Annex F:
Non-Invasive Attack Methods for FIPS PUB 140-3,
Security Requirements for Cryptographic Modules

September 10, 2009
Draft

NIST Computer Security Division

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

U.S. Department of Commerce
Secretary Gary Locke

Technology Administration
Under Secretary for Technology

National Institute of Standards and Technology
Deputy Director Patrick D. Gallagher

Annex F: Test Metrics
for FIPS PUB 140-3,
Security Requirements for Cryptographic Modules

1. Introduction

Federal Information Processing Standards Publication (FIPS PUB) 140-3, Security Requirements for Cryptographic Modules, specifies the security requirements that are to be satisfied by the cryptographic module utilized within a security system protecting sensitive information within computer and telecommunications systems (including voice systems). The standard provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3 and Level 4. These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of the cryptographic module. These areas include the following:

1. Cryptographic Module Specification
2. Cryptographic Module Interfaces
3. Roles, Authentication and Services
4. Software/Firmware Security
5. Operating Environment
6. Physical Security
7. Physical Security - Non-Invasive Attacks
8. Sensitive Security Parameter Management
9. Self-Tests
10. Life-Cycle Assurance
11. Mitigation of Other Attacks

The Cryptographic Module Validation Program (CMVP - www.nist.gov/cmvp) validates cryptographic modules for conformance to FIPS PUB 140-3 and other cryptography based standards. The CMVP is a joint effort between NIST and the Communications Security Establishment Canada (CSEC - www.cse-cst.gc.ca). Modules validated as conforming to FIPS PUB 140-3 are accepted by the Federal agencies of both countries for the protection of sensitive information (United States) or Designated information (Canada).

Under the CMVP, vendors of cryptographic modules use independent, accredited testing laboratories to have their modules tested. Organizations wishing to have validations performed would contract with the laboratories for the required services.

2. Purpose

The purpose of this document is to list non-invasive attack methods applicable to FIPS PUB 140-3.

Table of Contents

ANNEX F: NON-INVASIVE ATTACK METHODS

Annex F specifies particular non-invasive attack methods for determining conformance to FIPS PUB 140-3. For each applicable *shall* statement from FIPS 140-3, "*Security Requirements for Cryptographic Modules*", the validation authority may provide further test methods information.

Definitions

Correlation Power Analysis (CPA): an extended variant of the basic DPA, which uses a more precise power model such as the hamming weight or hamming distance model, detecting the highest correlation between measured power consumption and calculated power based on the model with each guessed key.

Differential Power Analysis (DPA): an analysis of the variations of the electrical power consumption of a cryptographic module, using advanced statistical methods and/or other techniques on a large number of measured power consumption values for the purpose of extracting the keys used in a cryptographic algorithm. Power models are generated based on assumptions about the targeted key and tested against measurements. The highest correlation reveals the key.

Differential Electro-Magnetic Analysis (DEMA): an analysis of the electro-magnetic emanation or the variations of the proximity magnetic field due to the electrical activity on a cryptographic module, using the same statistical techniques on the measured data and for the same purpose as those for DPA.

Simple Power Analysis (SPA): a direct (primarily visual) analysis of patterns of instruction execution (or execution of individual instructions), obtained through monitoring the variations in electrical power consumption of a cryptographic module, for the purpose of revealing the features and implementations of cryptographic algorithms and subsequently the values of cryptographic keys.

Simple Electro-Magnetic Analysis (SEMA): an analysis of the electro-magnetic emanation or the variations of the proximity magnetic field due to the electrical activity on a cryptographic module, using the same inspection techniques on the measured data and for the same purpose as those for SPA.

Timing Analysis (TA): an analysis of the variations of the response or execution time of a matching function or an operation in a cryptographic algorithm, which may reveal knowledge of or about a critical security parameter such as a PIN or cryptographic key.

Acronyms

CPA	Correlation Power Analysis
DEMA	Differential Electromagnetic Analysis
DPA	Differential Power Analysis
SEMA	Simple Electromagnetic Analysis
SPA	Simple Power Analysis
TA	Timing Analysis

Non-Invasive Attack Methods and Associated Security Functions

The non-invasive attack methods that FIPS 140-3 addresses are: Simple Power Analysis (SPA), Simple Electro-Magnetic Analysis (SEMA), Differential Power Analysis (DPA), Differential Electro-Magnetic Analysis (DEMA), and Timing Analysis (TA). The SPA and SEMA attack methods that FIPS 140-3 addresses include some extensions to basic SPA and SEMA attacks, such as the so called template attack. The DPA and DEMA attack methods that FIPS 140-3 addresses include some extensions to basic DPA and DEMA attacks, such as so called Correlation Power Analysis (CPA) and higher-order DPA attacks.

Within the scope of the security requirements specified in FIPS 140-3, each of these attack methods is associated with the particular security functions which use the CSPs targeted by the attacks. The associations are listed in Table F.1. Other non-invasive attacks and other associations between the attack methods and security functions may exist but defense against them is currently considered optional at all Security Levels. This Annex may be updated periodically to include within the scope of this standard new non-invasive attacks or associations between attack methods and security functions.

Non-Invasive Attack Methods	Security Functions / Algorithms
SPA and SEMA	Approved or Allowed asymmetric cryptographic algorithms
DPA and DEMA	Approved or Allowed symmetric cryptographic algorithms
TA	Approved or Allowed asymmetric cryptographic algorithms Approved or Allowed symmetric cryptographic algorithms Authentication mechanisms that control access to the module

Table F.1 : Associations between non-invasive attack methods and security functions

Approved symmetric and asymmetric cryptographic algorithms are listed in Annex A. Allowed security functions addressed by this standard are listed in Annex B.

Document Revisions

Date	Change
03/02/2009	**Initial Draft**

End of Document