Presentation Overview

• Background & Context
• The Supply Chain Challenge
• Industry Response
• Roadmap & Outreach Activity
• What You Can do Now
• Resources
Background & Context
Initial Requirements

• U.S. Government concerns
  • Increased use of Commercial Off The Shelf (COTS) Information Communication Technology (ICT)
  • Need to confidently identify trusted COTS ICT products & providers

• U.S. Government-industry roundtable - 2009
  • Initiated by U.S. Government Under Secretary of Defense

• U.S. Government recommendation
  • Establish consensus on best of breed practices based on industry experience to create a standard to which all providers can conform when building products
Additional Requirements

• Need to address critical infrastructure
  • Banking
  • Telecommunications
  • Utilities

• Needs of international governments and markets
The Supply Chain Challenge
## Technology Supply Chain Threat Matrix

<table>
<thead>
<tr>
<th></th>
<th>Taint</th>
<th></th>
<th>Counterfeit</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Upstream</td>
<td>Provider</td>
<td>Downstream</td>
<td>Upstream</td>
</tr>
<tr>
<td>Malware</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Malicious code</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>(masquerading as</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>vulnerabilities)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unauthorized</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>“Parts”</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unauthorized</td>
<td>✔</td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Configuration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scrap/ Substandard</td>
<td>✔</td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Parts</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unauthorized</td>
<td>✔</td>
<td></td>
<td></td>
<td>✔</td>
</tr>
<tr>
<td>Production</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The Supply Chain Challenge for ICT Providers

Product certification is not enough. Need assurance that best practices are followed through product life cycle including global supply chains.

Challenges:
- Need to secure our Global Supply Chains
- Need a full life cycle approach
- Need a standard of best practices for all constituents in the chain
- Need accreditation to help assure conformance to the standard
- Need public registry to identify trusted/accredited constituents
- Need customers to reward trusted/accredited constituents thru procurement

“Build with Integrity – Buy with Confidence”
A Threat-Based Problem

Global supply chain security for COTS products

- Commercial Off the Shelf Products are developed and used globally
- COTS products rely on components that are often globally sourced
- COTS products are integrated into Critical Infrastructure, Government systems and Commercial solutions

THREATS

- Counterfeit product
- Maliciously tainted
- Tainted
- Insiders
- Obsolescence
- Many others …
Critical Infrastructure: One way to categorize the many requirements

The **product** does what it’s intended to do functionally & performs at the required performance levels.

Operator organizations must ensure security & integrity of systems during operation.

The **product** meets certain security assurance levels based on requirements of the environment and the acceptable level of risk for that environment.

Integrators and **IT product providers** must follow best practices for security, integrity - design thru disposal (both in-house and in their supply chains).
The Industry Response
A global industry-led initiative defining best practices for secure engineering and supply chain integrity so that you can “Build with Integrity and Buy with Confidence™”
OTTF Principles

**Practical and effective**
Practitioner based, evidence that it works in the field

**Reasonable**
Achievable and implementable by a wide variety of vendors and stakeholders

**Open**
Based on open consensus standards and recognized industry best practices – publicly available to all

**Affordable**
Reasonably cost effective to implement

**Organizational/Process Based Accreditation**
Flexible enough to cover all scales of supply chain
Open Trusted Technology Provider™ Standard

The first version of the O-TTPS addresses the most pressing threats

- Maliciously Tainted Products
- Counterfeit Products
O-TTPS Standard – Mitigating Risks for Tainted and Counterfeit Products

- A **tainted product** is “produced by the provider and is acquired through reputable channels but has been tampered with maliciously”.

- A **counterfeit product** is “produced other than by or for the provider, or is supplied by other than a reputable channel, and is represented as legitimate”.

- Double risk if counterfeit products are also tainted
O-TTPS: Mitigating Maliciously Tainted and Counterfeit Products

O-TTPS applies to and mitigates threats across product life cycle

- Looks at process, not product
- Scope is flexible, from entire organization to one product
- Two areas of requirements
  - Technology Development - *mostly* under the provider’s in-house supervision
  - Supply Chain activities *mostly* where provider interacts with third parties who contribute their piece in the product’s life cycle
O-TTPS: Technology Development

• Product Development/Engineering Requirements in:
  • Software/Firmware/Hardware Design Process
  • Development/Engineering Process and Practices
  • Configuration Management
  • Quality/Test Management
  • Product Sustainment Management

• Secure Development/Engineering Requirements in:
  • Threat Analysis and Mitigation
  • Run-time Protection Techniques
  • Vulnerability Analysis and Response
  • Product Patching and Remediation
  • Secure Engineering Practices
  • Monitor and assess the impact of changes in the threat landscape
O-TTPS: Supply Chain Activities

- Supply Chain Requirements In:
  - Risk Management
  - Physical Security
  - Access Controls
  - Employee and Supplier Security
  - Business Partner Security
  - Supply Chain Security Training
  - Information Systems Security
  - Trusted Technology Components
  - Secure Transmission and Handling
  - Open Source Handling
  - Counterfeit Mitigation
  - Malware Detection
A Holistic Approach to Securing Global Supply Chains

Customer/Acquirer
Demands Accreditation certificate as evidence of conformance to Open Trusted Technology Provider™ standards

Integrator, Distributors, Resellers
Will seek business partners who meet Open Trusted Technology Provider™ requirements

Component Suppliers
May be hardware, software, global, open source - or not - multiple supplier layers

Provider
Will seek business partners who meet Open Trusted Technology Provider™ requirements

Standards Body
Will seek ways of achieving market up-take/ integrity of standards

Accreditation/Accreditation Body
Must be independent & vendor/technology-neutral

Copyright © The Open Group 2015
The O-TTPS Accreditation Program

The Open Group

Suppliers
Distributors
Providers
Integrators
Resellers

Standards Authority (OTTF):
develops and maintains Standard

Accreditation Authority
awards accreditation

O-TTPS Accreditation Program

Verifies Conformance

O-TTPS Recognized 3rd Party Assessors

Open Trusted Technology Providers™

Copyright © The Open Group 2015
The O-TTPS Accreditation Program
Accreditation Program

• Based on
  • Warranty from applicant organization
  • Conformance Assessment by Recognized Assessor
• Uses trademarked logo
  • Identifies accredited suppliers and their scope
• Open to
  • Component Suppliers
  • Providers
  • Integrators
  • Distributors
  • Resellers
  • Others…
Accreditation Program Description

• The Applicant can be a Technology Provider, Component Supplier, Integrator, Distributor (Value-Add), Reseller
• The Applicant warrants and represents their conformance to requirements throughout their declared Scope of Accreditation – that is they claim that they follow the best practices throughout the product life-cycle, including supply chain cycles for all of the products in their declared Scope
• Scope up to Applicant: product, product(s), product-line, organization, etc.
• Warranty backed by evidence of conformance and assessment of evidence by 3rd Party Assessors
• The Open Group will operate vendor-neutral program, provide oversight and consistency across applications
• Successful Applicant gets certificate and use of Trademark and Logo
• The Open Group manages Trademark and Logo use, problem reporting and appeals process.
• The accreditation period is 3 years before required renewal
• Launch of a public O-TTPS accreditation program December 2014 – open to any organization – don’t need to be a member
O-TTPS Accreditation Register

There are 1 Accredited Organizations

<table>
<thead>
<tr>
<th>Organization</th>
<th>Scope of Accreditation</th>
<th>Standard</th>
<th>First Accredited</th>
<th>Re-Accreditation</th>
<th>Status</th>
<th>Conformance Statement</th>
<th>Certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informatica Business Machines Corporation</td>
<td>IBM's Application Infrastructure and Middleware (AIM) Software Business Division</td>
<td>Open Trusted Technology Provider™ 1.0</td>
<td>30-Jan-2014</td>
<td>30-Jan-2017</td>
<td>Accredited</td>
<td><img src="image1.png" alt="icon" /></td>
<td><img src="image2.png" alt="icon" /></td>
</tr>
</tbody>
</table>
Assessments by 3rd Party Labs

• Publicly Available Assessment Procedures
  • Help achieve objectivity, repeatability, and consistency across accreditations

• Two types of requirements/evidence to be assessed: process and implementation
  • Process – Need evidence there are documented processes
  • Implementation – Need evidence that processes were implemented

• Formal Recognition of O-TTPS 3rd party labs
  • Must meet established criteria and assessors must pass O-TTPS Assessor exam.
  • Receive certificates and listed on public registry
This is to certify that the following Scope of Accreditation:
IBM's Application Infrastructure and Middleware (AIM) Software Business Division

from
International Business Machines Corporation

is accredited and complies with the requirements in the Open Trusted Technology Provider™ Standard (O-TTPS) Accreditation Program for:
Open Trusted Technology Provider™ 1.0

Date registered: 30 January 2014
Valid until: 30 January 2017
O-TTPS Recognized Assessor Requirements

Recognized Assessor Company

Accepted standards:
• ISO/IEC 17020: 2012: Conformity Assessment – Requirements for the operation of various types of bodies performing inspection,
• ISO/IEC 17021:2011: Conformity Assessment – Requirements for bodies providing audit and certification of management systems,
• ISO/IEC 17025:2005: General requirements for the competence of testing and calibration laboratories

Competent Assessors

Accepted qualifications:
• Lead auditor
  • ISO/IEC 27001
  • ISO 9001
• CMMI-DEV appraisers
• ISO/IEC 15408 or Common Criteria evaluator (with experience in evaluating life-cycle assurance requirements)
• ISO/IEC 19790 or FIPS 140-2 tester with experience in testing the process requirements of that standard

The Open Group Program relies on existing compliance with industry norms using standards commonly specified for information assurance (IA) assessor companies and process assessors
O-TTPS Recognized Assessor Requirements

Recognized Assessor Company

Has established a process for performing O-TTPS accreditations in accordance with its own established management system requirements and The Open Group Assessment Procedures

Competent Assessors

Have sufficient skills in:

- Supply chain management terminology and techniques
- Technical knowledge of O-TTPS Attributes & the assessment program
- Have successfully completed the O-TTPS Assessor Exam
O-TTPS Recognized Assessors

- atsec information security corporation
- EWA – Canada
- Booz Allen Hamilton (BAH)
Roadmap & Outreach Activity
## OTTF Milestones

<table>
<thead>
<tr>
<th>Year</th>
<th>Milestone</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010</td>
<td>Q1</td>
</tr>
<tr>
<td>2011</td>
<td>Q2</td>
</tr>
<tr>
<td>2012</td>
<td>Q3</td>
</tr>
<tr>
<td>2013</td>
<td>Q4</td>
</tr>
<tr>
<td>2014</td>
<td>Q1</td>
</tr>
</tbody>
</table>

- **Early Industry Collaboration**
- **Forum Launched**
- **Framework White Paper Published**
- **Standard Development:** Snapshot => Publish V 1.0
- **Define Conformance Criteria, Conduct Pilot Program**
- **Define & Approve O-TTPS Accreditation Program**
- **Implement and Launch Public O-TTPS Accreditation Program**

### 2012 Milestones

- **O-TTPS v. 1.0 published April 2013**
- **Conducted Pilot of the O-TTPS Accreditation**

### 2013 Milestones

- **Feb 3, 2014**
  - Announce:
    1. Public Launch of Accreditation Program
    2. First Accredited Open Trusted Technology Provider™
    3. First two O-TTPS Recognized Assessor Labs
The Open Group Trusted Technology Forum (OTTF) Roadmap

<table>
<thead>
<tr>
<th>Projects</th>
<th>1Q/2015</th>
<th>2Q/2015</th>
<th>3Q/2015</th>
<th>4Q/2015</th>
<th>1Q/2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO PAS Submission - Open Trusted Technology Provider Standard (O-TTPS) V 1.1</td>
<td>ISO DRAFT Ballot (Approved)</td>
<td>ISO FINAL Ballot</td>
<td>Publish ISO PAS Standard</td>
<td></td>
<td></td>
</tr>
<tr>
<td>O-TTPS 1.1. Translation (Simplified Chinese)</td>
<td>Review</td>
<td>Publish</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>O-TTPS Assessment Procedures – Revisions</td>
<td>Review 1.1</td>
<td>Publish 1.1</td>
<td>Consider ISO PAS Submission</td>
<td>Develop v1.2</td>
<td>Review 1.2</td>
</tr>
<tr>
<td>O-TTPS Accreditation Program – Update Policy and Supporting Documents</td>
<td></td>
<td></td>
<td>Initial</td>
<td>Develop</td>
<td>Review</td>
</tr>
</tbody>
</table>
## The Open Group Trusted Technology Forum (OTTF) Roadmap

<table>
<thead>
<tr>
<th>Projects</th>
<th>1Q/2015</th>
<th>2Q/2015</th>
<th>3Q/2015</th>
<th>4Q/2015</th>
<th>1Q/2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implementation Guide: Maps O-TTPS to NIST Cybersecurity Frame (NCF)</td>
<td>Review</td>
<td>Publish</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Executive Manger’s Guide to the Accreditation Program</td>
<td>Initial</td>
<td>Develop</td>
<td>Review</td>
<td>Publish</td>
<td></td>
</tr>
<tr>
<td>White Paper: Revision to the Initial Framework White Paper to promote market adoption</td>
<td>Develop</td>
<td>Review</td>
<td>Publish</td>
<td></td>
<td></td>
</tr>
<tr>
<td>O-TTPS 2.0</td>
<td>Initial</td>
<td>Develop</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## OTTF – Additional Publications

<table>
<thead>
<tr>
<th>Publications</th>
<th>Type</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>O-TTPS Recognized Assessor Program: Update Training Materials and Assessor Exam</td>
<td>Accreditation</td>
<td>Q2/15</td>
</tr>
<tr>
<td>Training Materials for Accreditation Applicants &amp; Market Adoption Materials for Customers</td>
<td>Accreditation</td>
<td>Q2/15</td>
</tr>
<tr>
<td>O-TTPS Mapping Table(s): Update and Provide Additional Mappings</td>
<td>Accreditation</td>
<td>Q3/15</td>
</tr>
<tr>
<td>O-TTPS Accreditation Program: Update Supporting Documents</td>
<td>Accreditation</td>
<td>Q3/15</td>
</tr>
</tbody>
</table>
Outreach & Harmonization

- Presentation to global government and industry
  - Conferences – ours and others e.g. RSA
  - East-West Institute
  - Council on Foreign Relations
  - US House Energy & Commerce Committee

- Harmonization
  - Submission to ISO
  - US Government Accounting Office Report: mentions O-TTPS as one of the two most cited supply chain standards efforts in their report
  - References to O-TTPS in NIST SP-161 draft
  - NASA RFP recommendation included O-TTPS in (SEWP V 2013)
    - Expect customers to begin demanding O-TTPS compliance

- Mapping to other standards
  - NIST Cybersecurity Framework
  - Common Criteria
What you can do now ....
What You Can Do Now …

• Customers (government, commercial):
  • Make your Suppliers, Integrators, VARs aware of O-TTPS
  • Encourage them to learn about it, prepare and get accredited
  • Let them know their accreditation is a differentiator in procurement

• Technology Providers (OEMs, component suppliers, Integrators, Value-add Resellers, Distributors):
  • Use the standard to improve the integrity and the security of your processes
  • Encourage your technology partners to get accredited.
  • Get accredited

• Customers, Technology Providers, Assessors:
  • Join the OTTF (Forum) to evolve the standard and accreditation program in a way that meets your needs
Resources
Resources

- The Open Group Trusted Technology Forum (OTTF)
- The OTTF Information Sheet Handout
- The O-TTPS (Standard) Version 1.1
- The Open Group represents OTTF at Congress
- OTTF Vendor Testimonials
- The O-TTPS Accreditation Website
- OTTF Podcast (Dana Gander with: Brickman, Lipner, Lounsbury, and Szakal)
- Press Release Feb 3, 2014 – Launch of the O-TTPS Accreditation Program
- The Open Group
Thank You!

For more information contact:

Mike Hickey m.hickey@opengroup.org

or

Sally Long s.long@opengroup.org