E-privacy & Infosmog

Verso un approccio integrato alla gestione individuale della privacy dei dati

Marco A. Calamari - marco@dada.it

Il Progetto Freenet

Firenze Linux User Group

Il Progetto Winston Smith

Ovvero ….

…. come cancellare i propri dati

Siete al seminario giusto ?

In questo seminario verranno trattate a livello elementare le problematiche di gestione dati relative alla privacy personale.

Ci concentreremo, data la ristrettezza dei tempi, sulla gestione dei dati locali ad un singolo computer, ed in particolare sulle modalita' di gestione dei dati che debbano, se e quando necessario, poter essere completamente eliminati, cosa complessa da realizzare in pratica.

Con questi limiti, arriveremo a poter fornire "ricette" pratiche per realizzare questo obbiettivo.

... ma ...

... non e' semplicissimo cancellare i dati ?

"Ma non e' banale cancellare i dati ?"

In una parola, no!

"Ma come, a me e' capitato di perdere l'agenda elettronica, la tesi, il sorgente del programma, la presentazione per il cliente ..... e' stato facilissimo!"

Infatti, ma questa e' normale trascuratezza, unita alla legge di Murphy, ai suoi corollari ed all'acutissima vista della sfiga.

Per non perdere i propri dati, ma poterli gestire ed eliminare in sicurezza. bisogna tra affrontare e risolvere problemi tecnici, di gestione dei dati e di gestione delle copie di backup. Sara' infatti evidente nel prosieguo che uno dei maggiori problemi da affrontare e' il proliferare dei dati dovuto all'esecuzione non metodica e pianificata di copie.

"Quindi per poter cancellare i dati non devo farne copie di sicurezza ?" No, le copie di sicurezza sono indispensabili ma per poter essere certi di poter sia conservare in sicurezza che eliminare i dati, e' necessario gestirle accuratamente e con metodo. Alla fine di questo intervento potremo delineare alcuni semplici regole per conservare con sicurezza i propri dati ed eliminarli con altrettanta certezza.

E se siete tra quelli che non fanno periodicamente copie di sicurezza, non pensate per questo che per voi sia piu' semplice cancellare i dati; e' solo molto piu' facile che li perdiate!

Infosmog

Infosmog, s.m.

la nuvola di dati che ciascuno produce e disperde nella societa' dell'informazione e nel cyberspazio.

Cerchiamo innanzitutto di capire perche' puo' essere necessario, anche per chi "non ha niente da nascondere" cancellare in maniera completa alcuni dati.

Nello scorso millennio e' stato coniato il termine Infosmog per definire la nuvola di dati che ciascuno produce e disperde nella societa' dell'informazione e nel cyberspazio. Siamo tutti nella situazione di Pig Pen, l'amico di Charlie Brown che viveva perennemente immerso in una nuvola personale di polvere e sporco.

Noi parliamo invece di una nuvola di dati; ogni nostra azione produce dati, che sono, nel senso ampio in cui e' necessario intenderli, dati personali; dovrebbero quindi essere tutelati dalla legge 675/96 sulla privacy, perche' appartenenti a chi li ha generati. Purtroppo le cose in Italia non stanno cosi', ma questa e' un'altra storia …… anche perche' all'estero la situazione e' peggiore!

Comprare una scheda telefonica, varcare il tornello di una banca, attraversare un casello autostradale, pagare con bancomat e carta di credito, telefonare col cellulare, fare la spesa con la carta fedelta', producono dati personali, atipici ma pur sempre personali, che vengono dispersi e dei quali perdiamo subito ogni possibilita' di controllo.

Usare un computer poi produce dati in quantita' industriale; in giro per l'hard disk, i floppy ed i cdrom ci sono quantita' incredibili di dati personali.

Non sto parlando solo dei documenti, delle presentazioni e dei programmi che avete scritto, ma anche e soprattutto della posta elettronica che avete spedito e ricevuto, dei bookmark dei siti che avete visitato memorizzati non sapete dove dal vostro browser, dei dati e delle immagini conservate nella cache del browser o nella cartella dei documenti recenti, nelle preferenze di ciascun programma .... e cosi' via.

Tutti i sistemi operativi, grafici e no, proprietari o liberi, fanno del loro meglio per moltiplicare e nascondere informazioni personali in giro per l'hard disk; in questo campo i software proprietari e liberi si comportano piu' o meno nello stesso modo. Sui dati del nostro computer, e solo su questi, abbiamo grandi possibilita' di gestione e controllo; il problema e' quello di convincersi dell'utilita' e della necessita' di attuarle.

Non si tratta di un atteggiamento paranoico, per quanto essere paranoici nel cyberspazio sia una virtu' e non un difetto, ma semplicemente razionale; non posso gestire i miei dati se non sono in grado di cancellarli.

Un esempio - l’agenda elettronica

Dato il carattere pratico di questo seminario, affronteremo il problema della cancellazione dei dati partendo da un esempio tipico, che probabilmente tutti abbiamo sul pc:

l'agenda degli appuntamenti e dei numeri di telefono.

Affrontiamo il problema della cancellazione dei dati partendo da un esempio tipico, che probabilmente tutti abbiamo sul pc, l'agenda degli appuntamenti e dei numeri di telefono.

Un'agenda e' l'immagine delle relazioni sociali di un individuo, e quindi e' un'informazione da gestire con la massima cura dal punto di vista della privacy. Anche cittadini esemplari, persone perbene e beneducate non amerebbero che il loro partner/capo/genitore venisse a completa conoscenza di tutti gli appuntamenti e contatti telefonici; tutti quegli incontri del giovedi' pomeriggio con la stessa persona potrebbero essere fraintesi. Vogliamo quindi conservare in maniera affidabile questi dati, ed essere tuttavia in grado di eliminarli definitivamente quando necessario.

Localizzazione dei dati

- **Prima regola** - sapere dove si trovano i dati, ed in che formato sono
- **Seconda regola** - sapere se i dati della nostra agenda vengono copiati, anche solo temporaneamente, in altri posti come in file temporanei generati dai programmi, o peggio ancora trasmessi in rete.
- **Terza regola** - tenere sempre conto che se non vengono adottati particolari e non banali accorgimenti, un dato memorizzato in un computer / database / server non direttamente e completamente sotto il vostro controllo deve essere considerato non riservato.

Ma prima di tutto, dove si trova la nostra agenda ? Quella di carta, con la copertina rossa di pelle si trova probabilmente nella borsetta o nella ventiquattrore, ma quella informatica ? E' nella memoria del palmare, sul pc nel programma di posta elettronica, oppure in un programma dedicato ? O magari in tutti questi posti contemporaneamente ?

Ah, sta solo nell'hard disk del mio computer ! Si, ma dove ? Nel registry, in una oscura directory puntoqualchecosa od in un file sepolto sotto 6 livelli di directory e difeso da un nome piu' criptico che se fosse scritto in katakana o cuneiforme-B ?

Prima regola - dobbiamo ASSOLUTAMENTE sapere dove si trovano i dati, ed in che formato sono; va da se che se sono contenuti in un unico file ed un unico oggetto, possono essere gestiti in maniera incomparabilmente piu' semplice che se sono dispersi in diversi file, directory o database

Seconda regola - e' necessario sapere se i dati della nostra agenda vengono copiati, anche solo temporaneamente, in altri posti come in file temporanei generati dai programmi, o peggio ancora trasmessi in rete. Siccome questa e' purtroppo la norma, i file temporanei, quando presenti, devono essere considerati parte integrante dei vostri dati personali.

Terza regola - dobbiamo aver sempre presente che se non vengono adottati particolari e non banali accorgimenti, di cui accenneremo tra breve, un dato memorizzato in un computer / database / server non direttamente e completamente sotto il vostro controllo deve essere considerato non riservato; se poi il dato viene trasmesso in rete, deve essere considerato di dominio pubblico.

Requisito per la cancellazione sicura della nostra agenda - sapere sempre esattamente dove si trovano i dati, comprese le loro copie temporanee e di backup, ed essere certi che non vengano mai trasmesse

Cancellazione sicura dei dati

La possibilita’ di cancellare completamente un dato contrasta con la necessita’ di effettuare copie di backup e di trasmettere il dato stesso

Supponiamo quindi di sapere esattamente dove ed in quale formato siano i dati della nostra agenda elettronica ed i relativi file temporanei; siamo altrettanto tranquilli di sapere anche dove sono tutte le loro copie. sia eseguite consapevolmente come backup che inconsapevolmente?

Senza pretendere di affrontare ora questo problema, annotiamo mentalmente che e' necessario gestire il backup non solo per essere sicuri di averne uno abbastanza aggiornato al bisogno, ma anche per poterli cancellare quando non piu' necessari, al fine di ridurre la nostra nuvola di Infosmog.

Se siete preoccupati dei vostri dati e ne fate spesso copie, dovrete ripensare il modo con cui le fate, altrimenti non sarete mai in grado di cancellare niente con certezza. Un effetto secondario piacevole di questo sforzo di autodisciplina sara' quello di evitare di essere sommersi da floppy e cdrom di cui non ricordate piu' il contenuto.

I modelli di minaccia

- **Modello di minaccia basso**: le informazioni sono minacciate dal collega curioso o malizioso che va a leggere i dati dal nostro pc, o dalla fidanzata/o gelosa/o che legge la posta elettronica, il log della chat ed i numeri di telefono dell'agenda.
- **Modello di minaccia medio**: le informazioni sono minacciate da un ladro, da una persona "esperta" di computer, da un consulente tecnico di parte della moglie/marito che vuole il divorzio, o da un'azienda concorrente che vuole ridurre i propri costi di ricerca & sviluppo
- **Modello di minaccia alto**: le informazioni sono minacciate da organizzazioni governative o non governative, con mezzi illimitati e non vincolate delle leggi ordinarie, quali mafie, servizi segreti, forze armate in tempo di guerra ed organizzazioni terroristiche.

Ma che modello di minaccia; in fondo io non ho niente (beh, quasi niente…) da nascondere; perche' dovrei mettermi a giocare alle spie?

Semplice, perche' la gestione in sicurezza dei dati si fa cosi'; in tutti i campi della scienza e della tecnica si seguono le regole dell'arte. Bisogna quindi seguire le regole auree della sicurezza anche per gestire in maniera sicura e riservata i propri dati. Uno dei paradigmi fondamentali della sicurezza e' che per progettare un sistema sicuro, dopo aver identificato che cosa bisogna proteggere, dobbiamo identificare da che e/o che cosa dobbiamo proteggerci, quale e' insomma il nostro “modello di minaccia”.

Avendo noi esigenze semplici, definiremo tre rozzi ma efficaci modelli di minaccia, e li battezzeremo, con uno sforzo immane di fantasia, basso, medio ed alto

Modello di minaccia basso: le informazioni sono minacciate dal collega curioso o malizioso che va a leggere i dati dal nostro pc, o dalla fidanzata/o gelosa/o che legge la posta elettronica, il log della chat ed i numeri di telefono dell'agenda.

Modello di minaccia medio: le informazioni sono minacciate da un ladro, da una persona "esperta" di computer, da un consulente tecnico di parte della moglie/marito che vuole il divorzio, o da un'azienda concorrente che vuole ridurre i propri costi di ricerca & sviluppo

Modello di minaccia alto: le informazioni sono minacciate da organizzazioni governative o non governative, con mezzi illimitati e non vincolate delle leggi ordinarie, quali mafie, servizi segreti, forze armate in tempo di guerra ed organizzazioni terroristiche.

Diciamo subito che contro un modello di minaccia alto e' inutile illudersi che esista una strategia informatica efficace, questo perche' la parte informatica (che puo’ essere comunque praticamente inviolabile se correttamente implementata e gestita) non e' che un anello della catena di sicurezza complessiva.

In questo caso usualmente e' l'elemento umano l'anello piu' debole del sistema, ed in particolare la sua tendenza a non rifiutare di fornire informazioni che siano richieste da un professionista in maniera non convenzionale e convincente.

Restano quindi gli altri due modelli, basso e medio, contro cui possono essere messe in atto contromisure tecniche, di cui ora esamineremo gli ingredienti principali.

Localizzazione e segregazione dei dati

- **Salvare tutti i dati sotto una unica directory, strutturandone il contenuto con un adeguato numero di sottodirectory, e non salvate mai niente al di fuori di essa. Il salvare tutti i dati in un posto solo rende tra l'altro molto piu' semplici le operazioni di backup e di migrazione dei dati da un computer vecchio ad un nuovo**

- **Porre particolare attenzione a dove vengono memorizzati i messaggi, gli indirizzi di posta, i bookmark dei browser; normalmente queste applicazioni permettono di solito di modificare i default e quindi memorizzare questi dati nel vostro albero di directory.**

- **Settare tutte le applicazioni che lo permettono perche' salvino nella sottodirectory opportuna, e di tanto in tanto controllate di non aver salvato qualcosa al di fuori con una ricerca su tutto il disco.**

Prerequisito per qualunque gestione in sicurezza dei dati e' sapere esattamente dove sono memorizzati. Salvate abitualmente i dati dove la vostra applicazione od il vostro sistema operativo ritengono sia meglio ?

Madornale errore! Voi sapete, dovete sapere, dove e' meglio che stiano i vostri dati. Salvate tutto sotto una unica directory, strutturandone il contenuto con un adeguato numero di sottodirectory, e non salvate mai niente al di fuori di essa. Il salvare tutti i dati in un posto solo rende tra l'altro molto piu' semplici le operazioni di backup e di migrazione dei dati da un computer vecchio ad un nuovo

Ponete particolare attenzione a dove vengono memorizzati i messaggi, gli indirizzi di posta, i bookmark dei browser; normalmente queste applicazioni permettono di solito di modificare i default e quindi memorizzare questi dati nel vostro albero di directory.

Regolate quindi tutte le applicazioni che lo permettono perche' rispettino la vostra volonta', e di tanto in tanto controllate di non aver salvato qualcosa al di fuori con una ricerca su tutto il disco.

Uso di media rimuovibili

L’uso di media rimuovibili (floppy, cdrom, nastri, schede di memoria, hard disk esterni) deve essere inquadrato in una ottica globale nella strategia di gestione dei dati

Il media rimuovible complica la gestione dal punto di vista della sicurezza fisica

Memorizzare i dati su un pc implica i doverli lasciare li quando si torna a casa dall'ufficio (o viceversa). Utilizzare supporti rimuovibili per la memorizzazione permanente dei dati implica che la loro affidabilita' sia sufficientemente alta,

Il supporto rimuovible sposta il problema della sicurezza dal solo piano informatico a quello anche fisico; se lasciate il floppy nella borsa, un ladro ve la puo' rubare od il collega curioso puo' farsi rapidamente una copia del floppy o del cdrom

Gestione dei file temporanei

I file temporanei e di swap devono essere considerati come facenti parte dei vostri dati riservati, perche' possono contenerne copie.

La loro gestione va quindi fatta allo stesso livello di sicurezza

Identificare ed eliminare file temporanei puo' essere fatto semplicemente osservando dove i programmi che usiamo memorizzano questi file, e spostandoli su dischi RAM, che vengono cancellati con sicurezza ogni volta che il computer viene spento.

E' anche possibile inserire tra i programmi che partono automaticamente al boot od allo shutdown un file di comandi od un programma che cancelli file e directory temporan

Gestione delle copie di sicurezza

La strategia di backup deve essere un compromesso tra la necessita' di recuperare dati e quella di poterli cancellare.

L'eliminazione di un singolo file dal disco deve prevedere la sua eliminazione da tutte le copie di sicurezza, od almeno garantire di poterlo rendere inaccessibile.

Gestite in maniera metodica i supporti di backup, essi sono parte integrante dei vostri dati. Oltre a conservarli in modo tale che la distruzione/furto del computer non implichi anche quella dei backup, decidete il loro riutilizzo e/o distruzione in base alla vostra necessita' di storicizzare i dati.

Cancellare un singolo file implica la necessita' di cancellarlo anche da tutte le copie di backup; puo' essere conveniente concentrare le informazioni piu' critiche (ad esempio la posta, le lettere di affari od i dati di R&S) in una directory a parte da gestire con una procedura di utilizzo e backup particolare.

Vedremo nel seguito che partizioni criptate possono possono essere molto utili in questi casi.

Gestione degli hard disk

- **Gli hard disk devono essere considerati supporti rimuovibili nel caso che vengano inviati in riparazione, sostituiti, riciclati o venduti.**
- **Devono quindi essere formattati a basso livello (consultate le specifiche della periferica e del controller) o distrutti**
- **Un hard disk guasto deve essere comunque distrutto**

Anche gli hard disk possono rientrare tra i supporti rimuovibili, se vengono inviati in riparazione, sostituiti, riciclati o venduti.

Nel modello di minaccia basso una formattazione a basso livello oppure una cancellazione della partition table e' sufficiente.

Se il modello di minaccia e' medio e' necessaria una cancellazione sicura dei dati, da eseguirsi con programmi appositi che cancellano piu' volte i dati sovrascrivendoli con pattern diversi, in modo da eliminare le tracce che rimangono con una singola sovrascrittura; esistono apparecchiature automatizzate che consentono di analizzare dischi sovrascritti una sola volta di cui parleremo tra poco.

Paradossalmente un hard disk guasto e' il supporto piu difficile da gestire; in un modello di minaccia basso il guasto in se e' sufficiente, mentre e' assolutamente insufficiente in quello medio. Il guasto impedisce pero' qualunque forma di cancellazione dei dati, per cui e' necessario distruggere meccanicamente i dischi con un buon martello, poiche' per quanto detto la distruzione della parte elettronica' (gia'a avvenuta) e' assolutamente insufficente.

Resta sempre valido l'utilizzo del vecchio caminetto; anche se l'alluminio pressofuso non brucia, portare la temperatura di un supporto magnetico oltre il punto di Curie (circa 500 gradi, calor rosso scuro) elimina qualunque traccia di magnetizzazione e distrugge chimicamente i rivestimenti magnetici dei piatti.

Trasmissione sicura dei dati

- **E’ un argomento complesso**
- **Ci sono i mezzi informatici per gestirla (Pgp/Gpg, SSH, stunnel, etc.)**
- **Non ce ne possiamo occupare in questa sede per motivi di tempo**
- **Nel prosieguo dobbiamo quindi escluderla da tutti i nostri modelli**

Trasmettere dati in rete, incluso via modem, GSM o Wi-Fi equivale ad averli resi pubblici e quindi averli posti aldila' di qualunque possibilita' di controllo.

La trasmissione deve quindi essere evitata quanto piu' possibile; ove fosse necessaria e' indispensabile l'oculato utilizzo di programmi di crittografia forte. Pgp/Gpg, SSH ed stunnel sono le risposte classiche a questa necessita', che non possono purtroppo trovare spazio in questa breve introduzione.

Cancellazione sicura di file

- **Cancellazione delle aree dati**
- **Cancellazione delle entry nella directory**
- **Cancellazione dello slack space**
- **Cancellazione con sovrascrittura multipla (DoD 5200.28-STD)**

- Mezzi e strumenti

Ed ora passiamo agli strumenti necessari per realizzare quanto ci siamo prefissi, e cioe' conservare in maniera affidabile e riservata, ed all'occorrenza poter cancellare in maniera completa i dati

- Cancellazione sicura di file

Sono ormai poche le persone convinte che per cancellare un file basti metterlo nel cestino e vuotarlo.

Come fortunatamente molti ormai sanno, e' indispensabile sovrascrivere i dati cancellati per avere un minimo di sicurezza, altrimenti essi possono essere recuperati in maniera veloce e completa con una miriade di programmi reperibili sia commercialmente che su internet.

Ma una parte dei dati restano memorizzati su disco anche dopo una sovrascrittura.

I dati su un disco vengono memorizzati in blocchi di lunghezza fissa, che vengono riempiti di dati; l'ultimo blocco di un file resta quindi parzialmente vuoto, ed i dati presenti in tale blocco dopo l'ultimo byte del file (detto slack space) sono ancora quelli precedenti, e non verranno mai sovrascritti fino a quando il file non verra' cancellato.

Ma anche i nomi assegnati ai file possono di per se' contenere informazioni; pensate ad un file "Lettera a Babbo Natale.txt" in cui ai nomi del simpatico vecchietto fosse sostituito da quello di altri protagonisti della cronaca. La semplice cancellazione del file rende riutilizzabile la riga della directory, ma non la sovrascrive fino a quando non verra' riutilizzata.

Infine, poiche' praticamente tutti i sistemi operativi esistenti gestiscono la memoria in modo virtuale, quando un programma manipola dati, puo' capitare che parti di esso e dei dati che sta manipolando vengano temporaneamente copiati nel file o nella partizione di swap.

Questa complessa situazione puo' per fortuna essere affrontata in maniera unitaria; esistono infatti numerosi programmi di cancellazione sicura che sovrascrivono una o piu' volte con dati casuali sia i file che i loro nomi, che cancellano lo slack space ed i file di swap.

Installare ed usare metodicamente un programma di questo tipo e' praticamente indispensabile, e per fortuna ce ne sono di semplici da usare.

Protezione mediante password

- **L’utilizzo di password e’ indispensabile per qualunque sistema di sicurezza informatica**
- **Non sentitevi furbi quando le scegliete; ci sono documenti appositi sulle strategie per crearle e memorizzarle**
- **In un contesto di privacy, la password e’ l’unica chiave per accedere ai dati; persa (o compromessa) quella ……**
- **Token, smartcard, biometria: ma per piacere …… (da considerare solo come misure aggiuntive)**

In ultima analisi tutti i sistemi di memorizzazione sicura richiedono l'uso di una o piu' password.

Una corretta scelta ed utilizzo di password e' indispensabile; il bilanciamento tra la necessita' di non dimenticare una password e la necessita' di sceglierla "difficile", di cambiarla di frequente e di non scriverla e' un onere tutto vostro.

Due consigli; il primo e' quello di non sentirsi mai furbi quando si sceglie una password, ed il secondo quello di leggere documenti a proposito che si possono facilmente trovare su internet con un motore di ricerca.

La protezione mediante password e' efficace quanto chi ha scritto il programma che la usa ha deciso; la protezione mediante password di un noto word processor puo' essere facilmente violata con un programmino a portata di mano di chiunque sappia usare il solito motore di ricerca.

Fidarsi delle protezioni fornite da singole applicazioni non dedicate alla sicurezza e’ sconsigliabile anche in un modello di minaccia basso, perche’ complica la gestione, e del tutto insufficiente in un modello di minaccia medio.

Criptatura di file e partizioni

- **I dati possono essere memorizzati in file, directory o partizioni crittografate con algoritmi forti**
- **l'utilizzo di questi metodi permette di risolvere molti problemi di gestione riservata dei dati**
- **la robustezza dei metodi utilizzati da questi programmi non deve ingenerare una falsa sensazione di sicurezza**
- **Alcuni software: Pgp for personal privacy, BestCrypt , StegoFS**

I dati possono essere memorizzati in file, directory o partizioni crittografate con algoritmi forti; l'utilizzo di questi metodi permette di risolvere molti problemi di gestione riservata dei dati; la robustezza dei metodi utilizzati da questi programmi non deve ingenerare pero' una falsa sensazione di sicurezza.

Un programma di criptatura utilizzato in maniera trascurata puo' essere inutile o peggio portare alla perdita irreversibile di dati.

Purtuttavia criptare una partizione dell'hard disk e' l'unico sistema per poter conservare insieme le varie tipologie di dati e gestirli in sicurezza senza complicarsi troppo la vita.

I programmi per criptare partizioni creano un file sul disco del computer della stessa dimensione della partizione criptata che si vuole realizzare; questo file puo' essere montato e smontato esattamente come un disco rimuovibile, e quando montato viene visto esattamente come un disco.

Quando e' necessario montare il disco, deve essere fornita la passphrase; e' poi conveniente abilitare i meccanismi di sicurezza per lo smontaggio automatico; e' infatti possibile definire un periodo di inattivita' a piacere, trascorso il quale il disco viene smontato automaticamente.

In questo modo anche se vi dimenticate il portatile incustodito, il rischio che qualcuno possa accedere ai dati protetti viene largamente ridotto.

E' poi possibile definire una combinazione di tasti che smonta immediatamente la partizione criptata, che potete utilizzare quando dovete abbandonare il computer incustodito o se dovete improvvisamente rendere inaccessibili i dati.

L'utilizzo di questi programmi e' piu' che sufficente anche nel caso di un modello di minaccia medio; in effetti sarebbero adeguati anche per un modello di minaccia alto, perche' molto "robusti" dal punto di vista della sicurezza crittografica.

Alcuni di questi programmi permettono di "nascondere" i dati, in modo da poterne negare in maniera plausibile l'esistenza.

E' infatti piuttosto difficile sostenere che su un computer con partizioni criptate non siano presenti dati riservati; ovviamente se ne puo' negare l'accesso, ma non l'esistenza, almeno non in maniera plausibile. E' l'esistenza stessa del programma usato che non lo permette.

E' tuttavia possibile definire partizioni criptate utilizzando lo spazio libero di altre partizioni criptate; attivando questo particolare meccanismo viene definita una ulteriore password che monta non la partizione criptata ma la partizione criptata "interna".

In questo modo si possono memorizzare nella partizione criptata delle copie di dati senza importanza, e mettere i dati "veri" all'interno della partizione criptata nascosta.

Alla richiesta della password, si fornira' quella della partizione interna; in questo modo non si accederanno i dati "falsi" ma quelli veri.

Fornendo invece la password della partizione normale, l'esistenza della partizione interna non puo' essere dedotta nemmeno

- Dischi RAM

- **I dischi Ram si cancellano completamente quando il computer viene spento**
- **devono avere dimensioni sufficienti da poter contenere i file temporanei piu' grossi ragionevolmente necessari**
- **allocare dischi Ram piu' grandi del necessario e' controproducente perche' si aumenta la possibilita' che la memoria Ram utilizzata dal disco venga swappata su file**
- **I dischi ram si creano normalmente con funzionalita' gia' comprese nel sistema operativo**

Abbiamo gia' sottolineato l'esigenza di gestire i dati temporanei (siano essi file normali o di swap) con la stessa attenzione riservata ai dati, perche' essi possono sempre contenerne delle copie parziali.

Creare dischi ram e' un'operazione molto semplice, ed e' sufficiente caricare un device driver o lanciare un programma per avere una directory od una unita' logica di dimensioni opportune che si trova in Ram, e che quindi viene cancellata irreversibilmente ad ogni spegnimento del computer.

E' necessario poi individuare dove le singole applicazioni salvano i file temporanei, e modificare i settaggi di default in modo che li salvino invece nel disco Ram.

Il disco Ram deve ovviamente avere dimensioni sufficienti da poter contenere i file temporanei piu' grossi ragionevolmente necessari; allocare dischi Ram piu' grandi del necessario e' controproducente perche' si sottrae ram alle altre applicazioni, e nel caso di dischi definiti in user space, perche' si aumenta la possibilita' che la memoria utilizzata dal disco venga swappata su file.

File di swap

- **I file di swap sono aree temporanee di memorizzazione gestite direttamente dal sistema operativo**
- **Le informazioni che vi vengono scritte non sono cancellate fino a sovrascrittura**
- **Possono essere cancellati con apposite utility**
- **Possono essere criptati, in modo che le informazioni scritte diventino irrecuperabili dopo il reboot**

Come gia accennato il file di swap sono una “pattumiera di informazioni” che deve essere svuotata appena possibile; esistono suite di sicurezza che forniscono per questo scopo due tipi di funzonalita’.

La prima e’ una banale funzionalita’ di sovrascrittura del file di swap con dati casuali, da attivare sia manualmente quando necessario, sia con job temporizzati od allo spegnimento del computer.

La seconda prevede invece di creare il file di swap su una partizione criptata; la chiave di criptazione viene generata a caso ad ogni avvio del computer e cancellata allo spegnimento.

In questo modo il file di swap, al successivo avviamento potra’ sempre contenere dati sensibili, ma questi dati saranno stati crittografati con una chiave cancellata e non riproducibile e saranno quindi inaccessibili.

Il recupero dei dati cancellati ...

… non e’ mai possibile, e non deve esserlo, ovviamente almeno “all’interno” del modello di minaccia prescelto

… non e’ mai possibile, e non deve esserlo, ovviamente almeno “all’interno” del modello di minaccia prescelto.

Per fare un esempio, in un modello di minaccia basso non e’ previsto che l’attaccante utilizze un disk editor, cosa che permette il recupero di dati non sovrascritti; nel caso che sia concepibile l’utilizzo di un tale tipo di applicazione, il modello di minaccia basso non e’ sufficiente ed e’ necessario almeno un modello di minaccia medio.

Ed in un modello di minaccia medio, non e’ previsto che l’attaccante utilizzi sistemi basati sulla microscopia elettronica ad effetto tunnel, che permettono di recuperare dati sovrascritti sono una o poche volte.

Non si tratta di sistemi fantascientifici; sono apparecchiature sofisticate e costose, che pero’ possono essere noleggiate da ditte specializzate a circa 2000 euro/ora, su cui si monta l’hard disk privato del controller, e che sono dotati di software di recupero dati molto sofisticati e semiautomatici, alla portata non solo di agenzie governative.

In questo caso e’ necessario salire ad un livello di sicurezza alto (realizzabile, per quanto detto prima, solo per la parte informatica) ed adottare algoritmi di cancellazione almeno al livello delle specifiche DoD 5200.28-STD, che prevedono pattern e sequenze particolari di sovrascrittura dei dati.

Personalmente, applicando il principio che la paranoia e’ una virtu’, trovo curioso che da oltre dieci anni non vengano piu’ pubblicati lavori di ricerca significativi sulla cancellazione sicura dei dati, e che la stessa specifica citata sia divenuta difficilissima

Olio di serpente

Parecchie applicazioni di cancellazione dati che si vantano di implementare mezzi sicuri e raffinati sono inutili, anzi rappresentano un vero e proprio olio di serpente

E' indispensabile una valutazione complessiva del sistema informatico che includa hardware, firmware, driver, sistema operativo ed applicazioni

Anche se puo' sembrare sorprendente, parecchie delle applicazioni di cancellazione dati che vantano di implementare queste specifiche' sono inutili, anzi rappresentano un vero e proprio olio di serpente.

Apriamo una parentesi, non tanto per il problema particolare, ma per dimostrare come sia in realta' difficile implementare correttamente modelli di minaccia alti.

Lo standard a cui si fa riferimento e' quello succitato del DoD, ed il lavoro di ricerca su cui e' basato, che e' uno degli ultimi facilmente reperibili e' "Secure Deletion of Data from Magnetic and Solid-State Memory" di Peter Gutmann, pubblicato alla sesta conferenza USENIX nel 1996.

I software di cancellazione sicura che fanno riferimento a quello standard applicano i pattern di cancellazione individuati da Guttmann in questo lavoro; il problema e' che questi pattern sono dipendenti sia dall'hardware che dai device driver e dal sistema operativo usati.

I pattern del paper suddetto sono validi soltanto nel caso di dischi che utilizzino la codifica RLL, e che siano privi di cache hardware sul controller onboard e sul controller lato computer.

Praticamente nessun compter recente soddisfa a queste caratteristiche, quindi i software che vantano l'aderenza al DoD 5200.28-STD sono probabilmente poco o punto efficaci, e dannosi in quanto ingenerano un falso senso di sicurezza

Gestione e distruzione dei supporti

- **Per quanto detto, come raccomanda anche il DoD, in un modello di minaccia medio od alto la formattazione dei supporti e degli hard disk non e' sufficiente a garantire una cancellazione sicura dei dati.**
- **E' quindi consigliabile, nel caso di hard disk, prevedere formattazioni di basso livello ben documentate, e pianificare appena possibile la distruzione fisica dei supporti rimuovibili, ormai quasi tutti di basso costo.**
- **Le procedure standard DoD per la distruzione di dati in situazioni di emergenza (di teatro o di evacuazione) prevedono la distruzione dei supporti come metodo di elezione**

Da quanto abbiamo detto, e da quanto raccomanda anche il DoD, in un modello di minaccia medio od alto la formattazione dei supporti e degli hard disk non e' sufficiente a garantire una cancellazione sicura dei dati.

E' quindi consigliabile, nel caso di hard disk, prevedere formattazioni di basso livello ben documentate, e pianificare appena possibile la distruzione fisica dei supporti rimuovibili, ormai quasi tutti di basso costo.

Le procedure standard DoD per la distruzione di dati in situazioni di emergenza (di teatro o di evacuazione) prevedono infatti la distruzione dei supporti come metodo di elezione, prevedendo la concentrazione dei dati sensibili su supporti rimuovibili, gestibili in maniera indipendente dalla apparecchiature informatiche.

Ricetta: modello di minaccia basso

- In un modello di minaccia basso questi accorgimenti sono di norma sufficienti:
  - password di boot
  - screen saver con password
  - concentrazione dei dati in un'unica directory
  - gestione in sicurezza dei backup con riciclo ed eventuale distruzione dei supporti
  - utilizzo di una partizione criptata con smontaggio automatico temporizzato

Bene, il nostro excursus teorico e' durato abbastanza, ma la necessita' di coprire completamente, anche se ad un livello elementare, una problematica cosi' sfaccettata richiedeva un spazio adeguato.

Allora, cosa puo' essere consigliato per coprire necessita' ordinarie nel caso dei modelli di minaccia che abbiamo elencato ?

In un **modello di minaccia basso** questi accorgimenti sono di norma sufficienti:password di boot

- screen saver con password
- concentrazione dei dati in un'unica directory
- gestione in sicurezza dei backup con riciclo ed eventuale distruzione dei supporti
- utilizzo di una partizione criptata con smontaggio automatico temporizzato

L'utilizzo della partizione criptata potrebbe sembrare eccessivo in un modello di minaccia destinato ad utenti con poche esigenze e magari di non grandi conoscenze informatiche.

In realta' l'utilizzo della partizione criptata, che puo' anche essere inizializzata con l'aiuto di una persona piu' esperta, e che non richiede nessuna conoscenza particolare per l'utilizzo, e' senz'altro fattibile, di alto valore aggiunto per la sicurezza dei dati anche da parte di utenti poco esperti.

Alcune versioni di windows supportano l'utilizzo di file e partizioni criptate a livello di sistema operativo.

La parte veramente dfficile da realizzare in un modello di gestione dei dati in sicurezza e' la segregazione dei dati e la disciplina per la gestione dei loro backup.

L'utilizzo della partizione criptata permette di realizzare backup sicuri facendo la copia del singolo file che contiene la partizione, e che puo' facilmente essere copiato su un supporto rimuovibile.

I backup stessi sono quindi protetti dalla medesima password della partizione, e la loro sottrazione non provocherebbe nessun danno.

E' da notare comunque che scelta, memorizzazione e gestione della password diventano di importanza centrale; la perdita di un'unica password renderebbe inaccessibili tutti i dati della partizione criptata; la compromissione della stessa password renderebbe privi di protezione tutti i dati.

Tutte le distribuzioni di GNU/Linux e le versioni di Windows sono dotate di screen saver con password, e tutti i personal computer Intel sono dotati di BIOS con password di boot; i primi due punti dell'elenco sono qundi facilmente soddisfatti.

La realizzazione di partizioni criptate in ambiente windows puo' avvenire con diversi prodotti commerciali e non; uno dei piu''semplici e' la suite Pgp for personal privacy di Computer Associates, che oltre ad una versione proprietaria di Pgp comprende anche un'utility per la gestione di partizioni criptate.

Un altro prodotto che merita adeguata considerazione e' BestCrypt della Jetico Inc.; si tratta di un prodotto odedicato,

Ricetta: modello di minaccia medio

- **In un modello di minaccia medio, queste precauzioni sono di norma sufficienti (le prime 5 sono le stesse previste per il modello medio):**
  - password di boot
  - screen saver con password
  - concentrazione dei dati in un'unica directory
  - gestione in sicurezza dei backup con riciclo ed eventuale distruzione dei supporti
  - utilizzo di una partizione criptata con smontaggio automatico temporizzato
  - utilizzo di un disco Ram per la gestione dei file/dati temporanei
  - utilizzo di un programma per la cancellazione del file di swap
  - utilizzo di programmi per la cancellazione sicura dei file e per la pulizia dei dischi

In un **modello di minaccia medio**, queste precauzioni sono di norma sufficienti (le prime 5 sono le stesse previste per il modello medio:

password di boot

- screen saver con password
- concentrazione dei dati in un'unica directory
- gestione in sicurezza dei backup con riciclo ed eventuale distruzione dei supporti
- utilizzo di una partizione criptata con smontaggio automatico temporizzato
- utilizzo di un disco Ram per la gestione dei file/dati temporanei
- utilizzo di un programma per la cancellazione del file di swap
- utilizzo di programmi per la cancellazione sicura dei file e per la pulizia dei dischi

In ambiente GNU/Linux un ramdisk puo' essere realizzato con le funzionalita' base del sistema operativo (in effetti durante il boot i sistemi unix-like utilizzano appunto un ramdisk).

In ambiente da dos fino a Windows 98SE puo' essere usato il device driver ramdisk.sys, mentre su NT, 2000 e XP e' reperibile su sito Microsoft un archivio ramdrive.exe che contiene il driver, file di supporto ed istruzioni.

C'e' da dire che utilizzare Windows 2000 SP3 o qualunque versione di WindowsXP per la gestione in sicurezza dei dati e', a parere mio e di molti altri, un controsenso, ma qui il discorso diventa molto piu' ampio e non abbiamo certo il tempo di affrontarlo.

Per la cancellazione dei file di swap esistono diverse utility, sia proprietarie che freeware o software libero.

Ambedue i prodotti che abbiamo citato precedentemente tuttavia le includono, e la loro eventuale scelta implica ragionevolmente anche quella della corrispondente utility. Sarebbe opportuno che la cancellazione del file di swap non avvenisse solo a mano, ma che fosse automaticamente eseguita allo startup o meglio allo shutdown del sistema, con i metodi previsti dal sistema operativo che si sta impiegando.

Infine, malgrado le precauzioni impegate, puo' capitare di dover copiare dei dati sensibili sul disco fisso (non criptato) del computer, sia perche' si tratta di dati che l'applicazione scrive in posti fissi che perche' ci si e' sbagliati; in questo caso, per i motivi che abbiamo elencato precedentemente, e' necessario cancellare lo slack space dei file, le entry inutilizzate delle directory ed ovviamente sovrascrivere tutto lo spazio libero presente sul disco.

Ricetta: modello di minaccia alto

Elenchiamo alcune linee guida che si impiegano, per la sola parte informatica, nel caso di un modello di minaccia alto.

•Tutti gli accorgimenti del modello medio sono un prerequisito.

•L'impiego di programmi, sistemi operativi e driver di cui non siano accessibili i sorgenti deve essere assolutamente evitato, in quanto non e' possibile garantire che il programma; in un modello di minaccia alto, il nemico ha a disposizione mezzi informatici illimitati.

•La creazione di un computer adeguato deve quindi prevedere la ricompilazione di tutto il software (device driver, sistema operativo ed applicazioni) a partire da sorgenti certificati e verificati (o comunque verificabili) od almeno acquisizione dei file eseguibili da sorgenti sicure.

Accenneremo infine, per completezza e senza la pretesa di fornire soluzioni, ad alcune linee guida da seguire per fronteggiare, almeno dal punto di vista informatico, un **modello di minaccia alto**.

Tutti gli accorgimenti del modello medio sono ovviamente un prerequisito.

L'impiego di programmi proprietari, o dei quali non siano accessibili i sorgenti deve essere evitato, in quanto non e' possibile garantire che il programma, od almeno il particolare file eseguibile che si carica sul proprio computer, sia esente da compromissioni o backdoor; si deve tenere sempre presente che in un modello di minaccia alto, il nemico ha a disposizione mezzi illimitati, anche dal punto di vista informatico.

La creazione di un computer destinato ad un tale impiego deve quindi prevedere la ricompilazione di tutto il software (device driver, sistema operativo ed applicazioni) a partire da sorgenti certificati e verificati (o comunque verificabili) od almeno acquisizione dei file eseguibili da sorgenti sicure (cosa molto difficile da realizzare in pratica).

Ricetta (parziale) : modello di minaccia alto

In un modello di minaccia alto si devono fronteggiare anche tipologie di attacco informatico particolari; ad esempio:

- il sistema Tempest che intercetta le emissioni radioelettriche del monitor
- la compromissione dell'hardware, come l'inserimento di device nella tastiera che memorizzano tutti i tasti premuti
- l'intercettazione delle emissioni delle periferiche wireless
- l'installazione da remoto di componenti "rogue" a livello di sistema operativo.

Questo spingerebbe quindi alla realizzazione di un computer dotato di software minimale, addirittura "spartano", al fine di minimizzare il lavoro necessario alla sua creazione.

Si tratta pero' di fronteggiare anche tipologie di attacco informatico particolari, come il metodo Tempest che intercetta le emissioni radioelettriche del monitor, la compromissione dell'hardware, come l'inserimento di device nella tastiera che memorizzano tutti i tasti premuti, o l'intercettazione delle emissioni delle periferiche wireless, od infine l'installazione da remoto di componenti "rogue" a livello di sistema operativo.

Grazie a tutti per l'attenzione.

per informazioni: **marcoc@dada.it - www.marcoc.it**

"Secure Deletion of Data ..." - Peter Gutmann, VI USENIX conference, 1996)
http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html
Jetico Inc. homepage (Bestcrypt)
http://www.jetico.com/
The International PGP Home Page
http://www.pgpi.org/
Pgp inc. homepage
http://www.pgp.com/
Sito del convegno "E-privacy 2003"
http://e-privacy.firenze.linux.it/
Il progetto Winston Smith
https://freenet.homelinux.net/SSK@Dgg5lJQu-WO905TrlZ0LjQHXDdIPAgM/pws/9//