



ISO/IEC JTC 1/SC 27 **N 7790**

ISO/IEC JTC 1/SC 27/WG 3 **N 990**

REPLACES: N

**ISO/IEC JTC 1/SC 27**

**Information technology - Security techniques**

**Secretariat: DIN, Germany**

**DOC. TYPE:** other

**TITLE:** Presentation on Tamper Protection Study Period

**SOURCE:** 38<sup>th</sup> SC 27/WG 3 meeting

**DATE:** 2009-05-05

**PROJECT:** -

**STATUS:** This document was made available at the 38th SC 27/WG 3 meeting held in Beijing, China, 4th – 8th May 2009. It is circulated within SC 27 for information.

**ACTION:** FYI

**DUE DATE:**

**DISTRIBUTION:** P-, O-, and L- Members  
W. Fumy, SC 27 Chairman, M. De Soete, SC 27 Vice Chair  
E. Humphreys, K. Naemura, M. Ohlin, M.C. Kang, K. Rannenber, WG-Conveners

**MEDIUM:** Server

**NO. OF PAGES:** 1 + 9



# **Report on the WG 3 STUDY PERIOD ON TAMPER PROTECTION REQUIREMENTS AND EVALUATION**

Call for contributions

N7403

NB contributions

N7604



## Background

Anti-tampering measures have their application in areas of the IT security field (protection of hardware resources, transport devices for passwords and cryptographic keys, biometric sensor devices etc), and as such are already present in the architectural aspects of ISO/IEC 15408 assurance components (ADV\_ARC) and of relevance to ISO/IEC 19790.

The exclusion from the existing security evaluation criteria of hardware countermeasures has created a grey area, in some cases clarified by the application of technology specific supporting documents, as is the case in the evaluation of smart cards. In these cases, the hardware-based supporting countermeasures that provide anti-tamper functionality are being specified and addressed as part of the device security evaluation.



The application of security requirements and evaluation using the ISO/IEC 15408 is broadening, for example to provide coverage to different regulations and sector specific approval schemes based on similar devices (e.g. passports, id-cards), and also based on different devices (e.g. tachographs, pin-entry devices, points of interaction in payment systems, etc), all of them having a deep dependency of their provided security in the hardware-based anti-tamper measures.

A Study Period concerning tamper protection requirements and evaluation has been initiated by ISO/IEC JTC1 SC 27/WG 3. Potential outcomes for the Study Period might include an NWI for a Standard to address this topic area



The NB's of SC 27 have been asked to provide input to this Study Period. Specifically the following issues may be addressed:

- ✓ the current treatment to hardware based anti-tamper mechanisms in the security evaluation of IT, and how security assurance can be stated for products where the security environment requires the support of such mechanisms;
- ✓ the need to provide extensions to existing standards related to the security requirements specification and evaluation criteria to address the relationship between IT and underlying hardware, including security properties and mechanisms, which encompass tamper protection;
- ✓ the need to harmonize the tamper protection requirements and evaluation with existing standards (namely ISO/IEC 15408, ISO/IEC 19790), if applicable.



Two responses have been received, namely

AU1

AU NB thinks that standardization of what tamper protection is defending and what should happen in the event that it is triggered is fine, but when it comes down to the particulars of the mechanisms employed many vendors may feel they are sensitive information that differentiates their products from those of their competitors.

Such information is typically guarded jealously by its inventors, and only shared with accreditation laboratories under heavy non-disclosure agreements.



If a standard for tamper protection requirements is to be created care must be taken to ensure the scope and content of such a document does not neuter the very purpose any such mechanisms were created in the first place.

- ✓ Who is the target audience for this document?
- ✓ What is the scope of such a document, and does its existence reduce or enhance IT security?
- ✓ If limited by commercial sensitivity considerations, what real purpose would it serve?
- ✓ If all secrets are revealed are the effective lifespan of such measures reduced?



✓ How such a document would be managed as measures detailed are systematically defeated perhaps by entities outside of the industry is also something to be considered.

We would suggest the best participants for such a group would be representatives from the accreditation labs themselves.

We are not convinced this is a good idea.



## UK CONTRIBUTION TO WG 3 STUDY PERIOD ON TAMPER PROTECTION

The UK is pleased to contribute the attached University of Cambridge Computer Laboratory Technical Report UCAM-CL-TR-711

*Thinking inside the box: system- level failures of tamper proofing to the WG 3 Study Period on Tamper Protection.*

Although all Computer Laboratory Technical Reports are freely available via the Internet, their use is subject to certain restrictions. We are pleased to confirm, however, that Professor Anderson has explicitly agreed on behalf of the authors that this Report may be used as a source document in the development of any future WG3 Standard. The UK National Body hopes that the successful attacks described in this Report will help to provoke discussion of how tamper proofing may sensibly be measured and evaluated.



**Discussion welcomed**

**Thank you.  
CCN**