Presi nella Rete

Quis custodiet ipsos custodes?

Corrado Giustozzi

Permanent Stakeholders' Group, ENISA

I temi che tratteremo

- Identità digitale e identificazione in Rete
- Autorità di certificazione e catene di fiducia
- Quattro casi di studio:
  - Stuxnet
  - Comodo
  - DigiNotar
  - Flame
- Conclusioni

Identità in Rete: come essere certi di chi è chi?

Identità digitali, autorità di certificazione e catena di fiducia

Il problema dell'identità digitale

"On the Internet, nobody knows you're a dog."

Furto di identità: fantascienza?...

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

Nuove forme di garanzia

- Per fornire garanzie alle identità digitali si usano tecniche di *validazione* ottenute come effetto collaterale delle moderne tecniche di *protezione* delle informazioni
- La *crittografia a chiave pubblica*, nata per proteggere le comunicazioni di massa, consente anche di attribuire *certezze* ad un documento digitale, ed in particolare ad un documento di identità
- La mutua certezza dell'identità digitale è fondamentale soprattutto nelle interazioni «*machine-to-machine*» in cui un client accede ad un server remoto per ottenere servizi "trusted" (lettura di email, transazioni finanziarie, servizi di e-Health e di e-governement, …)

Crittografia a chiave pubblica - 1

- Si basa su una coppia di «chiavi» e su un procedimento di calcolo che ne usa l'una o l'altra per cifrare un testo
- Il sistema gode di due importanti proprietà:
  - conoscendo una chiave non si può ricavare l'altra
  - un messaggio cifrato mediante una chiave si può decifrare solo mediante l'altra, e viceversa
- In un sistema del genere:
  - una delle due chiavi (K_p) viene resa **pubblica**
  - l'altra (K_s) rimane **segreta**, ossia è nota al solo proprietario
- Vantaggi rispetto alla crittografia convenzionale:
  - si possono cifrare messaggi per qualsiasi corrispondente, senza bisogno di condividere in anticipo un segreto con lui
  - consente la prova certa di autenticità del testo (firma digitale)

23 novembre 2012 Collegio Ghislieri 7

Crittografia a chiave pubblica - 2

- Il sistema è fortemente asimmetrico:
  - chiunque può cifrare un testo con la chiave pubblica A_p di un soggetto A appartenente al sistema
  - tuttavia 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 nessuno conosce la chiave segreta A_s di A, all'infuori di A stesso, allora ogni testo cifrato con A_s è necessariamente stato prodotto da A, e chiunque può verificarlo facilmente

23 novembre 2012 Collegio Ghislieri 8

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" il quale 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**

23 novembre 2012 Collegio Ghislieri 9

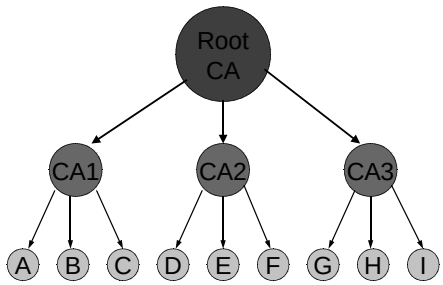
Autorità di certificazione e modelli di trust

I meccanismi tecnologici ed organizzativi cui è affidata la gestione della fiducia in Rete

Il processo di certificazione

- L'Autorità di Certificazione è un soggetto *super partes*, affidabile **per definizione**, il quale:
  - attesta la validità di una chiave
  - garantisce l'identità del titolare
  - gestisce l'elenco delle chiavi pubbliche
- Il Certificato Digitale da essa emesso contiene:
  - la chiave pubblica del titolare ed i suoi dati anagrafici (identità)
  - ulteriori dati di servizio (scadenza, limitazioni, …)
  - la firma digitale dei dati fatta con la chiave segreta della CA
- Il modello di certificazione ISO X.509:
  - è uno standard *de iure* basato sulle Certification Authorities
  - si basa su di una formale **struttura gerarchica di fiducia** nella quale ogni CA certifica quelle poste al di sotto di lei

Catena di fiducia secondo X.509



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 automatica 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, …)
- 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 abbia 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, era…) 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 un'ampia compromissione dei propri sistemi
- DigiNotar forniva al Governo olandese certificati per l'infrastruttura 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 (1/2)

- 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
  - appare presto chiaro che si tratta di un certificato fraudolento emesso da DigiNotar il 10 luglio in seguito ad un'intrusione
- 29/08/2011: su pressioni del GOVCERT-NL, DigiNotar revoca quel certificato
  - nei giorni successivi tuttavia si scoprono "in the wild" molti altri certificati analoghi emessi fraudolentemente da DigiNotar
- 30/08/2011: DigiNotar rivela di essersi accorta sin dal 19 luglio di un'intrusione, ma afferma che l'infrastruttura PKIoverheid non è stata compromessa
  - commissiona però alla società Fox-IT un audit approfondito su tutti i propri sistemi

Cronistoria dell'incidente (2/2)

- 02/09/2011: il Governo olandese ritira la fiducia a DigiNotar ma non revoca i certificati di PKIoverheid
  - afferma però di non poter garantire l'affidabilità della piattaforma di e-government ed invita formalmente i cittadini a non usarla
- 03/09/2011: il Governo assume il controllo diretto delle operazioni di DigiNotar, revoca i certificati di DigiD e PKIoverheid e li rimpiazza con certificati di un'altra CA
- 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 ben 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 alle ultime release né "patchati"

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 gigantesco 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

Caso n° 4: Flame

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

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
  - l'indagine, svolta con il CERT nazionale iraniano ed il CrySyS Lab dell'università di Budapest, nasceva dalla richiesta dell'ITU 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 l'origine 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 ha rapidamente corretto 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
  - l'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 (solo MS)
  - il 9 ottobre 2012 è stato rilasciato un aggiornamento automatico che ha reso invalidi tutti i certificati basati su chiavi RSA di lunghezza inferiore a 1024 bit

Conclusioni

C'è una morale in tutto ciò?...

Considerazioni finali

- Le vere infrastrutture critiche non sono solo quelle che dipendono dal funzionamento della Rete, ma soprattutto quelle **da cui dipende** il funzionamento della Rete:
  - la CA sono forse l'infrastruttura più critica per la Rete
- L'integrità della catena di fiducia è troppo sottovalutata:
  - quasi nessun browser accede alle liste di revoca per verificare dinamicamente la validità dei certificati che riceve
  - 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?"*

Presi nella rete

Grazie per l'attenzione

C.GIUSTOZZI@ACM.ORG