UNIVERSITÀ CAMPUS BIO-MEDICO DI ROMA E CONSORZIO NITEL
MASTER UNIVERSITARIO DI II LIVELLO IN HOMELAND SECURITY
ANNO ACCADEMICO 2014/2015

Backdoor nei sistemi crittografici: paranoia o incoscienza?

Relatore*:* ing. Gianluca CARICATO
Tutor: dott. ing. Simone TACCONI

Abstract

"More people are killed every year by pigs than by sharks, which shows you how good we are at evaluating risk" – Bruce Schneier

Il "*mondo digitale*", un mondo in cui le distanze spaziali diventano irrilevanti ed i tempi si comprimono, è ormai realtà.
Fibra ottica, reti radiomobili ad alta velocità, dispositivi portatili ad alta capacità elaborativa e dotati di sensoristica di ogni genere, virtualizzazione dell'hardware e capacità elaborativa e trasmissiva in ogni "oggetto". Il tutto a costi accessibili ai più.
Risultato?
Assistiamo alla progressiva **digitalizzazione** di *informazioni*, *processi* e *servizi*, non solo nelle aziende ma anche in ambito sociale (si pensi ai *social network*) e nella Pubblica Amministrazione, con indubbi vantaggi in termini di efficacia ed efficienza (minori costi e maggiore qualità): è un processo ormai irreversibile, che concorre a creare connessioni ed interdipendenze tra settori eterogenei.

In tale contesto diventano rilevanti le **problematiche di sicurezza** perché, nel mondo digitale, problemi locali (dovuti ad errori, o ad azioni malevole, è lo stesso) possono avere impatti su milioni di persone e divenire facilmente "sistemici". Affinché tutto funzioni, è necessario poter *proteggere* le informazioni e garantire il *corretto funzionamento* dei sistemi informativi a supporto di processi e servizi.
Per questo motivo sono oggi largamente utilizzati *principi*, *strumenti* e *metodi* ***crittografici***, validati dalla comunità scientifica e generalmente considerati sicuri, tramite cui sono garantiti i *servizi di sicurezza* necessari, quali: riservatezza, integrità ed autenticità dei dati, autenticazione e non ripudio.
Parliamo ad esempio di algoritmi e metodi di cifratura, di hashing, di firma digitale o di *key-agreement*, usati in ambito aziendale per il controllo accessi o la firma digitale di documenti, ma anche in attività di tutti i giorni, come fare acquisti online, accedere a sistemi di *home banking*, gestire le proprie (molteplici) identità digitali o, perché no, utilizzare le nuove valute elettroniche.

Tutto bene quindi.
O forse no, se si sposta l'attenzione dalla sicurezza delle informazioni e dei servizi, alla sicurezza degli strumenti crittografici usati per proteggerli. È infatti evidente che la compromissione dei meccanismi crittografici renderebbe automaticamente inefficaci le misure di protezione che ne fanno uso.
La sicurezza dei sistemi crittografici risiede nella robustezza degli algoritmi, nel modo in cui sono stati implementati, nella lunghezza/adeguatezza delle chiavi e nella modalità con cui si gestiscono le chiavi ed il materiale crittografico: in questo lavoro di tesi ci si è concentrati sulle tematiche afferenti la loro **implementazione**, approfondendo la possibilità di introdurre ***volontariamente*** delle vulnerabilità (**backdoor**) nei meccanismi di **generazione delle chiavi.**

Ed è proprio questo il tema affrontato: appurata e dimostrata la possibilità di rendere inefficaci strumenti crittografici ritenuti affidabili tramite l'introduzione di backdoor, si è cercato di analizzare il rischio associato alla minaccia individuando la corretta strategia per gestirlo.

In particolare, sono stati presi in esame i metodi che, sfruttando i parametri pubblici degli algoritmi per trasmettere in modo cifrato informazioni utili alla loro compromissione (*canali subliminali*), risultano non facilmente individuabili da analisi esterne e sono sfruttabili solo da chi le ha progettate (anche a fronte di analisi dell'hardware e del codice sorgente).
Sono stati analizzati due casi significativi, in grado di dimostrare l'esistenza e la pericolosità della minaccia in questione: la compromissione del meccanismo di generazione delle chiavi dell'algoritmo RSA e la compromissione di generatori di numeri pseudo-casuali (DRBG) basati su crittografia asimmetrica, con riferimento allo "strano caso" dell'algoritmo DUAL_EC_DRBG.

Per dimostrare la "facilità" di implementare backdoor di questo tipo, è stato realizzato un semplice programma in C# utilizzando il lavoro di due ricercatori (M. Yung e A. L. Young), in grado di creare coppie di chiavi RSA compromesse, per le quali si riesce a derivare la componente privata a partire da quella pubblica.

Dimostrata quindi l'esistenza della minaccia, è stato analizzato ad alto livello il rischio ad essa associato, identificando i possibili attaccanti, quantificando qualitativamente l'impatto e la probabilità di accadimento "attesi" e proponendo una strategia per il *risk treatment*.

Infine, sono state esaminate le possibili contromisure adottabili per mitigare il rischio in questione: dopo aver redatto una lista di possibili interventi ottenuta a partire dai controlli descritti negli standard ISO/IEC 27001:2013 e ISO/IEC 27002:2013, è stato preso in esame quello che prevede attività di test e validazione dei sistemi crittografici, verificando la presenza (in Italia e all'estero) di obblighi normativi o buone prassi per il trattamento di informazioni sia classificate che non classificate.

Ed ecco i risultati.
Il lavoro svolto dimostra che **qualunque sistema crittografico "black-box"**, cioè non verificato o non verificabile, **è potenzialmente insicuro**, in quanto esistono metodi per comprometterne l'efficacia che sono difficili da individuare, e che garantiscono all'attaccante un utilizzo esclusivo (nessun altro può farne uso).

L'analisi del rischio ha inoltre evidenziato che, seppure l'introduzione di backdoor negli strumenti crittografici sia difficile da portare a termine, richiedendo competenze specialistiche

ed una non semplice pianificazione dell'attacco, l'entità degli *impatti* possibili può giustificare interventi mirati per la **mitigazione del rischio**.
Va infatti considerato che:

- vulnerabilità di questo tipo, difficili da individuare, possono essere sfruttate per condurre attacchi complessi e di lunga durata (tipici delle APT - Advanced Persistent Threat);
- la minaccia può essere attuata anche da soggetti "fidati", come fornitori[1] o, almeno teoricamente, enti di standardizzazione[2].

L'analisi delle contromisure applicabili ha invece messo in risalto la necessità di intervenire, oltre che con processi di test e validazione dei prodotti crittografici, anche con **attività preventive** riguardanti le politiche di sicurezza dell'*organizzazione*, la formazione del *personale*, la gestione del *ciclo di vita del software e dei sistemi* ed i processi di *monitoraggio*.

Relativamente alle **attività di test e validazione**, è stato evidenziato come, sia in Italia che all'estero, siano previsti specifici obblighi nel caso di sistemi che trattano *informazioni classificate*.
La situazione cambia invece nel caso di *informazioni prive di una classifica di segretezza*: mentre negli U.S.A. ed in Canada è obbligatoria la certificazione (secondo lo standard FIPS PUB 140-2) dei sistemi utilizzati dagli enti governativi per trattare *informazioni non classificate ma sensibili* (SBU), in Italia esiste un obbligo normativo per i soli dispositivi di firma digitale[3].

Alla luce di quanto esposto, si ritiene che la minaccia in questione vada tenuta in considerazione almeno nella Pubblica Amministrazione e nelle aziende private che gestiscono infrastrutture critiche o che concorrono all'erogazione di servizi ai cittadini, attuando i controlli definiti dagli standard e prevedendo test di accettazione indipendenti, da valutare caso per caso in funzione dei rischi esistenti.

[1] Il "*Quadro strategico nazionale per la sicurezza dello spazio cibernetico*" (2013) parla ad esempio di un "rischio concreto" che altri Paesi inducano la propria industria a produrre componenti alterati al fine di superare le difese nazionali.
[2] Gli articoli scientifici ed i fatti inerenti il caso del DUAL_EC_DRBG ne dimostrano la fattibilità "tecnica".
[3] Secondo lo "*Schema nazionale per la valutazione e la certificazione della sicurezza di sistemi e prodotti nel settore della tecnologia dell'informazione*", istituito con il DPCM del 30 ottobre 2003.