# ISAE Master – 2012-2013
# Embedded Systems and Computer Security module

## Evaluation

Evaluation will be based on a written report concerning one specific topic (possible examples following).

Modus operandi :

- personal report (one writer)
- 2-3 pp. length
- a specific focus should be selected early during january 2013 (approval by professor)
- contact : rodolphe.ortalo@free.fr or rodolphe.ortalo@carsat-mp.fr (answer within 24/48h)
- final report due date at the beginning of march 2013 (*to be confirmed with ISAE*).

**NB :** Of course, these topics are to be investigated in a computer security-oriented approach. A personal presentation is requested (external references must be detailed in order to be positively evaluated – citations must be clearly indicated and raw copypasting must be avoided).

As a final note, given the overall domain of investigation, security, keep in mind that any dangerous activity will be *sanctionned*, whatever the technical skills or knowledge that it may demonstrate.

Suggestion list :

1 Students can choose their own subject of investigation, prior approval is mandatory.

2 Source code audit related to a cryptographic or security software component (in *open source*), for example : GnuPG, OpenSSL, GNUTLS, internal cryptographi modules of the Linux or a BSD kernel or a more general application subsystem (Firefox, Apache 2, Android subsystem, etc.)

3 Embedded systems security alerts management.

4 Identification and details of Bluetooth security mechanisms.

5 Identification and details of security mechanisms in any other field wireless protocol where information is available (Bluetooth ; please check full information availability first)

6 Identification of security mechanisms in one of the WiFi protocols (802.11 a/b/g/n*)*.

7 Latest developments concerning cryptographic hash functions (what about SHA3 ?).

8 Presentation of one of the unfortunate candidates of round 3 NIST SHA3 competition.

9 Biometrics techniques in embedded systems: perspective.

10 Comparison of embedded systems and desktop or server systems security requirements.

11 Alternatives to (inthefield) security updates.

12 Attempt at the definition of highlevel security requirements for a modern mobile phone (GSM, GPS, WiFi)

13 Presentation and analysis of DNSSEC.

14 Usage of databaserelated software in embedded systems.

15 TPM implementation efforts surrounding linux.

16 UEFI bios security mechanisms.

17 Latest news with respect to GSM security (A5 cipher family or base station components or latest attacks publicly presented). Ref.: openbsc.gnumonks.org

18 Security mechanisms associated to thirdparty application publication either on Android, Symbian or iPhone OS.

19 Analysis of other securityrelated features or information available on one of these mobile phones operating systems.

20 Security requirements, standards or technologies related to an electronic identity card.

21 Security requirements, standards or technologies related to voting machines.

22 Smartcardbased authentication software available on the Internet.

23 Study of sparse (http://lwn.net/Articles/87538/) annotations with respect to Linux kernel security faults detection.

24 Study of static analysis software approch or tool with respect to security fault prevention (LLVM, GCC, etc.).

25 Inventory and analysis (volumetry, interest) of various security alerts providers (CERT, vendors, etc.). Focus on comparison criteria definition or specific areas.

26 Backdoors implementation techniques.

27 Trojan horse implementation (with a specific focuss on embedded systems).

28 Attack development within metasploit (www.metasploit.com).

29 Comparison of dynamic linkers (.so, a.out, DLL) with respect to security issues. (How does program text load before execution?)

30 Android subsystem security study.

31 Ipsec operation.

32 Comparison of directory technologies security (NIS+, LDAP, A.D., others?).