PRIVACY, COMPUTER FORENSICS E CRIMINI INFORMATICI

L'anello debole nella catena della fiducia in Rete

Corrado Giustozzi

Sapienza
Università di Roma

Punti che discuteremo

- Autorità di certificazione e modelli di trust
- Quattro casi di studio:
  - Stuxnet
  - Comodo
  - DigiNotar
  - Flame
- Conclusioni

Identità in Rete, ovvero: chi c'è dall'altra parte?

Identità digitali, autorità di certificazione e catene di fiducia

Parliamo di identità digitale…

- Il netizen vive e si esprime sempre più soltanto in Rete
- Anche senza chiamare in causa la fantascienza, la Rete tende a mediare e sostituire i contatti sociali (il che non è sempre un male!é)
- Lôinterazione con la società digitale avverrà sempre di più mediante la Rete
- Il principale crimine del ciberspazio nel futuro sarà il **furto dôidentità**

Crittografia a chiave pubblica (1/2)

- Si basa su una coppia di ñchiaviò e su un procedimento di calcolo che ne usa lôuna o lôaltra
- Il sistema gode di due proprietà fondamentali:
  - la conoscenza di una chiave non consente di ricavare lôaltra
  - un messaggio cifrato mediante una chiave può essere decifrato solo mediante lôaltra, e viceversa
- In un sistema del genere:
  - una delle due chiavi (K_p) viene resa **pubblica**
  - lôaltra (K_s) rimane **segreta** ossia è nota al solo proprietario
- Vantaggi rispetto alla crittografia convenzionale:
  - si può scrivere ad uno sconosciuto senza dover preventivamente condividere con lui unôinformazione segreta
  - si può provare la paternità di un messaggio (firma digitale)

Crittografia a chiave pubblica (2/2)

- Il sistema è fortemente asimmetrico:
  - chiunque può cifrare un testo con la chiave pubblica A_p di un soggetto A appartenente al sistema
  - solo A può decifrare un messaggio cifrato con la sua chiave pubblica A_p, perché egli solo è in possesso della corrispondente chiave inversa A_s (la sua chiave segreta)
- Vale anche il viceversa:
  - chiunque può decifrare un testo cifrato da A con la propria chiave segreta A_s perché la chiave inversa corrispondente è la A_p ovvero la chiave pubblica di A
- Vige il principio fondamentale del **non ripudio**:
  - se solo A conosce A_s allora ogni testo cifrato con A_s è stato necessariamente prodotto da A (prova di identità)

L'anello debole del sistema

- Affinché tutto funzioni occorre stabilire:
  - chi e come gestisce l'elenco delle chiavi pubbliche
  - chi e come garantisce la validità dell'elenco
  - chi e come garantisce sull'effettiva corrispondenza fra identità dei soggetti e relative chiavi pubbliche
- Queste certezze fondamentali vengono fornite da un sistema cosiddetto di "certificazione" che fornisce adeguate garanzie sulla reale identità degli utenti e sulla validità ed integrità delle rispettive chiavi pubbliche
- La certificazione si attua mediante:
  - entità garanti → **autorità di certificazione**
  - strumenti tecnologici → **certificati digitali**

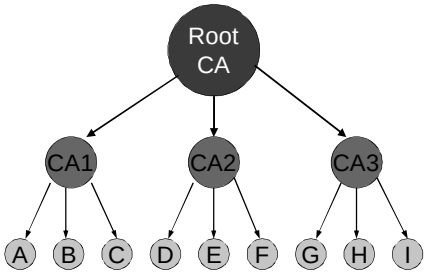
21 giugno 2012 e-privacy 2012 7

Il processo di certificazione

- Le Autorità di Certificazione (CA) sono soggetti *super partes*, affidabili **per definizione**, i quali:
  - attestano la validità delle chiavi che gestiscono/rilasciano
  - garantiscono l'identità dei rispettivi titolari
  - gestiscono l'elenco delle relative chiavi pubbliche
- I Certificati Digitali da esse emessi contengono:
  - la chiave pubblica e i dati anagrafici del titolare
  - ulteriori dati di servizio: scadenza, limitazioni, …
  - la firma digitale del tutto, mediante la chiave segreta della CA
- Il modello di fiducia ISO X.509:
  - è uno standard *de iure* basato sulle Certification Authorities
  - si basa su una struttura gerarchica organizzata formalmente nella quale ogni CA certifica quelle al di sotto di lei

21 giugno 2012 e-privacy 2012 8

Modello di fiducia X.509



21 giugno 2012 e-privacy 2012 9

Caso n° 1: Stuxnet

Rubare due certificati per sabotare una centrale nucleare

Stuxnet, un virus “firmato”

- Giugno 2010: i ricercatori di VirusBlokAda identificano un nuovo worm che si replica usando ben quattro vulnerabilità zero-day di Windows
- La diffusione parte da chiavette USB da cui vengono installati device driver **validamente firmati**
- Apparirà presto chiaro che si tratta di un malware estremamente sofisticato, il quale ha come bersaglio specifici sistemi SCADA della Siemens
  - patch emessa il 30 maggio 2012, 675 giorni dopo la scoperta!
- Il 60% dei sistemi colpiti si trova in Iran, il che ha fatto pensare ad sabotaggio agli impianti di arricchimento dell'uranio per le centrali nucleari iraniane
  - di recente gli USA hanno ammesso di esserne gli autori

Furto di certificati validi

- Stuxnet installa un rootkit i cui device driver sono **firmati digitalmente con certificati validi**, il che ne consente l'installazione autorizzata
- I certificati, emessi da Verisign, appartengono alle aziende elettroniche taiwanesi Jmicron e Realtek:
  - entrambe hanno sede nel complesso industriale Hsinchu Science Park di Taiwan, in edifici tra loro adiacenti
  - si pensa pertanto che i certificati siano stati trafugati mediante accesso fisico alle rispettive sedi, ma non è ancora chiaro come ciò sia potuto accadere
- Verisign ha prontamente revocato i certificati, ma è stato necessario un aggiornamento di Windows per distribuire la revoca su tutti i sistemi del mondo

Caso n° 2: Comodo

Compromettere una Registration Authority per tentare di leggere la posta altrui

Emissione fraudolenta di certificati

- Comodo CA è una certification authority regolarmente accreditata che vende molti tipi di certificati digitali (OV, DV, EV SSL, é)
- Nel marzo 2011, in seguito alla compromissione di un account in una RA affiliata (in Italia), Comodo ha emesso nove certificati validi ma fraudolenti intestati a:
  - mail.google.com, www.google.com
  - login.yahoo.com (tre certificati)
  - login.skype.com
  - addons.mozilla.org
- Si hanno prove che il certificato intestato a Yahoo ha effettivamente svolto attività su Internet

Analisi dell'incidente

- Comodo ha revocato i certificati non appena si è accorta della loro emissione fraudolenta
  - i produttori di browser hanno dovuto eliminare i certificati dai propri prodotti mediante aggiornamenti coordinati
- Dopo adeguate verifiche Comodo ha affermato che:
  - l'attacco ha riguardato e compromesso la sola RA
    - né i sistemi della CA né le chiavi nell'HSM sono stati compromessi
  - l'attacco:
    - era stato pianificato da tempo e svolto con cura chirurgica
    - proveniva da un IP allocato in Iran (212.95.136.18)
  - l'attaccante aveva controllo sull'infrastruttura DNS
- Comodo ritiene pertanto che la responsabilità dell'attacco sia di un governo straniero

Caso n° 3: DigiNotar

Colpire chirurgicamente una CA e mettere in ginocchio un intero Paese per intercettare a tappeto la posta di centinaia di migliaia di persone

Infrastruttura di trust per l'e-gov

- DigiNotar è (anzi, eraé) una CA olandese:
  - fondata nel 1997 dal notaio Dick Batenburg e dal Notariato olandese, per fornire ai notai servizi di TTP
  - acquistata nel 2010 da VASCO Data Security Int., posta in liquidazione volontaria il 20/09/ 2011 a seguito della scoperta di unôampia compromissione dei propri sistemi
- DigiNotar forniva al Governo olandese certificati per lôinfrastruttura di firma digitale del programma nazionale di e-government (PKIoverheid)
- In particolare era la Root CA per:
  - "Staat der Nederlanden"
  - DigiD, piattaforma centralizzata di autenticazione e-government
  - Rijksdienst voor het Wegverkeer (registro automobilistico)

Cronistoria dell'incidente (1/3)

- 27/08/2011: uno studente iraniano segnala su un forum di Google che il suo browser Chrome gli indica come non valido il certificato SSL usato dal server di Gmail
  - ben presto appare chiaro che si tratta di un certificato fraudolento emesso da DigiNotar il 10 luglio, a seguito di unôintrusione nella sua CA
- 29/08/2011: su pressioni del GOVCERT-NL, DigiNotar revoca quel certificato
  - nei giorni successivi tuttavia si scoprono ñin the wildòmolti altri certificati analoghi emessi fraudolentemente da DigiNotar

Cronistoria dell'incidente (2/3)

- 30/08/2011: DigiNotar rivela di essersi accorta sin dal 19 luglio di un'intrusione sui propri sistemi, ma afferma che l'infrastruttura PKIoverheid non è stata compromessa; commissiona però alla società Fox-IT un audit approfondito su tutti i propri sistemi
- 02/09/2011: il Governo olandese ritira la fiducia a DigiNotar ma non revoca ancora i certificati di PKIoverheid; tuttavia afferma di non poter garantire l'affidabilità della piattaforma di e-government ed invita formalmente i cittadini a non servirsene fino a nuova comunicazione

Cronistoria dell'incidente (3/3)

- 03/09/2011: il Governo olandese assume il controllo diretto delle operazioni di DigiNotar, revoca i certificati di DigiD e PKIoverheid e li rimpiazza con nuovi certificati emessi da un'altra CA (Getronics)
- 05/09/2011: viene pubblicato il report preliminare di Fox-IT che dimostra come la compromissione dei sistemi della CA sia molto più ampia del previsto
- Fra il 2 e il 9 settembre 2011 Windows e tutti i browser vengono aggiornati eliminando DigiNotar dalla lista delle Root CA riconosciute

Analisi dell'incidente (1/2)

- Non è stato possibile determinare il numero esatto di certificati emessi fraudolentemente:
  - vi sono indicazioni che siano certamente più di 531
  - DigiNotar non ha potuto garantire che tutti siano stati effettivamente revocati
  - soltanto Google ne ha posti in blacklist 247
- I certificati erano intestati ad oltre 300 domini tra cui:
  - Aziende e provider: Aol, Android, Google, Microsoft, Mozilla, Skype, Twitter, Yahoo, Facebook, Torproject
  - Servizi: Windows Update e Wordpress
  - Altre CA: Digicert, GlobalSign, Thawte, Comodo, VeriSign, CyberTrust
  - Enti governativi: Mossad, Cia, MI5

Analisi dell'incidente (2/2)

- Il report di Fox-IT dipinge uno scenario drammatico di incuria ed inadeguatezza nella gestione della CA:
  - assenza di separazione tra le componenti della CA
  - tutti i server, benché posti in locali anti-tempest, erano accessibili tramite la LAN di management
  - tutti i server erano nello stesso dominio Windows ed usavano un'unica coppia userid/password
    - la password era assai debole e quindi facilmente craccabile
  - sui server non erano installati antivirus/antimalware
  - mancava un sistema di raccolta ed analisi dei log
  - sui server critici erano presenti molteplici malware
  - i prodotti di front-end sui server Web non erano aggiornati/patchati

21 giugno 2012 e-privacy 2012 22

Risultati successivi

- L'analisi delle richieste di uso dei certificati (log del server OCSP) ha mostrato che l'area del loro utilizzo era concentrata soprattutto in Iran:
  - fra il 4 ed il 29 agosto il certificato intestato a Google è stato acceduto da oltre 300.000 IP diversi, di cui oltre il 99% di provenienza iraniana
- Ciò porta a ritenere che si sia trattata di una azione governativa finalizzata a costruire un sistema "man-in-the-middle" per l'intercettazione sistematica della posta scambiata su Gmail:
  - è verosimile che in seguito all'attacco siano state compromesse oltre 300.000 caselle di posta di Gmail appartenenti a cittadini iraniani

21 giugno 2012 e-privacy 2012 23

Caso n° 4: Flame

Raggiunto il sogno di ogni malware: installarsi automaticamente attraverso il servizio Windows Update

21 giugno 2012 e-privacy 2012 24

Una storia ancora in corso…

- Il 28 maggio 2012 Kaspersky Lab annuncia di aver scoperto un nuovo, sofisticatissimo, «attack toolkit»:
  - si tratta di un complesso sistema di spionaggio in grado di catturare selettivamente file, immagini, conversazioni audio, inviandole in forma cifrata a vari centri di C&C nel mondo
  - lôindagine, svolta con il CERT nazionale iraniano ed il CrySyS Lab dellôuniversità di Budapest, nasceva dalla richiesta dellôITU di investigare su un incidente al Ministero del petrolio in Iran
- Secondo Kaspersky, Flame era in azione sin dal febbraio 2010, anche se in modo assai selettivo:
  - solo ~1.000 sistemi colpiti, soprattutto in Iran ma anche in Israele, Sudan, Siria, Libano, Arabia Saudita, Egitto
- Appare ben presto evidente la relazione con Stuxnet:
  - il 20 giugno è confermata lôorigine NSA-CIA-Mossad

Un malware assai sofisticato

- Flame presenta molte caratteristiche peculiari:
  - è estremamente modulare
    - composto da oltre 20 moduli caricabili dinamicamente
  - è scritto principalmente in Lua con alcune parti in C++
  - ha una dimensione inusuale di oltre 20 Mbyte
  - usa un DB relazionale (SQLite) per gestire dati strutturati
  - implementa cinque diversi algoritmi crittografici
  - sfrutta due delle vulnerabilità zero-day usate da Stuxnet
  - possiede sofisticate capacità stealth
    - si automodifica in funzione della presenza di antivirus noti
  - è in grado di ricevere comandi dal centro di C&C
    - può autoeliminarsi in seguito ad un apposito comando
  - può interagire con dispositivi Bluetooth nelle vicinanze

Un'origine certificata

- Flame installa un rootkit e vari device driver il cui codice è regolarmente firmato con un certificato in apparenza valido **emesso da una CA Microsoft**:
  - per ottenere questo risultato è stato sfruttato un bug nella «Terminal Services licensing certification authority» assieme ad un sofisticato *collision attack*
  - in questo modo certificati che dovrebbero servire solo alla verifica delle licenze possono essere usati per firmare codice come se provenisse da Microsoft
- Utilizzando questo certificato illegittimo, Flame è in grado di installarsi silenziosamente su altri computer appartenenti al medesimo dominio spacciandosi per un aggiornamento legittimo proveniente dal servizio **Windows Server Update Services** (WSUS)

Correzioni ancora in arrivo…

- Microsoft sta rapidamente correggendo le vulnerabilità:
  - il 30 giugno 2012, con un aggiornamento critico non programmato, sono stati emessi:
    - un bollettino di sicurezza che descrive il problema
    - una patch che corregge il bug nella PKI dei Terminal Services
    - un aggiornamento che revoca due CA intermedie e relativi certificati:
      - Microsoft Enforced Licensing Intermediate PCA
      - Microsoft Enforced Licensing Registration Authority
  - il 11 giugno 2012 è stato aggiornato il servizio WSUS (V3.0 SP2) rinforzandone i canali di comunicazione:
    - non più consentita la deep packet inspection
  - il 12 giugno 2012 è stato rilasciato un nuovo updater per Vista e Win7 che (finalmente!) verifica la CRL dei certificati (Microsoft)
  - ad agosto 2012 verrà rilasciato un aggiornamento che renderà invalidi tutti i certificati che utilizzino chiavi RSA di lunghezza inferiore a 1024 bit

CONCLUSIONI

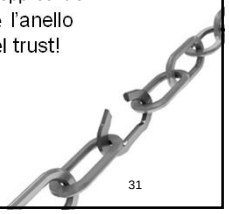
C'È UNA MORALE IN TUTTO CIÒ?...

Considerazioni finali (1/2)

- *"This is a nightmare scenario. You have to trust the companies selling these certificates and if we can't, then all bets are off."*
  - Mikko Hyppönen, responsabile della ricerca di F-secure
- Il futuro della società digitale si basa sul trust fra sistemi e utenti nell'interazione non in presenza
- In questo scenario le Certification Authorities:
  - svolgono un ruolo chiave, perché da esse dipende la fiducia di tutti nel corretto funzionamento del sistema
  - costituiscono un'infrastruttura critica estremamente appetibile per i malintenzionati, in quanto da esse dipende la possibilità di condurre azioni malevole importanti e/o su grandissima scala
- Le CA sono l'infrastruttura più critica della Rete

Considerazioni finali (2/2)

- I recenti episodi di attacchi alle CA suggeriscono tuttavia che il problema dell'integrità della catena del trust sia troppo sottovalutato in tutto il sistema:
  - quasi nessun browser accede alle liste di revoca per verificare dinamicamente la validità dei certificati
  - molti *root certificates* sono **cablati** nei sistemi client
  - molte CA rilasciano certificati senza troppi controlli
- Le CA rischiano quindi di diventare l'anello più debole nella delicata catena del trust!
- Vale sempre l'antico monito di Giovenale: ***"****quis custodiet ipsos custodes?****"***



21 giugno 2012 e-privacy 2012 31

La morale quindi è che…

21 giugno 2012 e-privacy 2012 32

L'ANELLO DEBOLE NELLA CATENA DELLA FIDUCIA

GRAZIE PER L'ATTENZIONE

C.GIUSTOZZI@ACM.ORG

21 giugno 2012 e-privacy 2012 33