Digital Forensics & Counter Forensics
Indagini di PG & Privacy

Il muro della crittografia tra diritti e doveri

Autore: Marco Mattiucci

www.marcomattiucci.it

(Ver. 1.0 – 20 Marzo 2015)

Piano della presentazione

1. Percorso di pensiero su informatica e crittazione
2. Digital forensics: studio, ricerca e pratica
3. Counter forensics: principi base
4. Privacy: l'importanza della crittazione
5. Indagini di PG: il problema della crittazione
6. I concetti di "traccia informatica" e di "profiling"
7. Un mondo senza cripto?

Informatica e Crittazione
Il mondo delle sequenze di 0 ed 1

…diverse migliaia di anni fa alcuni testi sacri orientali parlavano di 2 opposti (Yin/Yang in cinese) dalla cui interazione tutto l'universo era stato generato…

Mistico?! Religioso?! Surreale?!

Informatica e Crittazione
Il mondo delle sequenze di 0 ed 1

…nel 1850 circa il matematico G. Boole “sganciò” la logica dalla metafisica associandola proprio alla matematica. Nasceva l’algebra booleana, del vero/falso, dello 0/1…

Il lavoro fu ben accolto ma relegato a pura speculazione matematica fino al 1938…

Oggi l’argomento si studia alla scuola primaria…

Informatica e Crittazione
Il mondo delle sequenze di 0 ed 1

…nel 1900 circa il matematico D. Hilbert presentò in una famosa conferenza a Parigi la lista dei 23 problemi irrisolti della matematica tra cui:

#2 – Dimostrare che l'insieme degli assiomi dell'aritmetica è consistente ➔ *stabiliti simboli e regole tutti i teoremi si possono dimostrare con una procedura automatica*

#8 – Dimostrazione dell'ipotesi di Riemann ➔ *è possibile stabilire come si distribuiscono i numeri primi*

Informatica e Crittazione
Il mondo delle sequenze di 0 ed 1

…nel 1930 circa il matematico K. Gödel presentò i suoi famosi teoremi di incompletezza stabilendo che il "meccanismo", la "procedura", per la dimostrazione automatica di tutti i teoremi non può esistere…
BANALIZZANDO: *anche nella matematica ci sono affermazioni per le quali non è possibile dimostrare nulla!*

Informatica e Crittazione
Il mondo delle sequenze di 0 ed 1

…nel 1936 il matematico A. Turing dimostrò la stessa incompletezza introducendo la famosa Macchina di Turing, lo strumento concettuale fondamentale alla base della computazione, lo stesso strumento che gli permetterà di “affrontare” Enigma.

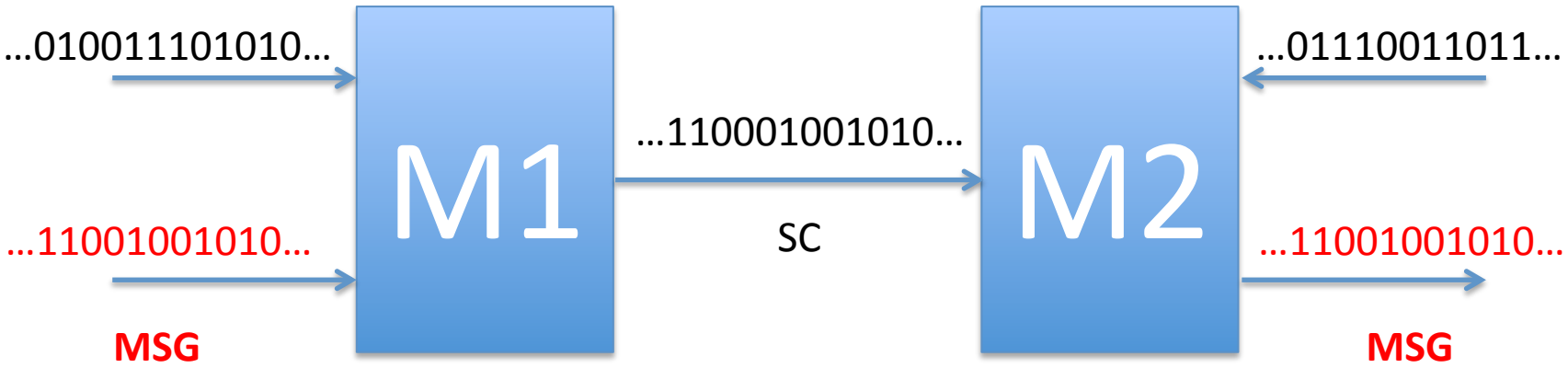
Informatica e Crittazione
Il mondo delle sequenze di 0 ed 1

Qualsiasi dato, segnale, informazione, valore è sequenza di 0 ed 1…

Qualsiasi ragionamento di calcolo umano può essere rappresentato da una Macchina di Turing…

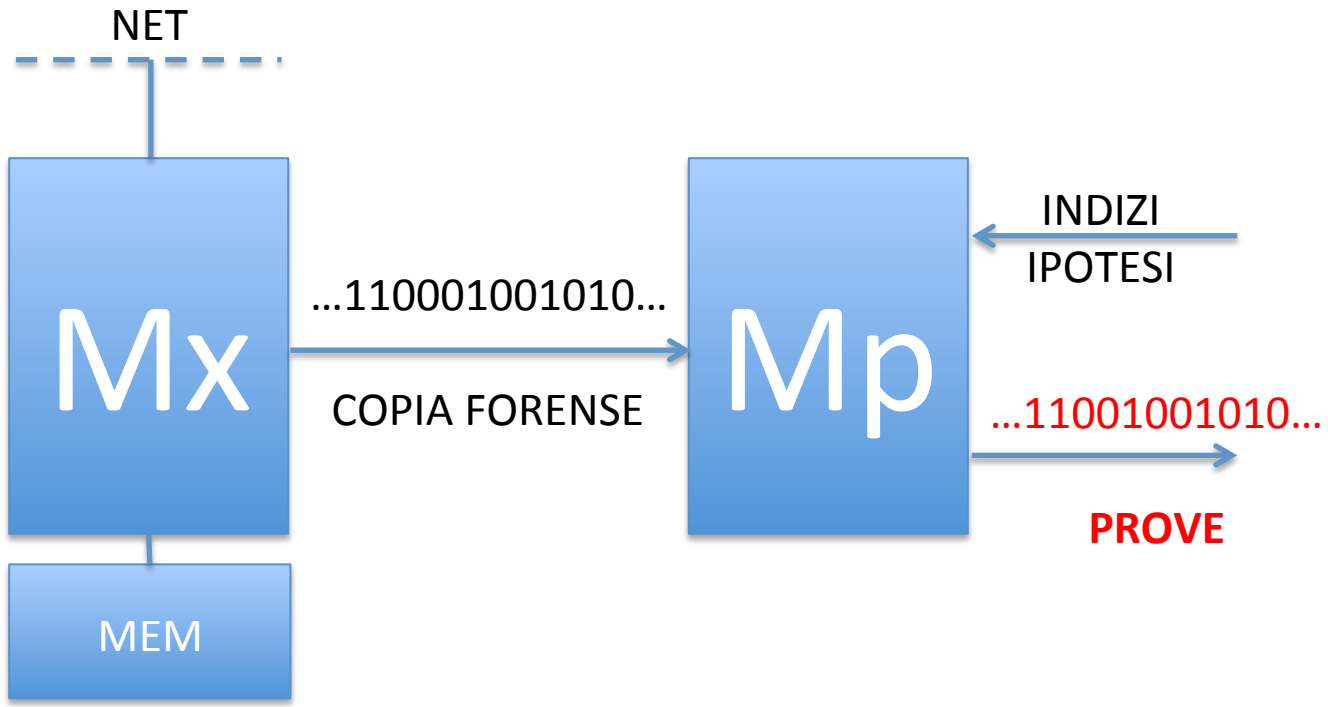
Qualsiasi macchina realizzata da essere umano può essere rappresentata da una Macchina di Turing…

CRIPTO & DECRIPTO



ASSUNZIONE #1: M1 ed M2 conosciuti da tutti
ASSUNZIONE #2: Sequenza comunicata (SC) visibile a tutti

DIGITAL FORENSICS



ASSUNZIONE #1: Mx, il reperto, è sotto controllo e non si modifica
ASSUNZIONE #2: Mp è uno strumento di indagine validato
ASSUNZIONE #3: tutto il processo è sottoposto a logging accurato

DATO, CALCOLO E SEQUENZA

DATO: …001001110101110…

MACCHINA DI CALCOLO (il tempo…):

t_1: …001001110101110…

t_2: …001001110101110…

…

t_n: …001001110101110…

…

DIGITAL FORENSICS

Le indagini di polizia giudiziaria, dal punto di vista tecnico, operano fondamentalmente su dati.

Esempi:

PC → HD →…00100101110… → Image file

CELL → FLASH →…0010001110… → Image file

WEB → DOWNLOAD →…0010110… → Image file

…

VIRTUAL DIGITAL FORENSICS

Le indagini di “frontiera” della ricerca iniziano ad operare sulle macchine…

Esempio elementare:

PC → HD →…001100101010… → Image file → **VM**

Proiezione futura… al tempo t stabilito:

PC(t) → HD(t)+RAM(t)+BIOS(t) →…0010111010… →

→ Evidence Container → **VM(t)**

Informatica: POTERI E PRIVACY (1)

“Potere” del calcolo

“Potere” della memorizzazione

“Potere” della comunicazione

Evoluzione temporale

Informatica: POTERI E PRIVACY (2)

“Potere” del calcolo

Posso impiegare o no la capacità di elaborazione di un sistema?

Es. un agente software **non distruttivo** che impiega parte della potenza di calcolo di un PC all’insaputa dell’utente…

Informatica: POTERI E PRIVACY (3)

“Potere” della memorizzazione

Posso impiegare o no la memoria di un sistema?

=

Posso “leggere dati da” o “scrivere dati in” tale memoria?

Es. cosa vuole dire possedere un dato informatico?

Il “dato informatico” è immateriale…

Cosa vuole dire “furto di dato”?

Informatica: POTERI E PRIVACY (4)

“Potere” della comunicazione

Posso comunicare tra due nodi di un sistema?

=

Posso “accedere” (leggere/modificare/cancellare) i dati da una rete?

Es. L’accesso ad un dato informatico presente su Internet deve essere soggetto a limitazioni legali o no?

Informatica:
IDENTITA', DOMICILIO E CRIPTO

Io sono X = sono l'UTENTE X

Ho un UID, PASS, BIOMETRICO, HARDWARE…

Io posso… ACCEDERE A…

X ha dei privilegi che gli consentono di accedere o meno a servizi informatici di vario genere

Il mio DOMICILIO INFORMATICO è…

Tutto ciò che X esplicitamente protegge ➔ CRIPTO

Informatica:
DATI PERSONALI E PRIVACY

Ad X possono essere associati dei dati personali

I dati personali di X possono essere usati, per scopi limitati, sia da X che altri;

Chiunque utilizzi i dati personali di X ne deve rendere avveduto X ed avere la sua autorizzazione;

Attenzione! Non esiste il furto di dati personali come potrebbe essere inteso fisicamente:

- La raccolta in archivi…
- L'uso…

Proteggere la propria privacy
Basi di Counter-Forensics

Se la Digital Forensics (DF) si occupa di recuperare e filtrare dati ad uso investigativo la Counter DF, talvolta chiamata Anti DF, studia come bloccare tale attività (proteggere la privacy??? ☺).

Tre fronti:

1) Calcolo / Elaborazione
2) Memoria / Installazione
3) Comunicazione / Accesso

Basi di Counter-Forensics: 1) Calcolo / Elaborazione

a) Conoscere i processi e servizi attivi sulla macchina che si protegge;
b) Supervisionare processi e servizi con cadenza almeno oraria;
c) Avere privilegi da Amministratore;
d) Impiegare la macchina solo quando necessario;
e) Disattivare fisicamente la macchina quando inutilizzata.

Basi di Counter-Forensics: 2) Memoria / Installazione

a) Avere un backup incrementale continuo di memoria centrale e memorie di massa con possibilità di rollback e destinazione esterna, meglio se remota e su disco cripto-nativi.
b) Installare sulla memoria di massa solo applicativi noti, sicuri ed in numero limitatissimo.
c) Installare un gestore di Macchine Virtuali (VM) e costruirne di prototipali da utilizzare alla bisogna.
d) Le VM vanno tenute in file cripto su dischi cripto-nativi o online e periodicamente cancellate.

Basi di Counter-Forensics: 3) Comunicazione / Accesso

a) Le numerose password vanno tenute in un file cripto su usbkey con partizione ombra.
b) Firewall ed IDS installati nelle VM e fuori da esse e comunque sempre attivi.
c) Comunicare in rete solo quando necessario.
d) Fare largo e continuo uso di proxy, anonimizzatori e canali cripto per comunicare.
e) Provvedere alla continua eliminazione di qualsiasi forma di log, cache o swap sulle memorie di massa

Basi di Counter-Forensics: 3) Comunicazione / Accesso

f) Avere una memoria centrale (RAM) molto ampia.
g) Operare il più possibile in RAM.
h) Eliminare l'impiego delle email.
i) No allo smartphone.
j) Creare ed impiegare, quando possibile, VM a tempo su Cloud extraterritoriali.
k) Nell'impiego di qualsiasi servizio Cloud (es. un remote drive come Dropbox / GDrive) mai installare il client e montare un proprio servizio cripto all'interno del cloud prima di usarlo.

Basi di Counter-Forensics: NOTE

Tutto ciò che è plausibile è inattaccabile perché l'essere umano si risveglia sul diverso e si addormenta sul consueto.

Una buona strategia applicata più di una volta porta sicuramente alla sconfitta, mai ripetersi!

Ricordare che la maggioranza delle persone (utenti) non fa ciò che sceglie di fare ma soddisfa necessità.

Indagini di PG e Crittazione (1)

La crittazione per le indagini di polizia giudiziaria è un doppio problema:

1) Tecnico: barriera da superare;
2) Legale: domicilio in cui entrare → autorizzazioni.

Indagini di PG e Crittazione (2)

Le indagini tecniche su sistemi telematici rimangono ancora possibili (nonostante l'esistenza del cripto-forte) a causa di:

1) Difficoltà di gestione delle numerose password;
2) Uso di password non randomizzate e corte;
3) Scarso uso di OTP;
4) Pigrizia dell'utente ed uso intensivo di usbkey e smartphone;

…in generale…

Le procedure di anti forensics sono preventive, pesanti, continue e richiedono una competenza tecnica notevole.

Indagini di PG e Crittazione (3)

Molti utenti scelgono di NON usare il cripto per i loro dati importanti da cui, ad esempio, crittano le aree di lavoro ma fanno dei backup in chiaro delle stesse.

Questa scelta apparentemente banale è dettata da un problema operativo molto serio delle memorie a contenuto criptato:

Qualora si presenti un errore o un guasto anche solo in pochi byte di un contenuto criptato è plausibile che non si recuperi più nulla!

Indagini di PG e Crittazione (4)

Le sequenze di bit che formano un contenuto cripto hanno normalmente alta entropia e forte intercorrelazione.

In altri termini non è così facile (talvolta è impossibile) individuare delle parti che abbiano un senso da sole e che quindi possano essere decrittate in autonomia da cui O TUTTO O NIENTE!

Indagini di PG e Crittazione (4)

Per tale motivo gli utenti hanno spesso copie multiple dei “file importanti” anche se li crittano…

Sempre per questo motivo molte usbkey che assicurano la “privacy”, in quanto dotate nativamente di password, in realtà crittano solo l’indice dei file e NON i file, per cui vengono vendute come “sicure” ma è tutto in chiaro, richiedono solo un po’ di impegno nel ricostruire l’indice…

CONCLUSIONI

La conservazione della privacy sui sistemi informatici e telematici è frutto di procedure e preparazione esattamente come il mantenimento della sicurezza informatica.

Nessun prodotto, da solo, può assicurarvi la privacy.

Nessuna traccia può essere eliminata se non quella che non esiste!

Bisogna ormai prendere atto che se si impiega un servizio gratis su Internet si è quasi con certezza oggetto di "profiling".

Le indagini tecniche informatiche di polizia giudiziaria sono ben poca cosa se si vanno a considerare le attività di "intelligence" e "profiling" portate avanti da motori di ricerca e social network…

Potrebbe esistere un mondo senza cripto?

Digital Forensics & Counter Forensics
Indagini di PG & Privacy

Il muro della crittografia tra diritti e doveri

FINE

Autore: Marco Mattiucci

www.marcomattiucci.it

(Ver. 1.0 – 20 Marzo 2015)