Application Brief

Analyzing Strength of Security

The world is full of examples of bad security. Developers of systems containing information in need of protection will understand how easily security mechanisms that appear to be impenetrable can contain subtle flaws that can be exploited by a determined attacker. It is also often difficult to determine if those who profess themselves to be experts in complete security systems have actually developed and maintained that broad skill set or have simply learned basic concepts and memorized impressive buzzwords.

One way to avoid these problems is to have systems evaluated by an independent organization whose results can be trusted and verified. An international group of government and commercial organizations has created the Common Criteria Evaluation and Validation Scheme (CCEVS) to perform that service for a wide range of software and hardware products. A challenge to that mandate comes from the breadth of products needing their security implementations evaluated, the range of environments where these products reside, and the increasing sophistication of the attack methods used to target sensitive information in the products. The CCEVS addresses this challenge by establishing a tiered system of Evaluation Assurance Levels (EAL) that set limits to the amount of time, expertise, cost, and equipment against which a product must maintain security protections.

A product with an EAL4 evaluation must defend against significantly more complex and expensive attacks than one evaluated at a lower level. Secure IC product evaluations by labs who have mastered these methods can be expected to take several months to a year to complete, and can cost hundreds of thousands of dollars. This situation focuses a spotlight on the challenges faced by system developers who are consumers of security ICs and who need to make informed choices on IC-based security systems at a reasonable cost.

One of these challenges is the uncertainty about exactly what is certified by a Common Criteria (CC) evaluation. A passing CC evaluation does not guarantee absolute security, and, in fact, successful attacks against certified products have been publicly documented. The evaluation lab conducts tests that target only those specific security functions individually detailed in the supporting documentation. Security functions not included in the documentation are not tested, and tests are conducted only at a level consistent with the target EAL.

EAL definitions are established by the CCEVS and set thresholds for the expected time, expertise, equipment, and costs associated with tests corresponding to each EAL. While some protections are specifically mandated by the Joint Interpretation Lab (JIL) evaluation guidance, many security functions must be identified by the IC manufacturer and documented in the Protection Profile, Security Target, Security Architecture, Functional Specification, and other documents required by the CC evaluation process. The Protection Profile (PP), in particular, which serves as a summary document itemizing the list of security functions covered by an evaluation, can suffer from inadequate coverage of the functions critical to a complete security system. An unfortunate consequence of the CC infrastructure is that the final responsibility for assuring complete coverage lies with the end consumer of the evaluated product – the system designer

tasked with integrating the security IC into a larger system. No checks exist to determine which functions may be missing or poorly defined in the PP. For this reason, the most effective PP documents are those generated by third parties, such as standards committees, who are motivated to perform a broad security system analysis.

Atmel® has performed CC evaluations of multiple security ICs against third party PP documents whose coverage of security features has been vetted by industry experts. This experience has enabled Atmel to directly apply knowledge gained in validation of one product to others within its secure products family that may not be subjected to the formal security evaluation process. These products benefit from the scrutiny and lessons learned through a formal evaluation process without incurring the costs associated with repeated evaluations of the same security implementation. Familiarity with the development of products that have successfully completed high EAL evaluations means the Atmel engineering team has developed experience in all phases of the security evaluation process:

- The identification and documentation of the entire range of critical security functions needed to combat attacks in real-world system environments
- The development of hardware and software components that can mitigate attacks targeting these security functions
- The execution of tests and attack methods at a level equivalent to those of certification evaluation laboratories
- The integration of hardware, firmware, and software solutions from previously certified products into new chips that will not complete a formal evaluation

These skills and techniques demonstrate an in-depth knowledge of security concepts by the Atmel secure products development, engineering, and manufacturing teams. The documented completion of CC evaluations of flagship security chips, such as the Trusted Platform Module (TPM), prove the capability of Atmel performing internal design, integration, characterization, and validation of genuinely secure IC solutions. The transfer of security strategies and evaluated component modules from unevaluated products has enabled Atmel to build a family of security products that meet both the level of protection and pricing requirements of customers.

1. Revision History

Doc. rev.	Date	Comments
8754A	04/2011	Initial document release

Atmel Corporation
2325 Orchard Parkway
San Jose, CA 95131
USA
Tel: (+1)(408) 441-0311
Fax: (+1)(408) 487-2600
www.atmel.com

Atmel Asia Limited
Unit 01-5 & 16, 19F
BEA Tower, Millennium City 5
418 Kwun Tong Road
Kwun Tong, Kowloon
HONG KONG
Tel: (+852) 2245-6100
Fax: (+852) 2722-1369

Atmel Munich GmbH
Business Campus
Parkring 4
D-85748 Garching b. Munich
GERMANY
Tel: (+49) 89-31970-0
Fax: (+49) 89-3194621

Atmel Japan
9F, Tonetsu Shinkawa Bldg.
1-24-8 Shinkawa
Chuo-ku, Tokyo 104-0033
JAPAN
Tel: (+81)(3) 3523-3551
Fax: (+81)(3) 3523-7581