CYGNACOM
SOLUTIONS

Scoping the TOE

Nithya Rachamadugu
September 24, 2008

Topics

- Introduction
- TOE boundary discussions
- Conclusion

Introduction

- Over the past years several products have been evaluated under the CC paradigm.
- Products and technologies have evolved and so are the ways products are developed, built and sold.
- The drive is to be build efficient, smaller modules with more re-usability.
- More and more COTS products are used and bundled for easier deployment.

Introduction (cont.)

- Common Criteria evaluation of bundled products has become complex and challenging. This presentation is a forum focusing on some of the key questions that arise in these situations.
- There is no single answer to these scenarios and not all questions have an answer. This presentation is an attempt to bring attention to these issues.

Introduction (cont.)

Topics

- Applications bundled with environmental 3rd party products
- Software sold as appliances
- Automatic software updates
- TOE built as target OEM candidates
- Crypto testing for non-crypto centric products
- High availability versus load balancing

Applications bundled with environmental 3rd party products

Many products are now bundled as packages that include:

- Operating systems
- Databases like Oracle, Sybase
- Communication protocols like SSL/TLS

Applications bundled with environmental 3rd party products (cont.)

Advantages:

- TOE works as a whole in a known environment
- Ease of installation
- No additional license and procurement for the consumer
- Ease of product support

Applications bundled with environmental 3rd party products (cont.)

Challenges:

- Is TOE boundary only the product or the whole bundled package?
- Perhaps TSF is only the product and TOE is the whole bundled package?
- Is interaction with the 3rd party software and hardware an internal or external interface?
- Do patches to 3rd party software or hardware put the product out of its evaluated configuration?
- How often should assurance maintenance be conducted for environmental changes?

Product as appliance

- Products are bundled with hardware

Advantages:

- Customized environment
- Tested as one unit
- Scalability
- Cheaper for the customer
- One stop shopping for the customer
- Easier support

Product as appliance (cont.)

Challenges:

- Is the hardware included or excluded from the evaluation?
- Is the hardware part of the product, but not part of the TOE?
- Is the hardware part of the TOE, but is not the TSF?
- Do we look at the hardware diagrams at EAL4?
- Can the developer sell the CC software on different hardware without re-evaluating it?

Automatic software updates

- Patch managements and vulnerability assessment products sometimes have automatic software updates

Advantages:

- Bug fixes delivered immediately
- Bug fixes applied ASAP
- Transparent to customer
- Easier support

Automatic software updates (cont.)

Challenge:

- Patches put the configuration out of the CC evaluated configuration

Would either of these approaches be acceptable?

- Apply patches manually
- Apply assurance continuity to patches

TOE Built as Target OEM Candidates

- Software built with intentions to sell to multiple vendors for use as OEM (Original Equipment Manufacture)
- OEMs are products bought from another manufacturer and resold or incorporated into a product and then sold under a different brand name.

TOE Built as Target OEM Candidates (cont.)

Advantages for the original developer:

- Vendor sells to multiple corporations expanding their market
- Focused marketing
- Typically developed by small companies with limited resources

TOE Built as Target OEM Candidates (cont.)

Advantages for acquiring corporation:

- Cheaper to buy product than to develop it
- Become an Value Added Reseller (VAR)
- Leverages its existing market and marketing to sell the product
- Higher profit
- Support and maintenance from the developer

TOE Built as Target OEM Candidates (cont.)

Challenges/issues if the original developer wants the original product CC evaluated:

- Have to choose a hardware, OS and other environmental elements for the evaluation
- Can the OS and hardware be excluded from the evaluation?
- Can the acquiring corporation claim the OEM product as CC evaluated?

TOE built as target OEM candidates (cont.)

Challenges if the acquiring corporation wants the original [OEM] product CC evaluated:

- If CC certificate has been issued to the original developer, can the acquiring corporation claim CC?
- Will the corporation have to recertify?
- Could this be a component evaluation?
- Does assurance continuity apply?

Crypto for Non-Crypto Products

- Some products use crypto features, but are not crypto-centric
  - i.e., main functionality of the product does not involve crypto
- E.g., Product uses SSL/TLS to protect communications between TOE components such as the server and an agent

Crypto for Non-Crypto Products (cont.)

Challenges:

- Should communication protocols be part of the TOE?
- Should there be an SFR in the TOE or is it sufficient to describe the use of the communications protocol in Description and TSS sections?
- Should there be SFRs defined in both the TOE and the environment?

Crypto for Non-Crypto Products (cont.)

Challenges:

- Which SFRs should be used to describe protection being provided?
  - FDP_UCT Inter-TSF user data confidentiality transfer protection
  - FDP_UIT Inter-TSF user data integrity transfer protection
  - FPT_ITT Internal
  - FPT_ITC Inter-TSF trusted channel
  - FTP_TRP Trusted path
  - FPT_ITT Internal TOE TSF data transfer

Crypto for Non-Crypto Products (cont.)

Challenges:

- Should there be a crypto SFR?
  - E.g., FCS_COP - Cryptographic Operations
- What about the dependencies?
  - FCS_CKM.1 – Key generation
  - FCS_CKM.4 – Key destruction

High availability vs Load balancing

- High availability: system designed to ensure a degree of operational continuity
- Load balancing: distribution of work load over multiple resources for better performance
- These concepts are sometimes confused:
  - Load balancing is not the same as high availability.

High Availability vs Load balancing (cont.)

- In load balancing, if one resource fails another takes the load,
  - All resources could fail so high availability is not enforced
- Should load balancing be included in the Logical TOE Boundary?
  - FRU_FLT Fault tolerance can be used for High availability?
  - Is there an SFR for load balancing?

Conclusions

- Commercial packaging and industry present some interesting and complex questions for Common Criteria evaluations.
- No one solution exists!
- A solution should be agreed upon so the vendor can leverage of the benefits of the certification

Thanks!

Questions : ???

Thank you!

Contact: Nithya Rachamadugu
Director, CygnaCom CCTL, USA
Nithya@cygnacom.com
703-270-3551