Update from the Supply Chain Technical Working Group

September 11, 2013

Mike Grimm, Microsoft Corp.

Terrie Diaz, Cisco Systems, Inc.

Agenda

- Background
- 2012 draft supporting document
- Current status
- Planning for trial evaluations
- Next steps

Background

Motivation and history

- Gaining appropriate visibility and transparency into supply chains for hardware and software products is a common interest in many government ICT customers.
- Goal is to create a resource for protection profile authors that demonstrates security assurance in the supply chain
- Timeline
  - Spring, summer 2011: informal study group.
  - 2011 ICCC: concept paper, invitation to join the study group.
  - 2012 CCDB: submitted a problem statement, proposed scope, terms of reference, deliverables.
  - August 2012: sent completed draft *Supply Chain Security Assurance (SCSA)* supporting document to CCDB, CC Executive Committee, CC Management Committee.
  - 2012 ICCC: begin discussing approaches for pilot evaluations that verify developer's procedures and policies.
  - May 2013: received feedback on the draft from the CC Maintenance Board.
  - Summer 2013: digested feedback and now revising the draft SCSA.

2012 Draft Supporting Document

2012 Draft SCSA

- Scope:
  - Mitigating the threat of counterfeit products and components.
  - Mitigating threats based on aspects of taint that violate product or component integrity.
- Serves as supplemental information for a protection profile and evaluation methodology.
- Specifies extent of the supply chain that needs evaluation.
- Handles supplier networks, sub-suppliers, multiple suppliers
- Aligns with SCRM models: design, source, build, fulfillment, distribution, sustainment, disposal
- Contains objectives, threats, refined assurance requirements, developer and evaluator guidance; delivered as an assurance package.

Feedback on the 2012 SCSA

- Thank you CCMB for the thorough review!
  - We asked for comments and received many.
- Three main areas of feedback
  - CC and Supporting Documents formalism [we are new at this].
    - The CCDB should consider developing a guide for how to create a Supporting Document, which is also one of the expected outputs from a iTC/cPP.
  - CC already addresses this area [we already knew that but the CEM activities are too generic].
    - Draft has more specific guidance to evaluators that is based on technology type.
  - There is a gap in CC which could be addressed [more on this later].
    - Would involve changes to CC Part 3 requirements.
- Feedback on the feedback
  - The SCSA was sent in August 2012, feedback was in May 2013.
    - Consider a more lightweight process to provide earlier feedback.
    - Individual schemes could send feedback; CCMB sends consolidated, agreed-upon comments.
    - Since we strive for consensus, all comments are welcome.

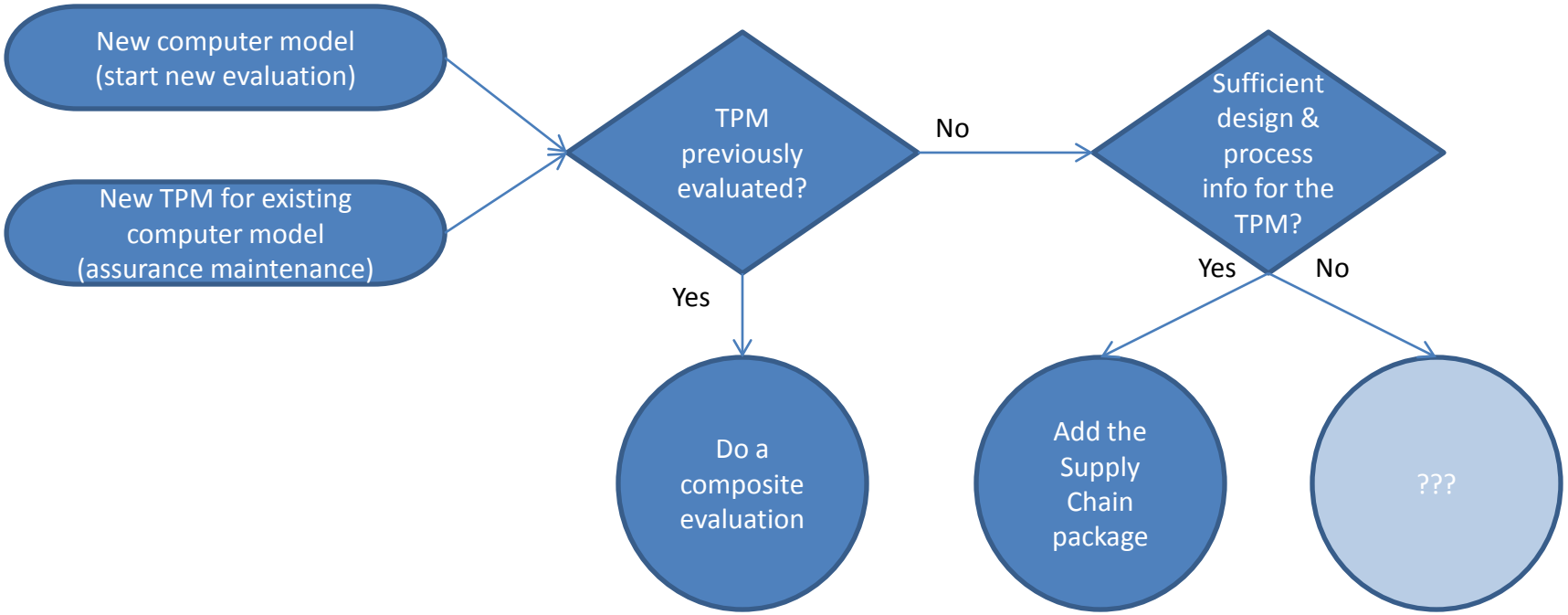
Current Status

Current status

- Supporting Document development
  - June, July 2013: Digested CCMB feedback.
  - July 2013: “Way ahead” proposal to start discussion for the 2013 draft.
  - July, August 2013: Discussed use cases for the next draft.
- Research and planning
  - June 2013: Proposal for how to manage trial evaluations.
  - July 2013: Literature survey for related topics, including smart-card and site certification.
- Collaboration tools
  - Moved from a separate site on TeamLab to an open site within the CCUF TeamLab portal.
- Membership
  - 83 individuals from 43 organizations.
  - 16 vendor orgs, 8 labs, 5 consultants, 6 schemes, 3 other government agencies, 3 non-profits.

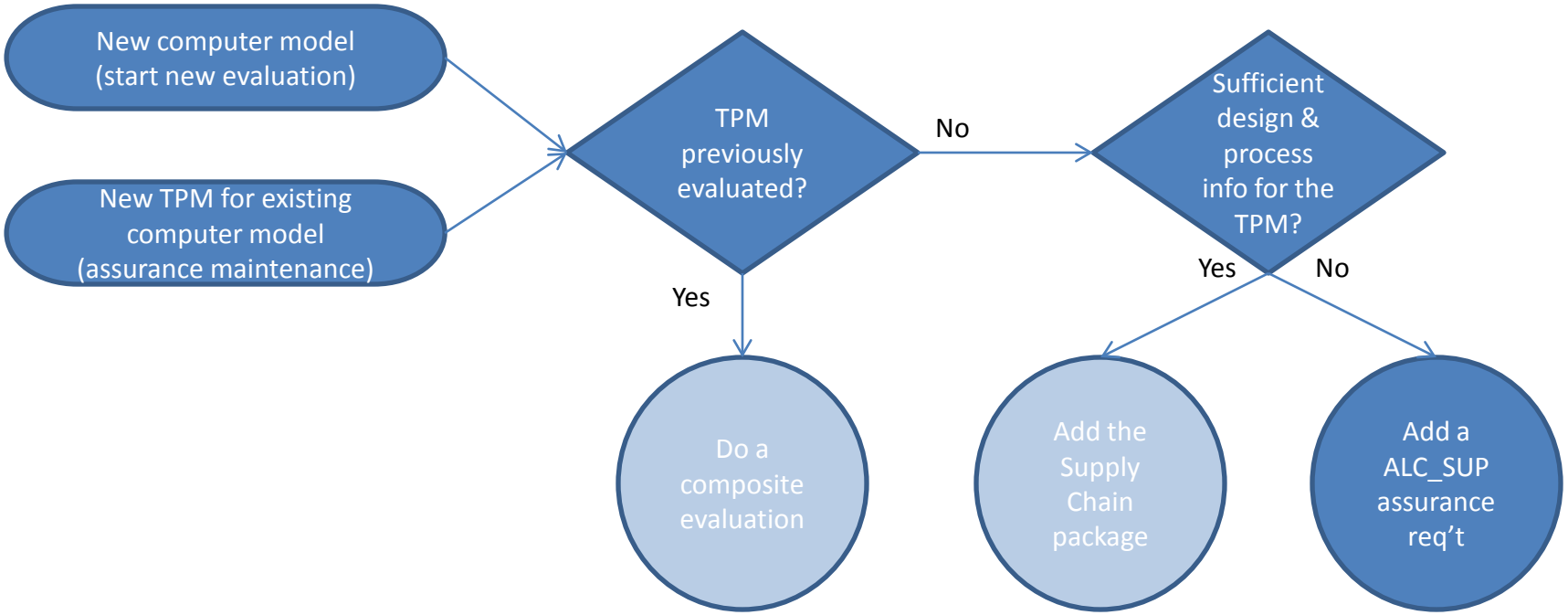
Use Case 1: Computer with a TPM

- Supporting Document has technology-specific guidance for the evaluator to check the developer processes to mitigate taint and counterfeit parts.
- It also defines a "Supply Chain Security" assurance package that contains existing requirements from ALC_CMS, ALC_CMS, ALC_LCD, ALC_DVS, and ALC_DEL.



Use Case 2: Computer with a TPM

- **The group is still discussing the applicability of this scenario.**
- There is a supported interface to use the TPM and procedures to check for counterfeit and tainted TPM, but little visibility into the TPM developer's practices. CC, as applied today, often treats this part of the product as outside the TOE. This is problematic.



One potential direction

- Axioms
  - Customers acquire products, not “TOE”s.
  - Evaluating a network of suppliers is not feasible due to depth or complexity of the supplier network.
  - Evaluating the product developer’s process has more impact than checking suppliers or obtaining evidence from suppliers solely for CC purposes.
- Under discussion: Gain incremental assurance through a new ALC_SUP family.
  - ALC_SUP.1.1D The supplier shall document and provide supply chain procedures addressed by the non-TOE configuration items supplier.
  - ALC_SUP.1C The supply chain documentation shall describe the internal configuration management procedures used to guarantee the integrity of the configuration item made available from third parties.
  - ALC_SUP.2C The supply chain documentation shall describe all the security measures that are necessary to protect the confidentiality and integrity of the configuration item in its development environment.
  - ALC_SUP.1.3C The supply chain documentation shall describe the procedures that are necessary to maintain security when distributing versions of the configuration item to the consumer.
  - ALC_SUP.1.4C The supply chain documentation shall describe the steps necessary to be performed by the TOE manufacturer or final user for the secure acceptance of the configuration items.

Planning for Trial Evaluations

Goals and metrics for trial

- Scope
  - New or on-going evaluation effort
- Objectives
  - Validate the requirements and assurance activates in the SCSA
  - Validate the assurance gained
- Metrics
- Determine the value

SCSA trial

- Kick-off / Completion
- Product
  - Hardware , Software or combination
    - Security critical components
- Participants
  - Developer
  - Lab
  - Scheme
  - CCDB
- Artifacts
  - Information Sharing
- Lessons Learned
- Recommendations

Conclusion

Next steps

- Continue to refine the TPM use cases, add new use cases for third-party crypto libraries and network appliances. [August, September]
- Decide if the workgroup recommends adding a ALC_SUP requirement to check configuration management practices for non-TOE parts of the product.
- Revise the 2012 supporting document

Wrap-up

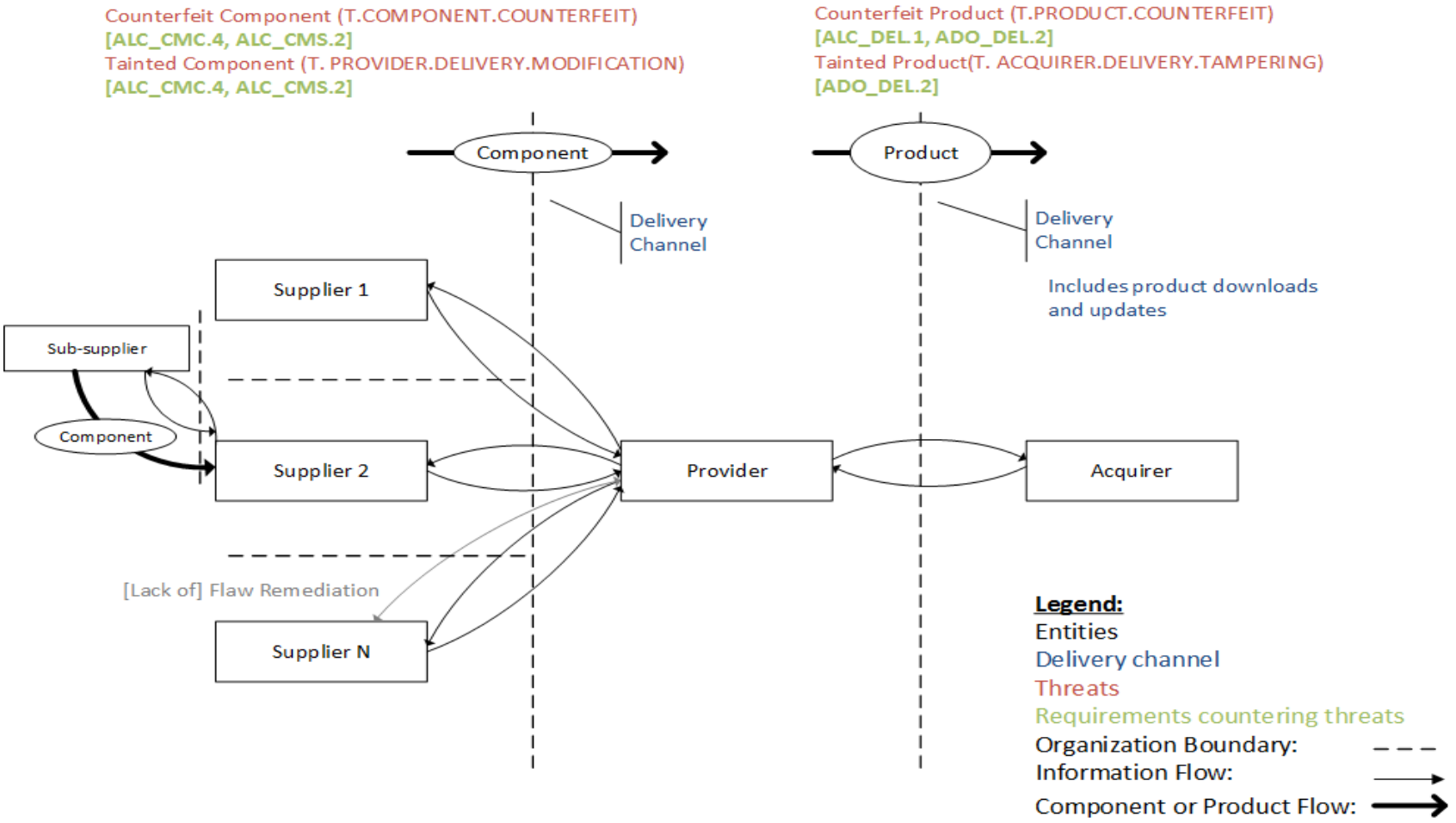
- Thank you for your time and attention.
- Visit https://ccusersforum.teamlab.com/products/projects/tmdocs.aspx?prjID=418795 to learn more.
- Please consider joining the workgroup.

Backup

ICCC Abstract

- This presentation is a status report from the Supply Chain Security Technical Workgroup which was formed in March 2012 with the approval of the Common Criteria Development Board, in order to produce a Common Criteria Supporting Document that technical communities can use and adapt for their protection profiles.
- The information and communications technology (ICT) supply chain has become increasingly complex, with logically long and geographically diverse routes, including multiple tiers of outsourcing. This leads to a significant increase in the number of organizations and individuals who "touch" a product, and thus, increases the likelihood that a product's integrity will be compromised. Ensuring that ICT products from commercial software and hardware providers are free from vulnerabilities introduced via the product developer's supply chain is an increasing concern which is manifested in proposed legislation and draft government regulations, as well as publicized attacks.
- Exacerbating those concerns is the fact that awareness of supply chain risks and potential mitigations is not widely shared within the ICT industry, academia, government regulators, and product acquirers.
- The product lifecycle and its corresponding supply chain aspects extend from design to sourcing, manufacturing, distribution, delivery, installation, support, and end-of-life. Each stage presents potential threats of attack: the introduction of counterfeit products or components; elements of product taint, for example via malware or an integrity breach; disruptions to logistics and delivery; as well as tampered communications between the product developer and the customer or the customer and supplier.
- The August 2012 Supply Chain Security Supporting Document described several of these threats in more detail, specified additional threats, suggested assurance requirements, and recommended best practices for product manufacturers, evaluators, certifiers and end users.
- This presentation is a status report from the workgroup on progress since the 2012 ICCC.

Current Threat Model



Security Threats to a Software or Hardware Supply Chain