METODOLOGIE DI PROGETTO DI SISTEMI HARDWARE/SOFTWARE SICURI MISSION-CRITICAL

Paolo Gubian, Andrea Savoldi

Dipartimento di Ingegneria dell'Informazione (DII), 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.

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 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, 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.

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.

L'indagine è poi proseguita con lo studio delle caratteristiche hardware e software di importanti sistemi digitali *embedded* quali sono i moderni dispositivi palmari e smartphone. Per ciascuna di queste due categorie è stata svolta una indagine approfondita sulle possibilità di intervenire con metodi sia elettrici che via software per nascondere informazioni in modo non rilevabile. Tali risultati sono stati accompagnati dalla corrispondente diffusione dello strumento di rilievo e rimozione della informazione stessa; tutti gli strumenti hanno le caratteristiche necessarie per un impiego in sede forense, in termini di documentabilità e riproducibilità dei risultati.

Referenze

[01] 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, pp. 105-119.

[02] 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.

[03] 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.

[04] 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, pp. 16-20, 2008.

[05] 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.

[06] 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.

[07] 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.

[08] 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).

[09] 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).

[10] 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).

[11] 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).

[12] 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).

[13] A. Savoldi, P. Gubian - Volatile Memory Collection and Analysis for Windows Mission-Critical Computer Systems - International Journal of Digital Crime and Forensics Vol. 1 No. 3 July-September 2009, pp. 42-61.