

Perché proteggere i dati

Alberto Ferrante

OSLab & ALaRI, Facoltà d'informatica, USI

ferrante@alari.ch

4 febbraio 2010

Sommario

Privacy

Privacy

Rischi

Rischi

Sicurezza

Sicurezza

Conclusioni

Conclusioni

Privacy

- > Privacy? Cos'è?
- > Perché?

Rischi

Sicurezza

Conclusioni

Privacy

Privacy? Cos'è?

Privacy

> Privacy? Cos'è?

> Perché?

Rischi

Sicurezza

Conclusioni

- I dati appartengono alle persone/aziende;
- ognuno ha una propria percezione della privacy:
 - ◆ ognuno dovrebbe essere in grado di rendere disponibile agli altri solo ciò che ritiene opportuno!!
 - ◆ un certo livello minimo (stabilito dalla legge) dev'essere sempre garantito!

Perché?

Privacy

> Privacy? Cos'è?

> Perché?

Rischi

Sicurezza

Conclusioni

- Su Internet è estremamente facile reperire informazioni sulle persone;
- con i calcolatori è molto facile correlare diverse informazioni;
- queste informazioni possono essere usate per molti scopi:
 - ◆ per offerte commerciali mirate;
 - ◆ per sapere qualcosa di più su di voi...
 - “come si comporta questa persona che vorrei assumere?”.

Privacy

Rischi

- I dati
- Rischi
- Le password
- Bug, Cattiva configurazione
- I dati che non vogliono morire...
- Non solo i dati sono importanti ...
- L'accesso remoto... Amplifica i problemi
- Virus, worm ...
- Intercettare le comunicazioni... Si può

Sicurezza

Conclusioni

Rischi

I dati (1/2)

Privacy

Rischi

➤ I dati

➤ Rischi

➤ Le password

➤ Bug, Cattiva configurazione

➤ I dati che non vogliono morire...

➤ Non solo i dati sono importanti ...

➤ L'accesso remoto... Amplifica i problemi

➤ Virus, worm ...

➤ Intercettare le comunicazioni... Si può

Sicurezza

Conclusioni

- I dati vengono salvati in molti dispositivi elettronici:
 - ◆ diverse azioni, nostre o di terzi, possono esporli a rischi;
 - ◆ indagini informatiche;
 - ◆ dispositivi persi;
 - ◆ dispositivi venduti;
 - ◆ dispositivi “rottamati”.

I dati (1/2)

Privacy

Rischi

➤ I dati

➤ Rischi

➤ Le password

➤ Bug, Cattiva configurazione

➤ I dati che non vogliono morire...

➤ Non solo i dati sono importanti ...

➤ L'accesso remoto... Amplifica i problemi

➤ Virus, worm ...

➤ Intercettare le comunicazioni... Si può

Sicurezza

Conclusioni

FBI loses laptops with classified information

POSTED: 5:19 p.m. EST, February 12, 2007



STORY HIGHLIGHTS

- Inspector general says at least 10 missing laptops had sensitive information
- 160 laptops lost or stolen during four-year period
- 51 missing laptops may also contain sensitive information
- Equal number of weapons also missing

Adjust font size:

WASHINGTON (CNN) -- The FBI lost at least 10 laptop computers containing classified information during a four-year period ending in 2005, the Justice Department's inspector general has found.

The 10 were among the 160 laptops lost or stolen during a 44-month period ending September 30, 2005, Inspector General Glenn Fine reported. An equal number of weapons also went missing.

The report said the number of missing items, while still a problem, represents a sharp improvement over a 2002 audit, which found more than 300 laptops and 300 weapons lost or stolen during the previous 28-month period.

<http://www.cnn.com/2007/US/02/12/fbi.laptops/index.html>

I dati (1/2)

Privacy

Rischi

➤ I dati

➤ Rischi

➤ Le password

➤ Bug, Cattiva configurazione

➤ I dati che non vogliono morire...

➤ Non solo i dati sono importanti ...

➤ L'accesso remoto... Amplifica i problemi

➤ Virus, worm ...

➤ Intercettare le comunicazioni... Si può

Sicurezza

Conclusioni

- I dati vengono salvati in molti dispositivi elettronici:
 - ◆ diverse azioni, nostre o di terzi, possono esporli a rischi;
 - ◆ indagini informatiche;
 - ◆ dispositivi persi;
 - ◆ dispositivi venduti;
 - ◆ dispositivi “rottamati”.

I dati (2/2)

Privacy

Rischi

➤ I dati

➤ Rischi

➤ Le password

➤ Bug, Cattiva configurazione

➤ I dati che non vogliono morire...

➤ Non solo i dati sono importanti ...

➤ L'accesso remoto... Amplifica i problemi

➤ Virus, worm ...

➤ Intercettare le comunicazioni... Si può

Sicurezza

Conclusioni

- I dati vengono trasmessi:
 - ◆ diverse azioni, nostre o di terzi, li espongono a rischi;
 - ◆ indagini informatiche.

Privacy

Rischi

➤ I dati

➤ Rischi

➤ Le password

➤ Bug, Cattiva configurazione

➤ I dati che non vogliono morire...

➤ Non solo i dati sono importanti ...

➤ L'accesso remoto... Amplifica i problemi

➤ Virus, worm ...

➤ Intercettare le comunicazioni... Si può

Sicurezza

Conclusioni

- Lettura dei dati:
 - ◆ danni derivanti dall'acquisizione di informazioni riservate da parte di terzi.
- Modifica dei dati:
 - ◆ danni derivanti dall'incapacità di capire:
 - che ci sono state delle modifiche;
 - che modifiche sono state fatte.

Le password

Privacy

Rischi

➤ I dati

➤ Rischi

➤ **Le password**

➤ Bug, Cattiva configurazione

➤ I dati che non vogliono morire...

➤ Non solo i dati sono importanti ...

➤ L'accesso remoto... Amplifica i problemi

➤ Virus, worm ...

➤ Intercettare le comunicazioni... Si può

Sicurezza

Conclusioni

- Spesso sono... L'inizio del problema:
 - ◆ deboli;
 - ◆ riutilizzate;
 - ◆ condivise (consciamente o meno) con altre persone;
 - ◆ appiccicate sul dispositivo stesso.
- debolezze sfruttate per accedere al sistema:
 - ◆ conosco la password, accedo;
 - ◆ attacchi brute force.

Le password

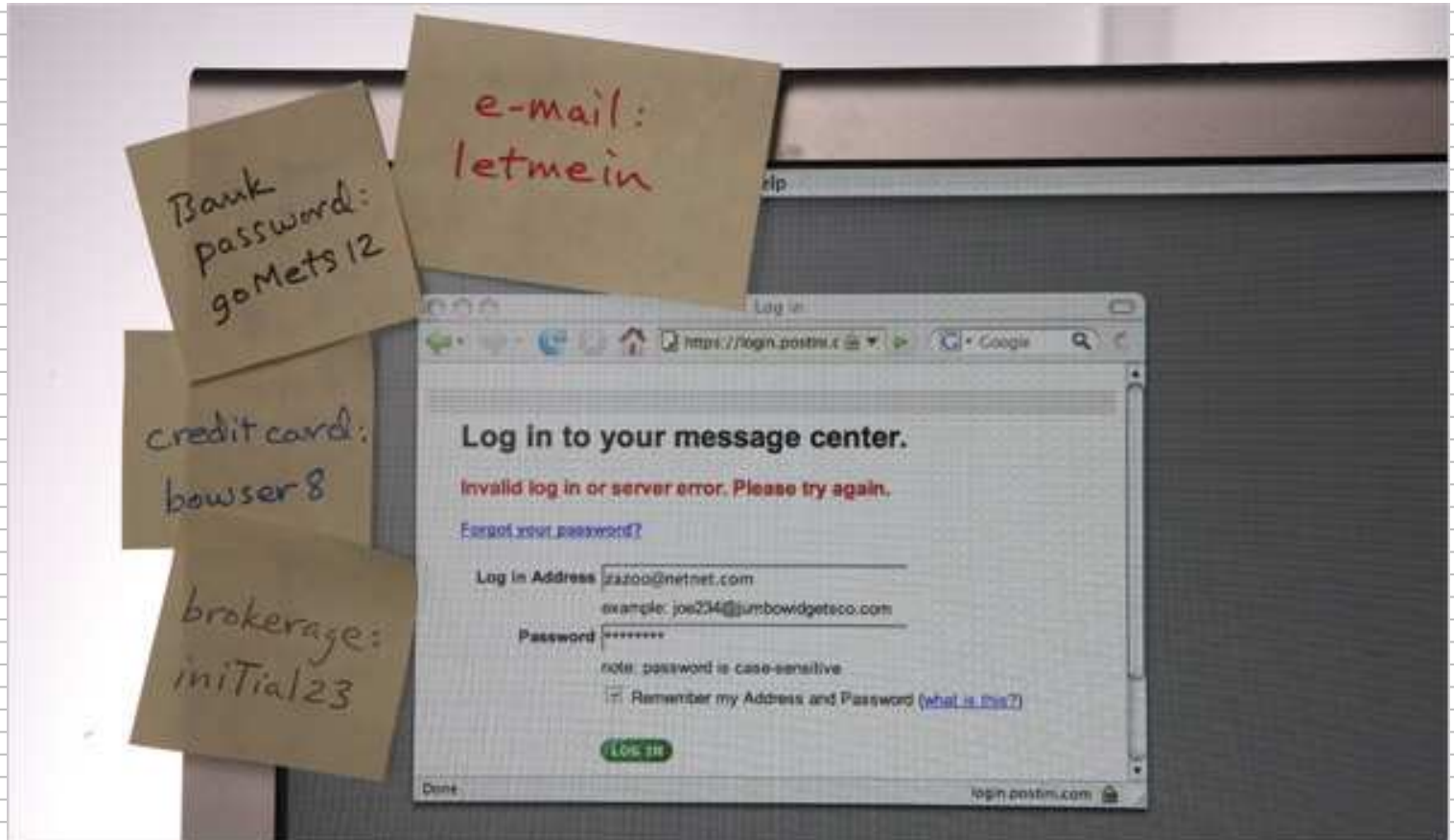
Privacy

Rischi

- I dati
- Rischi
- **Le password**
- Bug, Cattiva configurazione
- I dati che non vogliono morire...
- Non solo i dati sono importanti ...
- L'accesso remoto... Amplifica i problemi
- Virus, worm ...
- Intercettare le comunicazioni... Si può

Sicurezza

Conclusioni



<http://stanbiron.com/content/binary/passwordPostIt.jpg>

Le password

Privacy

Rischi

➤ I dati

➤ Rischi

➤ **Le password**

➤ Bug, Cattiva configurazione

➤ I dati che non vogliono morire...

➤ Non solo i dati sono importanti ...

➤ L'accesso remoto... Amplifica i problemi

➤ Virus, worm ...

➤ Intercettare le comunicazioni... Si può

Sicurezza

Conclusioni

- Spesso sono... L'inizio del problema:
 - ◆ deboli;
 - ◆ riutilizzate;
 - ◆ condivise (consciamente o meno) con altre persone;
 - ◆ appiccicate sul dispositivo stesso.
- debolezze sfruttate per accedere al sistema:
 - ◆ conosco la password, accedo;
 - ◆ attacchi brute force.

Bug, Cattiva configurazione

Privacy

Rischi

➤ I dati

➤ Rischi

➤ Le password

➤ Bug, Cattiva configurazione

➤ I dati che non vogliono morire...

➤ Non solo i dati sono importanti ...

➤ L'accesso remoto... Amplifica i problemi

➤ Virus, worm ...

➤ Intercettare le comunicazioni... Si può

Sicurezza

Conclusioni

Per accedere ai dati si possono sfruttare:

- bug di sistema;
- una cattiva/errata configurazione del sistema:
 - ◆ politiche di accesso;
 - ◆ protezione di BIOS e boot.

I dati che non vogliono morire...

Privacy

Rischi

➤ I dati

➤ Rischi

➤ Le password

➤ Bug, Cattiva configurazione

➤ I dati che non vogliono morire...

➤ Non solo i dati sono importanti ...

➤ L'accesso remoto... Amplifica i problemi

➤ Virus, worm ...

➤ Intercettare le comunicazioni... Si può

Sicurezza

Conclusioni

- La cancellazione dei dati è critica:
 - ◆ quello che pensiamo di aver distrutto in realtà rimane nel dispositivo per molto tempo.
- attenzione soprattutto quando regaliamo/vendiamo/gettiamo qualcosa!
- tool per recovery (forensics):
 - ◆ fatback (recovery file su FAT);
 - ◆ foremost (recovery file per tipo);
 - ◆ galleta (recovery cookies IE);
 - ◆ testdisk (recovery partizioni).

Non solo i dati sono importanti . . .

Privacy

Rischi

- I dati
- Rischi
- Le password
- Bug, Cattiva configurazione
- I dati che non vogliono morire...
- **Non solo i dati sono importanti . . .**
- L'accesso remoto... Amplifica i problemi
- Virus, worm . . .
- Intercettare le comunicazioni... Si può

Sicurezza

Conclusioni

- Attenzione a diversi dettagli:
 - ◆ le azioni compiute sui dati vengono spesso registrate (history, . . .);
 - ◆ nomi dei file;
 - ◆ . . .

L'accesso remoto... Amplifica i problemi

Privacy

Rischi

- I dati
- Rischi
- Le password
- Bug, Cattiva configurazione
- I dati che non vogliono morire...
- Non solo i dati sono importanti ...
- **L'accesso remoto... Amplifica i problemi**
- Virus, worm ...
- Intercettare le comunicazioni... Si può

Sicurezza

Conclusioni

I problemi di sicurezza locale vengono amplificati:

- una gestione corretta delle password diventa ancora più importante;
- più facile sfruttare eventuali buchi nel sistema.

Virus, worm . . .

Privacy

Rischi

- I dati
- Rischi
- Le password
- Bug, Cattiva configurazione
- I dati che non vogliono morire...
- Non solo i dati sono importanti . . .
- L'accesso remoto... Amplifica i problemi
- **Virus, worm . . .**
- Intercettare le comunicazioni... Si può

Sicurezza

Conclusioni

- Virus, worm e altre forme di software malevoli sono spesso usati per carpire dati oltre che per danneggiare il sistema:
 - ◆ per es, usano la rete per inviare dati dell'utente ad un server apposito.

Intercettare le comunicazioni... Si può

Privacy

Rischi

- I dati
- Rischi
- Le password
- Bug, Cattiva configurazione
- I dati che non vogliono morire...
- Non solo i dati sono importanti ...
- L'accesso remoto... Amplifica i problemi
- Virus, worm ...
- Intercettare le comunicazioni... Si può

Sicurezza

Conclusioni

- Reti wireless aperte o con poche protezioni;
- intercettazione dei pacchetti sulla rete wired;
- uso della rete internet.

Intercettare le comunicazioni... Si può

Privacy

Rischi

- I dati
- Rischi
- Le password
- Bug, Cattiva configurazione
- I dati che non vogliono morire...
- Non solo i dati sono importanti ...
- L'accesso remoto... Amplifica i problemi
- Virus, worm ...
- Intercettare le comunicazioni... Si può

Sicurezza

Conclusioni

Irnsync.cap - Ethereal

No.	Time	Source	Destination	Protocol	Info
5	0.609753	66.70.73.150	192.168.0.216	TCP	rsync > 33005 [PSH, ACK] Seq=2303827507 Ack=176875483
6	0.609766	192.168.0.216	66.70.73.150	TCP	33005 > rsync [ACK] Seq=176875483 Ack=2303827519
7	0.614751	66.70.73.150	192.168.0.216	TCP	rsync > 33005 [ACK] Seq=2303827519 Ack=176875483
8	0.614761	192.168.0.216	66.70.73.150	TCP	33005 > rsync [PSH, ACK] Seq=176875483 Ack=2303827519
9	0.914711	66.70.73.150	192.168.0.216	TCP	rsync > 33005 [PSH, ACK] Seq=2303827519 Ack=176875483
10	0.916692	66.70.73.150	192.168.0.216	TCP	rsync > 33005 [ACK] Seq=2303827779 Ack=176875484

Frame 9 (326 bytes on wire, 326 bytes captured)

- Ethernet II, Src: 00:20:18:a2:1b:b2, Dst: 08:00:46:6a:d5:1e
- Internet Protocol, Src Addr: 66.70.73.150 (66.70.73.150), Dst Addr: 192.168.0.216 (192.168.0.216)
- Transmission Control Protocol, Src Port: rsync (873), Dst Port: 33005 (33005), Seq: 2303827519, Ack: 176875483, Len: 260

Data (260 bytes)

```
0040  71 9a 57 65 6c 63 6f 6d 65 20 74 6f 20 74 68 65  q.Welcome to the
0050  20 73 61 6d 62 61 2e 6f 72 67 20 61 6e 6f 6e 79  samba.org anony
0060  6d 6f 75 73 20 72 73 79 6e 63 20 61 72 63 68 69  mous rsync archi
0070  76 65 73 2e 0a 0a 43 6f 6e 74 61 63 74 20 74 70  ves...Contact tp
0080  6f 74 40 73 61 6d 62 61 2e 6f 72 67 20 69 66 20  ot@samba.org if
```

Filter: / Reset Apply Data (data), 260 bytes

<http://www.linuxjournal.com/article/6842>

Intercettare le comunicazioni... Si può

Privacy

Rischi

- I dati
- Rischi
- Le password
- Bug, Cattiva configurazione
- I dati che non vogliono morire...
- Non solo i dati sono importanti ...
- L'accesso remoto... Amplifica i problemi
- Virus, worm ...
- Intercettare le comunicazioni... Si può

Sicurezza

Conclusioni

- Reti wireless aperte o con poche protezioni;
- intercettazione dei pacchetti sulla rete wired;
- uso della rete internet.

Privacy

Rischi

Sicurezza

> Security

> Il fattore umano

Conclusioni

Sicurezza

Sicurezza (1/2)

Privacy

Rischi

Sicurezza

> Security

> Il fattore umano

Conclusioni

- La sicurezza è un processo:
 - ◆ policy;
 - ◆ personale addestrato;
 - ◆ tecniche e prodotti.

La sicurezza di un sistema è data dalla sicurezza dell'elemento più debole.

Sicurezza (2/2)

Privacy

Rischi

Sicurezza

> Security

> Il fattore umano

Conclusioni

- Non esiste la **sicurezza assoluta**:
 - ◆ relativa e commisurata a quello che vogliamo proteggere;
 - ◆ relativa ad attacchi conosciuti/previsti;
 - ◆ è un compromesso.

Il fattore umano (1/2)

Privacy

Rischi

Sicurezza

> Security

> Il fattore umano

Conclusioni

Le persone sono spesso l'anello debole della security chain:

- i dati sono spesso condivisi con altre persone senza alcun bisogno di accedere al sistema informatico;
- password deboli;
- password condivise;
- ...

Il fattore umano (2/2)

Privacy

Rischi

Sicurezza

> Security

> Il fattore umano

Conclusioni

- Cattiva configurazione del sistema:
 - ◆ errori umani;
 - ◆ per evitare lavoro addizionale.
- “Ma perché mai dovrebbe capitare a noi?” :
 - ◆ nessuna o limitata protezione del sistema;
 - ◆ meccanismi per la sicurezza installati ma disabilitati.

Privacy

Rischi

Sicurezza

Conclusioni

➤ Conclusioni

➤ End

Conclusioni

Conclusioni

Privacy

Rischi

Sicurezza

Conclusioni

> Conclusioni

> End

- La protezione dei dati è essenziale;
- esistono numerosissimi problemi tecnici legati alla sicurezza;
- proteggere i dati non è solo una questione tecnologica!

End

Ringrazio per l'attenzione...

Alcuni diritti riservati:



<http://creativecommons.org/licenses/by-nc-sa/3.0>