Hackmeeting 0x0A

Pisa, 28-30 settembre 2007

Metodi di compromissione di sistemi di comunicazione privata ed anonima in Rete

Tassonomia ed esempi pratici di applicazione ai sistemi per l'anonimato esistenti

Marco A. Calamari - marcoc@winstonsmith.info

Progetto Winston Smith

Prologo ...

Non siamo **furbi** !

Od almeno, non siamo i **piu'** furbi ...

O, come minimo, non possiamo essere **sempre** furbi.

E comunque **non basta** essere furbi (e competenti, ed attenti...) e' necessario soprattutto essere consapevoli dei limiti propri, delle tecnologie e dei sistemi informatici.

Per questo motivo oggi non parleremo di PET, Privacy Enhancing Technologies, tecnologie per il miglioramento della privacy, ma di **attacchi** alle PET.

Le PET sono belle, funzionano e ci fanno sentire sicuri. Od almeno un po' piu' sicuri .... beh, forse **troppo** sicuri.

... Prologo ...

Crittoanalisi, **analisi del traffico, correlazioni temporali, analisi know plaintext, replay attack** sono solo alcuni dei metodi con cui possono essere compromessi i sistemi per la privacy.

In questo intervento cercheremo di presentare degli esempi di un settore, quello degli attacchi alle PET, che include una quantita di tecniche, crittoanalisi, analisi dei protocolli di rete, tecniche investigative tradizionali di cui si parla poco, forse perche' considerate appartenenti al “lato oscuro”.

Non potendo certo tenere un corso di tecniche matematiche ed informatiche, procederemo per esempi, esaminando le tipologie di attacco che possono essere portate contro alcuni dei piu' noti sistemi PET. L'esposizione partira' dalla descrizione di una applicazione PET, seguita da quelle degli attacchi che possono essere usati contro di essa.

... Prologo

Ma prima di continuare, dobbiamo aver ben chiaro che oltre agli **attacchi contro le PET,** ci sono **le trappole, attacchi agli utenti delle PET** che sfruttano **comuni errori di chi le usa** sono solo alcuni dei metodi con cui possono essere compromessi i sistemi per la privacy.

Sempre di attacchi alla privacy si tratta; alcune notizie hanno parlato di alcune PET come Tor definendole suscettibili alla “stupidita'” dei loro utilizzatori.

Senza la pretesa di essere completi, fardmo esempi anche di questi “attacchi”

Pubblicita'

Il **Progetto Winston Smith** e' una organizzazione informale di persone preoccupate per la privacy in Rete.

Realizza iniziative di tipo tecnologico, legale e formativo per favorire l'uso delle tecnologie di comunicazione privata e sicura.

Allo scopo di essere una organizzazione “ricorsiva”, fornisce una prova di fattibilita' del completo anonimato raggiungibile con queste tecnologie istanziandosi tramite una personalita' virtuale, collettiva ed anonima, che, ispirandosi al lungimirante ed attualissimo romanzo “***1984***” prende il nome dal protagonista ***Winston Smith***.

Maggiori informazioni: **https://www.winstonsmith.info**

Di cosa parleremo ?

- **Tassonomia delle tecniche anti-PET**
- **Pgp**
- **Mixmaster**
- **Freenet**
- **Tor**
- **Tor e gli utonti**
- **Conclusioni**

Tassonomia anti-PET ...

- Attacchi di coercizione psico-fisica
- Attacchi di coercizione legale (di gran moda!)
- Attacchi tecnologici out-of band (microspie, intercettazioni telefoniche, tempest)
- Attacchi tecnologici di computer forensic
- Attacchi bruteforce contro chiavi e password
- Attacchi known plaintext
- Attacchi chosen plaintext

… Tassonomia anti-PET

- Analisi di correlazione temporale
- Analisi di correlazione dimensionale
- Attacchi di replay
- Attacchi di partizionamento
- Attacchi DoS esterni
- Attacchi DoS interni (nodi cancer)
- Attacchi di sovversione (nodi rogue)
- Attacchi di infiltrazione (rootkit)

- Attacchi ai **dummies**

Pgp

Pgp ...

Pgp ed il suo clone libero Gpg hanno rappresentato l'inizio delle PET, e hanno a buon titolo il diritto di essere il nostro punto di partenza.

Pgp e' un sistema crittografico a chiave pubblica che permette di cifrare qualsiasi file, e viene tipicamente utilizzato per cifrare la posta elettronica. Decifrare un messaggio richiede l'uso di un piccolo file (la chiave privata) che e' di solito bloccata da una password.

Violare un messaggio cifrato con Pgp con tecniche informatiche e' molto complesso.

Ma esistono altri metodi ..... comunque cominciamo dall'inizio.

Pgp: attacchi fisici e legali

Un attaccante di profilo sufficentemente alto puo' violare Pgp semplicemente obbligando, tramite **coercizione psicofisica o legale**,(non ci avevate pensato eh?) il possessore alla consegna della chiave private e della relativa password di blocco.

Sulla coercizione fisica, sempre di moda nella storia dell'umanita', lasciamo tutto alla vostra immaginazione.

Dal punto di vista legale in alcuni paesi e' reato **“di per se'”** non consegnare chiavi e/o password di sistemi crittografici che siano oggetto di indagini di polizia. La privacy non e' ammessa, e la smemoratezza nemmeno.

Pgp e' ovviamente vulnerabile a questo tipo di attacchi, come tutti i sistemi PET di prima generazione.

Pgp: attacchi bruteforce

Nella maggior parte dei sistemi che implementano PET, la sicurezza operativa dipende in ultima analisi da una **password** od una passphrase, e dal possesso di una chiave.

Un attacco di brute force contro una password puo' essere reso **apparentemente** improponibile in maniera semplice con l'utilizzo di password lunghe.

In realta' programmi di cracking a dizionario e dotati di una certa dose di “intelligenza” come il celebre **L0pthcrack** riescono nella pratica a violare rapidamente anche chiavi lunghe che non siano state scelte con particolare cura.

E' interessante, per un paranoico di professione, notare come l'attivita' di ricerca pubblicata in questo settore si limiti a pochi filoni, come il bruteforcing con supercomputer, e non esplori direzioni diverse, legate al linguaggio e/o alla psicologia ....

Pgp: analisi forensiche

Pgp non fornisce di per se nessuna protezione contro analisi condotte sull'hardware che viene utilizzato, in particolare ad un'analisi di tipo forensico del disco fisso.

L'input di password, lo sblocco di chiavi private e la decifrazione dei messaggi possono lasciare tracce rivelatrici nei file cancellati e nelle aree di swap dei sistemi operativi moderni.

Un attaccante di profilo medio, ed in certi casi basso puo' con questi metodi e con **utility preconfezionate reperibili in Rete** ottenere informazioni che permettono di conoscere il contenuto di singoli messaggi o di decrittarli tutti.

Pgp: attacchi criptoanalitici

I sistemi crittografici in generale, pur basati su algoritmi inattaccabili, sono comunque suscettibili ad attacchi di tipo crittoanalitico; e' infatti possibile facilitare la decodifica di un messaggio crittografato e/o l'individuazione della chiave privata nel caso che:

- Si conosca la versione in chiaro di almeno un messaggio crittografato (**known plaintext**)
- Si possa far crittografare ed esaminare un messaggio scelto con criteri particolari (**chosen plaintext**)

Ambedue queste tecniche furono usate nella seconda guerra mondiale contro il cifrario tedesco Enigma; si tratta comunque di attivita' da attaccanti di profilo alto.

Pgp: analisi del traffico

L'uso di Pgp e dei sistemi crittografici per cifrare la posta elettronica rende privati i contenuti delle comunicazioni, ma non l'e**sistenza delle comunicazioni stesse**, i mittenti ed i destinatari.

Mittenti e destinatari dei messaggi sono infatti facilmente rilevabili intercettando in tempo reale la posta durante la trasmissione, o meglio costringendo i provider a memorizzare per lunghi periodi questi tipi di informazioni ed a creare database (idea originale, eh?).

La perdita di privacy **derivante dalla sola analisi del traffico** puo' avere effetti pratici simili a quelli della decrittografazione dei contenuti.

Mixmaster

Mixmaster ...

Mixmaster e' una rete di server (remailer anonimi) che permette di inviare messaggi anonimi via posta elettronica, utilizzando una cifratura a piu' strati (**onion**) ed un routing manuale, che realizza una “**mixnet**”.

L'invio dei messaggi avviene tramite normale posta elettronica, ed essi sono di solito anche cifrati con Pgp.

Gli operatori (remop) gestiscono il loro server in maniera completamente autonoma tra di loro. Inviando il messaggio attraverso almeno 3 remailer, a' sufficente che **uno** dei server **non** sia compromesso perche' il messaggio resti anonimo.

Viene nascosta l'identita del mittente, ma non l'esistenza di una comunicazione effettuata tramite remailer.

Mixmaster: attacchi fisici e legali

I **remops**, ben identificabili via Rete, possono essere soggetti ad attacchi di tipo fisico e legale. Nessuno puo' pero' essere obbligato a rivelare quello che non sa. Mixmaster e' stata la prima PET a proteggere i suoi operatori, dimostrando matematicamente che essi non possono conoscere i mittenti dei messaggi che sono passati dal proprio remailer.

Possono pero' essere costretti a consegnare le chiavi private, permettendo ad un attaccante di alto profilo di tentare di prendere il controllo della maggioranza dei remailer e rivelare cosi i mittenti di una buona parte dei messaggi transitati nell'intera mixnet.

Un Mixmaster e' in grado di “sopportare” un'alta percentuale di nodi “**rogue**”. E' voce comune che una parte dei remailer Mixmaster siano controllati dalla Chiesa di Scientology, nemica storica dei remailer, avendone sperimentato l'efficacia.

Mixm: correlazione dimensionale

I messaggi scambiati non sono comprensibili ma possono essere distinguibili, e questo permette di effettuare **attacchi di tipo statistico**. Precedenti tipi di remailer anonimi presentavano il problema che la dimensione di un messaggio era caratteristica del messaggio stesso, e che essa variava diminuendo di una quantita' prevedibile ad ogni passaggio da un remailer all'altro, e quindi di seguire un dato messaggio.

Mixmaster supera questo problema spezzettando ogni messaggio in parti di dimensioni standard, ed inserendo zavorra nell'ultimo. Il remailer finale riassembla il messaggio e lo invia al destinatario.

Questo impedisce di distinguere su base probabilistica il cammino di un messaggio che parte da un mittente noto, o di ricavare all'inverso da dove proviene un messaggio ricevuto da un determinato destinatario.

Mixmaster: correlazione temporale

I messaggi che partono, transitano attraverso un remailer ed arrivano a destinazione lo fanno in **istanti precisi**, che possono essere rilevati ed a**nalizzati su base statistica**.

Per questo motivo i messaggi ricevuti da un remailer non vengono inoltrati immediatamente, ma trattenuti e rilasciati dopo un **tempo variabile con modalita' pseudocasuali**.

La conoscenza degli algoritmi pseudocasuali usati e l'uso di tecniche statistiche piu' raffinate permettono comunque di ottenere informazioni da un'analisi temporale, anche se piu' incerte ed in quantita' minore.

Mixmaster: attacchi replay

I messaggi che entrano in una mixnet recano al loro interno le indicazioni del cammino da percorrere. E' possibile percio' registrare un certo messaggio nel momento in cui viene trasmesso dal mittente, e successivamente postarne una grann numero di copie, che **seguiranno lo stesso cammino**.

Questo produce un **picco di traffico di rete** che puo' essere rilevato mentre **attraversa i vari remailer** e si dirige verso i destinatario.

I remailer di tipo piu' primitivo erano suscettibli a questo tipo di attacco, mentre quelli Mixmaster tengono nota di un hash dei messaggi che li attraversano, e scartano eventuali copie successive.

Mixmaster: partizionamenti

I messaggi che attraversano un remailer compromesso rivelano all'attaccante una parte della loro struttura interna, anche se non il loro contenuto.

Questo e' dovuto all'esistenza, nei protocolli dei remailer anonimi, di **parametri** il cui valore e' deciso arbitrariamente dal mittente, il quale tende a ripetere sistematicamente certe scelte che costituiscono nel loro complesso una spece di “impronta digitale”.

Nel tempo questo consente di correlare vari messaggi transitati come provenienti dallo stesso mittente, fino ad associarli tutti ad un **indirizzo reale** se il remailer compromesso viene anche **utilizzato come primo anello della catena**.

Freenet

Freenet ...

Freenet e' un s**istema di pubblicazione anonima** di informazioni, dotato di un **data storage criptato e distribuito**.

Scritta in Java, e' in grado di spezzettare, crittografare, duplicare e disperdere un file, ed incredibilmente e' in grado di eseguire l'operazione inversa e recuperarlo.

Il nodi Freenet sono paritari, ed e' necessario installarne uno sul proprio pc per poter accedere a Freenet.

Un proxy incorporato permette di accedere alle informazioni pubblicate in forma di sito web anonimo, lento ma indistinguibile da un sito web ordinario.

Freenet: attacchi fisici e legali

Freenet e' progettata per ampliare al massimo la **negazione plausibile** di responsabilita' da parte di chi la usa.

Infatti le informazioni memorizzate su un certo nodo sono crittografate e quindi inaccessibili al suo operatore ammenoche egli non conosca la chiave di richiesta.

Inoltre la presenza di queste informazioni su un certo nodo puo' essere dovuta sia al loro inserimento o lettura, che allo spontaneo ed automatico funzionamento della rete Freenet, rendendo non perseguibile un operatore che avesse dati rivelatisi questionabili sul proprio disco.

Freenet **impedisce totalmente attacchi di tipo censorio,** realizzati costringendo a cancellare informazioni; nessuno, neanche chi l'ha inserita, puo' cancellare una informazione da Freenet, che ne gestisce la “cancellazione” automaticamente.

Freenet: attacchi DoS

Freenet, avendo una capacita' limitata di contenere informazioni, puo' essere attaccata inondandola di informazioni senza senso, allo scopo di cancellare quelle preesistenti.

Gli algoritmi di routing forniscono una certa resilienza a questo tipo di attacco “segregando” i nuovi inserimenti “vicino” ai nodi che li effettuano; in questo modo il resto di Freenet non viene interessato dall'inondazione e le informazioni in esso presenti non vengono cancellate.

E' possibile inoltre “vendemmiare” un elenco completo dei nodi Freenet esistenti, e condurre un attacco DoS inondando le loro porte di rete con richieste ripetute di inserimento e recupero di informazioni. **Qualunque PET e' suscettibile a questo tipo di attacchi al protocollo di trasporto**, che e' per fortuna possibile solo ad attaccanti di profilo molto alto e per periodi limitati.

Freenet: attacchi di sovversione

Il protocollo Freenet e' sia pubblico che molto complesso; questo rende possibile, per un attaccante di alto profilo, realizzare potenzialmente nodi modificati destinati a sovvertire il funzionamento della rete.Concettualmete questi nodi sono di due tipi: **cancer** e **rogue**.

Un nodo Freenet di tipo **cancer** potrebbe ad esempio impersonare un nodo legittimo ma scartare qualunque informazione gli venisse passata e fornire informazioni errate che gli venissero richieste. L'uso di firme crittografiche ed un protocollo di routing adattativo (distanza lessicale) permette di rendere questo tipo di attacchi molto difficili.

Un nodo Freenet di tipo **rogue** potrebbe ad esempio funzionare regolarmente, ma registrando informazioni sugli inserimenti e sugli accessi, cercando di correlare queste informazioni tra loro al fine di rivelare autori e lettori.

Tor

Tor

Tor ...

Tor (The second generation Onion Routing) e' una **rete anonimizzante di proxy criptati** che permette di rendere anonima qualunque comunicazione avvenga tramite l'utilizzo di TCP.

Utilizzata come proxy SOCKS5a, permette di usare tutti i piu' comuni programmi per l'accesso ad internet quali browser web, chat, posta elettronica, newsgroup e qualunque applicazione utilizzi solo **circuiti TCP** (niente UDP, quindi niente streaming).

Tor e' una applicazione di seconda generazione, sviluppata con particolare cura e che attua gia' a livello di progetto la difesa anche legale (plausible deniability) del gestore di un router Tor.

Tor: attacchi di correlazione

Caratteristica comune di tutti gli utenti di mixnet e' quella di non poter nascondere la **propria appartenenza alla mixnet** stessa. Il vecchio detto "***piu' siamo e meglio stiamo***" si applica perfettamente alle mixnet, dove il livello massimo di anonimato teorico ottenibile e' direttamente proporzionale alla dimensione della mixnet.

Tor e' una mixnet ben progettata, ma che si propone di ottenere una bassa latenza. La bassa latenza consente la possibilita' di analisi temporale del traffico, e quindi di ricavare informazioni atte a correlare i due estremi della connessione stabilita' attraverso Tor, oppure a localizzare un hidden service.

Contro questo tipo di analisi vengono prese certe contromisure, come l'accorpamento di piu' circuiti separati, **ma non altre** (come la generazione di traffico fittizio) che non vengono giudicate "economicamente" soddisfacenti.

Tor

Tor e gli utonti

Tor: sniffing di informazioni

Un router Tor di tipo rogue, quando usato come nodo di uscita dalla mixnet, si trova nella posizione ideale per intercettare informazioni inviate in chiaro. Nessuno garantisce che i router Tor che utilizzate siano genuini, e non modificati in maniera malevola, cioe' **rogue**.

Infatti un nodo Tor rogue di uscita non solo puo' sapere da quale router proviene il flusso di informazioni (anche se non puo risalire oltre esso) ma se queste sono in chiaro puo' leggerle, memorizzarle, analizzarle e correlarle con altre.

Questo permette di usare **cookies, referer, header http** ed altro per violare l'identita' e la privacy di chi usasse Tor per fare browsing http.

Tor: compromissione del client

Un router Tor di tipo rogue, quando usato come nodo di uscita dalla mixnet, si trova nella posizione ideale per eseguire un attacco di tipo “man in the middle” contro un utente distratto, che abbia il browser http settato malamente.

Si pensi ad esempio all'**iniezione**, nella pagina web acceduta tramite Tor, di uno **script Javascript** che rilevi e comunichi l'ip del computer, od un file Flash che si colleghi direttamente con il server che ospita il nodo rogue senza usare Tor, rivelando cosi' l'**IP dell'utente**.

Ambedue questi comportamenti, in realta' esterni al protocollo Tor, sono stati rilevati nella realta'.

Tor: main-in-the-middle

Un router Tor di tipo rogue, quando usato come nodo di uscita, si trova nella posizione ideale per eseguire un attacco di tipo “**man in the middle**” contro un utente distratto anche se egli usa il protocollo http, impersonando un server web con credenziali false.

Intercettando la richiesta di apertura della connessione verso il server, il nodo rogue vi offre un certificato simile a quello autentico; il browser ovviamente vi segnala la cosa, ma se come mille altre volte cliccate “OK” e' fatta. Il browser puo' aprire una connessione con voi simulando il server web, ed usare le vostre informazioni per aprire una connessione verso il vero server web fingendosi voi. Poi il limite e' il cielo, per voi **l'inferno**.

E' quindi assodato che anche l'uso di una PET “trasparente” ed user friendly come Tor **richiede una continua attenzione**, e non e' quindi “automaticamente” sicuro per utenti inesperti.

Conclusioni

Conclusioni

Le PET moderne garantiscono una buona resistenza contro attacchi di tipo informatico, di rete, legale ed anche fisico.

Se usate con la cura del "*buon padre di famiglia*" possono garantire una ottima sicurezza condotti da attaccanti di profilo basso o medio.

Richiedono pero' di funzionare su sistemi non compromessi, e mantenere un sistema sano puo' essere molto difficile, mentre infiltrare un sistema poco controllato e', al giorno d'oggi, una attivita' quasi di routine.

Grazie a tutti per l'attenzione

ci sono domande ?

Potete contattarmi all'indirizzo:

marcoc@winstonsmith.info

Il Progetto Winston Smith

http://www.winstonsmith.info/pws

freenet:SSK@Dgg5lJQu-WO905TrlZ0LjQHXDdIPAgM/pws/17//

Bibliografia

Bibliografia

- **“Kriptonite: fuga dal controllo globale”** - *Joe Lametta* Edizioni Shake, 1998 (disponibile in rete)
- **“Code: and other law of Cyberspace”** - *Lessig Lawrence* Basic Books, 1999
- **Pgp** http://www.pgpi.org
- **Mixmaster** http://www.mixmaster.net
- **Freenet** http://www.freenetproject.org/ https://lists.firenze.linux.it/mailman/listinfo/freenet-list
- **Tor** http://tor.eff.org
- **Progetto Winston Smith** http://www.winstonsmith.info