Metodologie di progetto di sistemi hardware/software sicuri mission-critical: follow up (2)

P. Gubian, A. Savoldi

Dipartimento di Elettronica per l'Automazione, Università di Brescia
Via Branze, 38 - 25123 Brescia

Il problema della sicurezza di funzionamento, intesa sia come garanzia della correttezza delle operazioni che dell'impossibilità di alterare il funzionamento stesso in maniera più o meno volontaria, dei sistemi complessi hardware/software oggi in uso è sempre più sentito e importante, specie nel momento in cui si vuole assegnare ai sistemi stessi funzioni molto critiche ed affidare ad essi l'incolumità stessa degli esseri umani. Nonostante molti sforzi siano in corso al fine di ottenere risposte complete ed affidabili, non esistono ad oggi metodologie d'indagine che consentano di certificare la sicurezza di tali sistemi.

Nella fattispecie si è rivolta l'attenzione alle SIM/USIM card. La sicurezza di tali sistemi può essere valutata sia sul piano hardware che su quello software. Dal punto di vista hardware si avverte, in modo sempre più crescente, l'esigenza di avere delle metodologie costruttive che siano tali da rendere il dispositivo robusto al *reverse engineering* a livello fisico. Sul fronte software vi è una continua ricerca volta alla creazione di sistemi operativi implementati con metodologie di verifica del codice sorgente. Inoltre sono in fase di studio sistemi di tipo sandbox che permettono l'esecuzione controllata di applicazioni installabili su smart card, il che è fondamentale per prevenire potenziali attacchi da parte di codice maligno.

Nell'ambito delle telecomunicazioni, un'applicazione della smart card che ha indubbiamente preso piede è quella della SIM/USIM card. L'obbiettivo della ricerca in questo ambito è quello di sviluppare strumenti open-source [2][3] idonei all'acquisizione di tutti i dati digitali osservabili utili per un'analisi forense. A tal proposito è stato implementato uno strumento software, in linguaggio ANSI C e Perl, preposto all'acquisizione ed alla successiva interpretazione del contenuto osservabile di una SIM/USIM card. Questo si rivela estremamente utile per derivare elementi probatori che sono fondamentali nell'ambito di un'indagine giudiziaria.

La ricerca si è focalizzata successivamente sugli aspetti caratterizzanti le SIM/USIM card, in particolare sulla reale costituzione del filesystem di questi dispositivi. Da un'accurata analisi si è determinata la reale conformazione di tale filesystem mettendo in risalto alcune problematiche fondamentali relative alla sicurezza di tali sistemi. Infatti, a dispetto di quanto menzionato dagli standard internazionali di riferimento [4], vi sono locazioni non standard all'interno del filesystem delle SIM/USIM card, analoghe allo *slack space* rinvenibile negli hard disk dei tradizionali calcolatori, usabili per memorizzare informazione arbitraria e quindi rendendo tali dispositivi usabili come *covert channel*, vale a dire utilizzabili per trasmettere informazione arbitraria tramite un mezzo non preposto a tal fine [5][6][7][9][10].

Un altro promettente settore oggetto dell'indagine è stato quello relativo alla steganalisi delle immagini jpeg. E' noto che un'immagine fotografica digitale di questo formato può essere utilizzata come *covert channel*, vale a dire come vettore per dati arbitrari come ad esempio un immagine od un file testuale. A fronte dei possibili rischi derivanti da un

abuso di queste tecniche di *data hiding* è doveroso dare una risposta mediante lo studio di sistemi [8][11] che possano dire, con un ragionevole grado di accuratezza, se l'immagine, oggetto dell'indagine, abbia o meno evidenze digitali occultate al proprio interno. Un interessante estensione di questo principio è stata applicata al dominio dei sistemi embedded [13][14][15][16][17][18][19][20][21].

Bibliografia:

[1] Wolfgang Rankal, Wolfgang Effing, Smart Card Handbook. Third Edition, John Wiley & Sons, Ltd.

[2] CARRIER B.: Defining Digital Forensic Examination and Analysis Tool Using Abstraction Layers, International journal of Digital Evidence, vol. 1, issue 4, 2003.

[3] DFRWS: A roadmap for digital forensic research, DFRWS TECHNICAL REPORT DTR-T001-01 FINAL, 2001.

[4] ETSI TS 100 977 v8.13.0: Digital cellular telecommunications system (Phase 2+), http://webapp.etsi.org/action/PU/20050628/ts_100977v081300p.pdf

[5] National Computer Security Center: A Guide to Understanding Covert Channel Analysis of Trusted System , http://www.radium.ncsc.mil/tpep/library/rainbow/NCSC-TG-030.html

[6] F.Casadei, A.Savoldi, P.Gubian, **SIMBrush: an Open-Source Tool for GSM and UMTS Forensic Analysis**, in Proceeding of First International Workshop on Systematic Approaches to Digital Forensic Engineering 2005, Taipei, TW, 2005 (pagg. 105-119)

[7] F. Casadei, A. Savoldi, and P. Gubian. **Forensics and SIM Cards: an Overview**. On International Journal of Digital Evidence. Fall 2006, Volume 6, Issue 1

[8] A.Savoldi and P.Gubian. **A Methodology to Improve the Detection Accuracy in Digital Steganalysis**. In Proceedings of International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Pasadena, Proc. IEEE, pgg. 373-376, 18-20 December 2006.

[9] A.Savoldi and P.Gubian. **SIM and USIM Filesystem: a Forensics Perspective**. In Proceedings of Symposium on Applied Computing, Computer Forensics Track, Seoul, Proc. ACM, pgg. 181-187, 11-15 March 2007.

[10] A.Savoldi and P.Gubian. **Data Hiding in SIM/USIM Card: A Steganographic Approach**. In Proceeding of Second International Workshop on Systematic Approaches to Digital Forensic Engineering, Seattle, WA, Proc. IEEE, pgg. 86-97, 10-12 April 2007.

[11] A.Savoldi and P.Gubian. **Blind Multi-Class Steganalysis System Using Wavelet Statistics**. To appear in Proceedings of International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Kaohsiung, TW, Proc. IEEE, 27-29 November 2007 (Invited paper).

[12] A.Savoldi and P.Gubian. **Data Hiding and Recovery on Windows CE Based Handheld Devices**. In Proceedings of Fourth Annual IFIP WG 11.9 International Conference on Digital Forensics (Chapter book), Kyoto University, Kyoto, Japan, Proc. Springer, January 27 - 30, 2008.

[13] A.Savoldi and P.Gubian. **Logical and Physical Data Collection of Windows CE Based Portable Devices**. In Proceedings of Symposium on Applied Computing (ACM SAC 2008), Fortaleza - Brazil, March 16 - 20, 2008.

[14] B.Park, A.Savoldi, P.Gubian, J.Park, S.Lee and S.Lee. **Recovery of Damaged Compressed Files for Digital Forensics Purposes**. In Proceedings of international conference on Multimedia and Ubiquitous Engineering (MUE 2008), Busan, Korea, Proc. IEEE, April 24-26, 2008.

[15] J.Choi, A.Savoldi, P.Gubian, S.Lee and S.Lee. **Live Forensic Analysis of a Compromised Linux System Using LECT (Linux Evidence Collection Tool).** In proceedings of international conference on Information Security and Assurance (ISA 2008), Busan, Korea, Proc. IEEE, April 24-26, 2008.

[16] A.Savoldi and P.Gubian. **Towards the Virtual Memory Reconstruction for Windows Live Forensic Purpose.** In proceeding of Third International Workshop on Systematic Approaches to Digital Forensic Engineering, Oakland, CA, Proc. IEEE, 22 May 2008.

[17] A.Savoldi and P.Gubian. **Symbian Forensics: An Overview**. In Proceedings of International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Harbin, China, Proc. IEEE, 15-17 August 2008 (Invited paper).

[18] L..Pan, A.Savoldi and P.Gubian. **Measure of Integrity Leakage in Live Forensic Context**. In Proceedings of International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Harbin, China, Proc. IEEE, 15-17 August 2008 (Invited paper).

[19] K.Lee, A.Savoldi, P.Gubian, K.Lim, S.Lee, and S.J.Lee, **Methodologies for Detecting Covert Database**. In Proceedings of International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Harbin, China, Proc. IEEE, 15-17 August 2008 (Invited paper).

[20] S.Yun, A.Savoldi, P.Gubian, Y.Kim, S.Lee, and S.Lee. **Design and Implementation of a Tool for System Restore Point Analysis**. To appear in Proceedings of International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Harbin, China, Proc. IEEE, 15-17 August 2008 (Invited paper).

[21] Y.Kim, A.Savoldi, P.Gubian, H.Lee, S.Yun, J.Choi, S.Lee, and J.Lim. **Design and Implementation of a Tool for Detecting Accounting Frauds**. To appear in Proceedings of International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Harbin, China, Proc. IEEE, 15-17 August 2008 (Invited paper).