and types of information to be accepted) between parties
  - Exchange information in the Trusted Context
    - Exchange information between parties within the bounds of the trust relationship
  - Establish and Enforce Policy
    - Identify executable policy statements and stores, information sources and sinks, decision authorities, execution points, obligations on parties and policy hierarchies
- Define use cases using the vocabulary associated with the core primitive functions
  - Provide information from a confidential source to a recipient in another tenant domain with assurance of the ability to trust the information is reliable
  - Determine if workload from a tenant domain can be provisioned to an external cloud provider in accordance with the policies of both the provider and consumer of services

http://www.trustedcomputinggroup.org/resources/tcg_trusted_multitenant_infrastructure_use_cases

TMI Reference Framework: Phase 2: Reference Model

Goals:

- Acknowledge that actual cloud usage models are evolving
- Cooperative adoption of best of breed standards

Approach:

- Define Use Cases and related Usage Scenarios
- Derive Behavior Patterns from the Use Cases
- Align Behavior Patterns to Implementation Standards

Benefits:

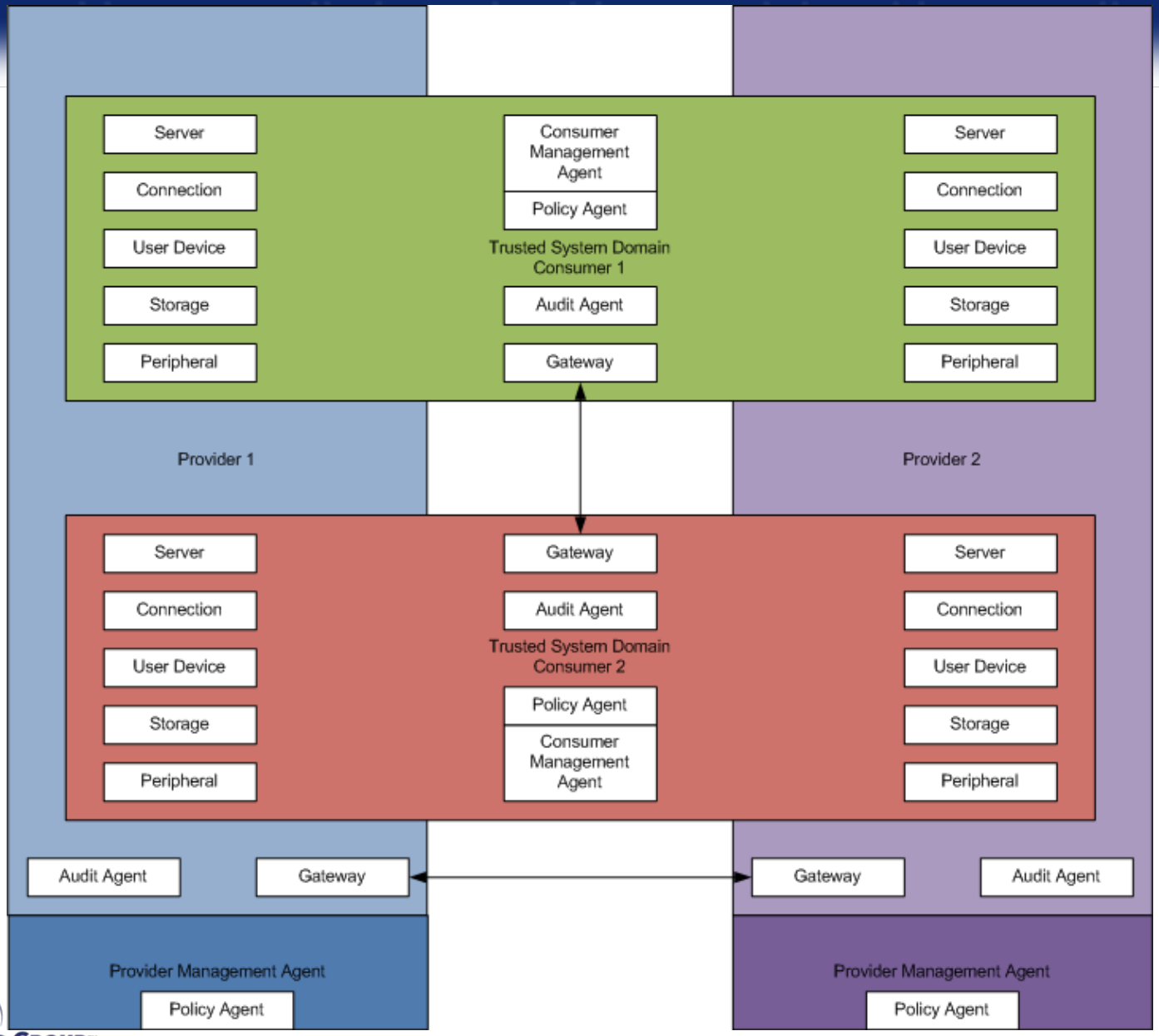
- Library of patterns can grow and evolve with actual usage models
- Support cooperative development and open vendor implementation

Model topics for V1

- Core Services
- Monitoring and Management Services
- Provisioning Services
- Reporting and Audit Services

Using the Reference Model

- Define the business problem
- Determine the asset types required
- Align Use Cases to create domains and identify assets to be provisioned
- Identify Solution Requirements that must be met
- Select Implementation Patterns that best allow requirements to be met for assets and policy requirements
- Use pattern alignment to standards to select products and services to implement a trusted infrastructure solution for the business problem



How will this change the game?

In an IT commons based on multi-tenant, shared infrastructure, the challenge is to:

- Establish trust in the provider of IT services
- Establish and monitor compliance to changing IT policy
- Assess and monitor compliance to cost, policy and performance objectives
- Do this in a multi-sourced, multi-supplier ecosystem

To establish and maintain trustworthy ecosystems:

- Enable consumers to assess the trustworthiness of supplier systems
- Enable real-time assessment of compliance as part of the provisioning process
- Define and implement best practices and standard patterns for building and operating trustworthy infrastructures
- Define mapping of standards against a reference model to improve integration of trustworthy components
- Support real time assessment and enforcement of policy to ensure shared infrastructure remains in compliance

The use of open trusted platform standards provides consumers a way to assess the suitability, compliance and performance of shared systems

Trusted Computing Group: Embedded Systems Work Group

Sung Lee

Wave Systems, Corp.

Computing Platforms are Everywhere!

Embedded into:

- Turbine to Toast and everything in between
- With varying degrees of complexity
- Deeply intertwined with everyday life

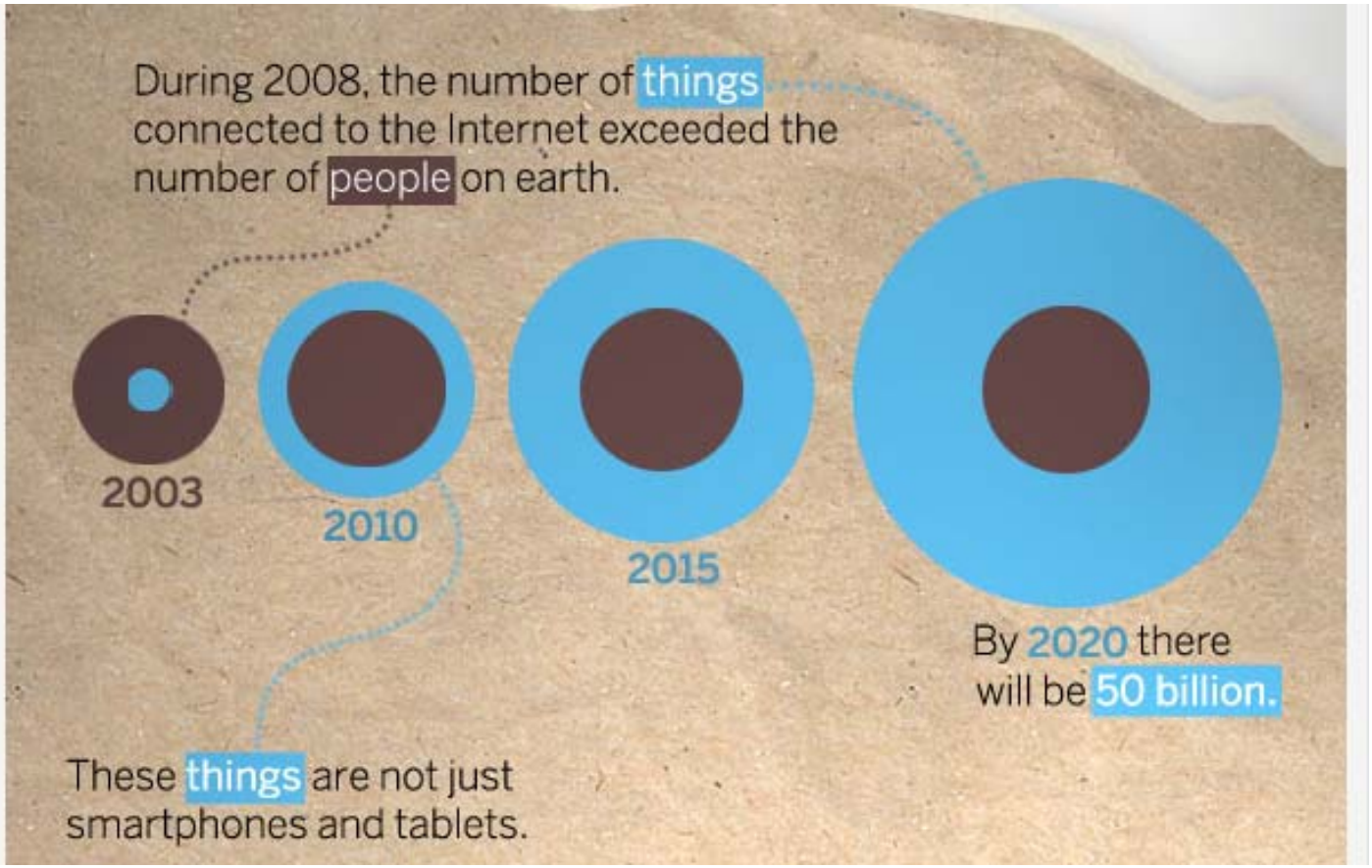
No longer just your usual IT network devices

Embedded computing is mostly hidden and invisible, but ubiquitous and persistent !

THE INTERNET OF THINGS

"The next logical step in the technological revolution connecting people anytime, anywhere is to connect inanimate objects. This is the vision underlying the **Internet of things: anytime, anywhere, by anyone and anything**" – ITU, November 2005

Networked



Source: http://blogs.cisco.com/news/the-internet-of-things-infographic/

Devices talk to each other!

Large Scale & Long Term Deployment

Source: http://www.chevrolet.com/assets/en/images/model/2012/volt/gallery

Chevy Volt has over 100 microcontrollers & a unique IP address!

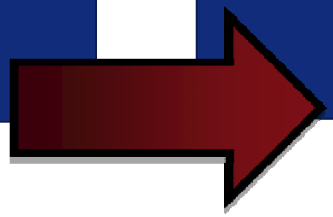
Remote and Unattended

No perimeter to manage and protect!

Embedded Systems Are

- Resource constrained
- Networked
- Large scale deployment
- Long term deployment
- Remote
- Unattended

- Limited options
- Device to device
- FW/SW upgrade is unavoidable
- Nightmare to manage, if not impossible



Attacks on embedded system itself may be minimal, but it could be turned into a stepping stone!

Aren't Embedded Systems Safe?

Embedded systems have lost their security innocence

- Security by obscurity days are over
- Motivation for many reasons
  - Financial, political, fame, …

- Stuxnet: http://www.stuxnet.net/
- Make your water undrinkable: http://www.networkworld.com/news/2011/072711-blackhat-phone-hacks.html
- Remote update of printer firmware: http://www.huffingtonpost.com/2011/11/29/security-flaw-in-printers_n_1119558.html
- Hacking medical devices – Continuous Glucose Monitor: http://www.thesecurityblog.com/2011/08/bh-2011-hacking-medical-devices-for-fun-and-insulin/
- Hackers break into a car via text message: http://www.engadget.com/2011/08/04/hackers-break-into-subaru-outback-via-text-message/

Various Protection Mechanisms Needed

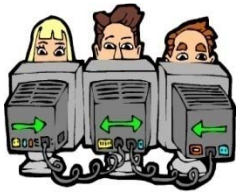
Detect Intrusions Limit Damage

Firewalls

Intrusion Detection Systems

PKI

Boundary Controllers



VPNs

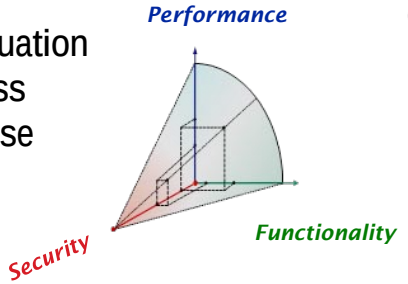
Operate Through Attacks

Intrusion Tolerance

Graceful Degradation

Big Board View of Attacks Real-Time Situation Awareness & Response

Hardened Core



But, Must not be Easy to Circumvent

Root of Trust for Embedded Systems

Trusted device to device communication

Trusted FW/SW update

Secure or verified boot

Trusted Computing Base with

- *Small footprint*
- *Resource aware*
- *Self provisioning and configuring*

Strong device identity

Device integrity

Attestation

TRUSTED COMPUTING GROUP™

Trusted Embedded Computing Fulfills the Demand for Security and Safety in Our Infrastructure

- TCG specifications address society's growing security and privacy problems by moving trust to hardware
- TCG EmSys secures embedded computing systems, devices, applications and networks more effectively than software
- Trusted Computing proactively prevents loss of integrity, data manipulation, leakage and viruses
- Trusted Embedded Computing enables machine identity and integrity to be trusted, especially remotely

More Will Come, Stay Tuned

TRUSTED COMPUTING GROUP™

Trusted Computing will become a Necessary Part of Advanced, Future Embedded Applications

Annex A: Public (Government Sponsored) Research Programs Concerning Embedded Trusted Computing

www.tecom-project.eu Trusted Embedded Computing (TECOM), analysis and use cases

www.tecom-itea.org Another TECOM project, also very useful

www.opentc.net Open Trusted Computing in an Linux and embedded Eco system; A lot of reports, software, links, books etc; This is a must

evita-project.org Trusted computing for next generation automotive car to X communication

www.secricom.eu Secure crisis communication with the assistance of trusted computing technology

www.sepia-project.eu Secure Embedded Platform with advanced Process Isolation and Anonymity capabilities

www.SecFutur.eu Unleash the potential of security in embedded environments through the provision of standardised security building blocks

http://www.teresa-project.org **T**rusted Computing **E**ngineering for **R**esource Constrained **E**mbedded **S**ystems **A**pplications

Annex B: Open Source Code Useful When Working on Trusted Embedded Computing

https://lkml.org/lkml/2011/7/22/137 I2C driver on Linux kernel-org

ibmswtpm.sourceforge.net Several sw API modules for trusted computing, esp. libtpm as low level library for embedded applications

tpmj.sourceforge.net Java-based API for the Trusted Platform Module (TPM), also useful for Android OS

http://git.chromium.org/gitweb/?p=chromiumos/third_party/u-boot.git;a=tree;f=drivers/tpm/slb9635_i2c;hb=chromeos-v2011.03 I2C and UBoot based on TPM

sourceforge.net/projects/libtnc OS independent implementation of the Trusted Network Connect (TNC) specification from Trusted Computing Group (TCG)

sourceforge.net/projects/trustedgrub Trusted boot loader for Linux; Code is in general useful for initializing a Trusted Platform Module and execute integrity measurement based on trusted computing

Additional Information

- **Trusted Mobility Solutions Work Group:**
  http://www.trustedcomputinggroup.org/developers/trusted_mobility_solutions

- **Trusted Multi-tenant Infrastructure Work Group:**
  http://www.trustedcomputinggroup.org/developers/trusted_multitenant_infrastructure

- **Embedded Systems Work Group:**
  http://www.trustedcomputinggroup.org/developers/embedded_systems

- **TCG Membership Information:**

  http://www.trustedcomputinggroup.org/join_now/membership_benefits

Q&A

Please Submit Your Question Now

Resources

To View This or Other Events On-Demand Please Visit:

www.netseminar.com

For more information please visit:

www.trustedcomputinggroup.org