Corso di Formazione

Incaricati di trattamento dati personali

Autenticazione & Autorizzazione

- Sistemi di Autenticazione
- Identificazione tramite password
- Altri meccanismi di identificazione
- Le password negli applicativi
- Scelta delle password
- Sistemi di autorizzazione
- Domande & Risposte

Autenticazione

- Meccanismo con cui il sistema identifica l'utente
  - Chi è l'utente
  - L'utente è veramente quello che dice di essere?

Tipi di autenticazione

- Una cosa l'utente conosce
- Una cosa l'utente ha
- Come l'utente è
- Per maggior sicurezza una combinazione di queste

Conoscenza

- Cosa l'utente conosce
  - Un codice tipo PIN o password
  - Una frase: passphrase
  - La risposta ad una domanda personale
    - Dove sei nato, in quale scuola ti sei diplomata, il nome da ragazza di tua madre, il tuo colore preferito, sequenze di domande risposte concordate

Cosa possiede

- Una smartcard
- Una chiave (usb, seriale)
- Un certificato digitale (un file)
- Una lista di codici

Come l’utente è

- Confronto tra aspetto fisico dell’utente e dati registrati
  - Impronta digitale
  - Scan della retina
  - Timbro della voce

Autorizzazione

- A quali risorse deve poter accedere l'utente dopo l'autenticazione?
- Esempio. Database Management:
  - Alcuni utenti possono cambiare i dati immagazzinati
  - Altri utenti possono solo leggere le informazioni del database

Autorizzazione

- Risponde a queste domande:
  - L’utente X può accedere alla risorsa R?
  - L’utente X può eseguire l’operazione P?
  - L’utente X può eseguire l’operazione P sulla risorsa R?

Relazione tra A e A

- Autenticazione e Autorizzazione sono meccanismi strettamente connessi
- I sistemi di autorizzazione dipendono dai sistemi di autenticazione per prevenire che utenti non autorizzati accedano a risorse protette.

Username e Password

- Ad ogni utente viene assegnato un nome (di fantasia o derivato dal nome proprio) e una parola segreta
  - Sistema molto comune a cui tutti sono abituati
  - Non serve portarsi dietro una card o una chiave
  - Utenti mobili (funziona da qualsiasi posto)
  - Password usabile su diversi computer

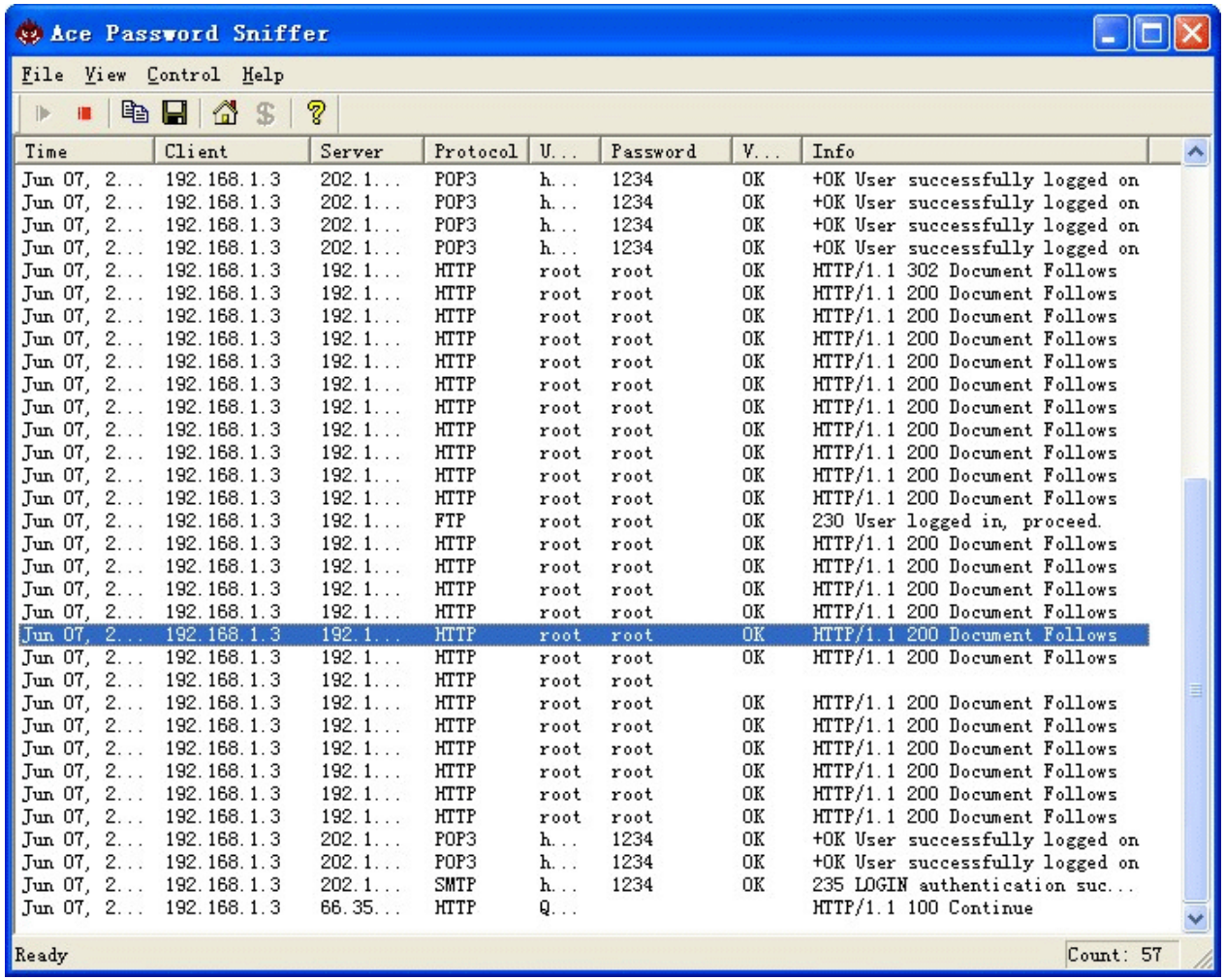
Problemi della password

- Password troppo facili si possono indovinare facilmente
  - uguale alla username, al numero di telefono, data di nascita, nome della moglie/marito, del figlio, targa della macchina, altri nomi comuni
- Password troppo difficili
  - L'utente le dimentica e quindi le richiede spesso
  - L'utente se le scrive su un bigliettino o post-it che attacca sotto la tastiera, sul monitor, lavagna di fronte, nel cassetto.

Password spiate

- Mentre vengono digitate da qualcuno che vi sta passando dietro alla schiena
- Vengono intercettate da programmi spia che leggono la tastiera o la rete (keyboard logger, network sniffer)

Password Sniffer



Password disperse

- Password condivise da due o più persone
  - Un segreto non è più un segreto se lo sanno più di due persone (o una?)

Tante password o poche password?

- Tante password, una per ogni sistema:
  - Se una viene scoperta non si compromette la sicurezza di altri sistemi
  - Difficili da ricordare tutte le password, soprattutto se scadono in tempi diversi e sono create con criteri diversi
- Poche password – Single Sign-On
  - Una sola password ma scelta con cura, usata spesso e quindi mai dimenticata
  - La perdita di questa password compromette tutti i sistemi

Come scelgo la password

- Lunga almeno otto caratteri
  - Per evitare attacchi “brute force” in cui vengono provate tutte le possibili combinazioni
- Non presente in un dizionario
  - I programmi di “Crack” provano per prime le parole presenti nei dizionari delle lingue più usate

Come scelgo la password

- Senza riferimenti personali
  - Per evitare che qualcuno la possa indovinare dalla conoscenza di questi dati personali
  - Per esempio dal nome-cognome → CAP, numero di telefono di casa
  - Targa della macchina
  - Nome del cane, dei figli, marito etc…

Come scelgo la password

- Con misto di caratteri e numeri
  - I numeri possono essere usati al posto di alcune lettere
  - Esempio 3 → E ; 0 → O ; 1 → I ; 4 → A
  - Esempio 2 → to, 4 → for
- Parole in dialetto
- Iniziali di frasi

Esempi di password

- Frase, proverbi, pezzi di canzoni
  - **A C**avallo **D**onato **N**on **S**i **G**uarda **I**n **B**occa → **ACDNSGIB**
  - **T**ra **I**l **D**ire **E** **I**l **F**are **C**‘**E**’ **D**i **M**ezzo **I**l **M**are → **TIDEIFCEDMIM**
  - **S**punta **L**a **Lu**na **Da**l **Mo**nte → SLLuDaMo

Esempi di password

- Trasformazioni:
  - BARONEROSSO → B**4**R**0**N**3**R**0**SS**0**
  - SEE YOU LATER → CUL8R
  - Esempio di testo oscurato → **3**s**3**mp**10** d**1** t**3**st**0** **0**scur**4**t**0** → **3$3**mp**10** **P1** t**3$**t**0** **0$(5**r**4t0**

Esempi di password

- Password “pronunciabili” generate dal computer
  - es. **expinter, sticiall, trendain, sandylam, sidamins, mentaint**
- http://www.winguides.com/security/password.php
  - Esempio con lettere:
  - **triacrla trIAmoed poUXiusW**
  - E anche numeri
  - **ko7Triu8 , 2Len4uSi , pRo7CoEp**

Cura della password

- Distinguere la password personale dalla password del ruolo
  - Es. Password personale per il proprio account di posta; Password dell'account del gestore di un servizio (protocollo, modifica di una pagina web) o dei settaggi di una macchina
  - La seconda password può essere condivisa tra tutte le persone che devono accedere al servizio, o modificare la pagina o settare la macchina
  - Quando uno è assente, l'altro o gli altri colleghi hanno ancora accesso al servizio, alla risorsa

Password di amministratore

- Spesso esiste un utente speciale con tutti i poteri
  - Si chiama ***root*** (unix), administrator (windows), ***QSECOFR*** (AS/400), ***SYSTEM*** (VAX/VMS)
  - Anche questo è un ruolo. Quindi non bisogna usare questo account che ha “superpoteri” nelle operazioni normali perchè ci sono protezioni ridotte contro gli errori

SuperPoteri

- Creare account, distruggere account
- Modificare il sistema operativo
- Cambiare la protezione ai files protetti
- Creare una nuova password

SuperPoteri e password

- ATTENZIONE: Di solito non riesce a conoscere la vostra password
- ATTENZIONE: Può fare “tutto” SENZA la vostra password, non ha bisogno di chiedervela
- DIFFIDATE da chi vi chiede la vostra password fingendo di essere l’amministratore

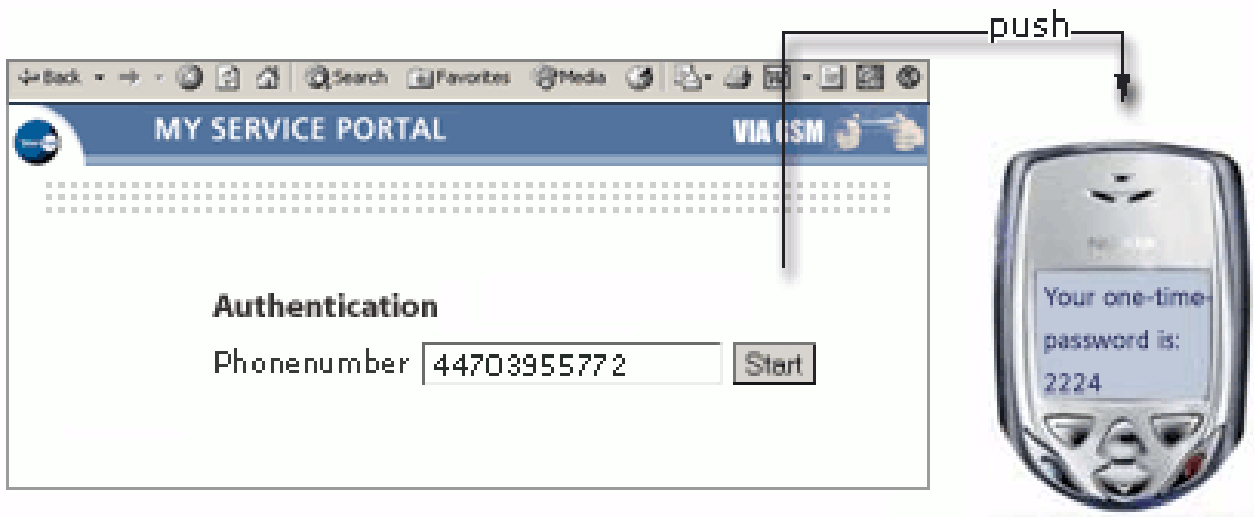
La protezione delle password

- La vostra password personale protegge i vostri files, i vostri mail
- La password dell'amministratore protegge tutta la macchina, il sistema operativo, i files di tutti
- Per forzare l'accesso e il controllo di una macchina non conoscendo la password di amministratore ci sono due metodi:
  - Una falla nel sistema operativo
  - Accesso fisico alla macchina

Perdita della password

- Se pensate che qualcuno conosca la vostra password
  - Cambiatela
  - Avvertite gli amministratori
- Se pensate che qualcuno abbia la password di amministratore
  - Chiedete che venga reinstallata la macchina: ci possono essere programmi spia nascosti

One Time Password

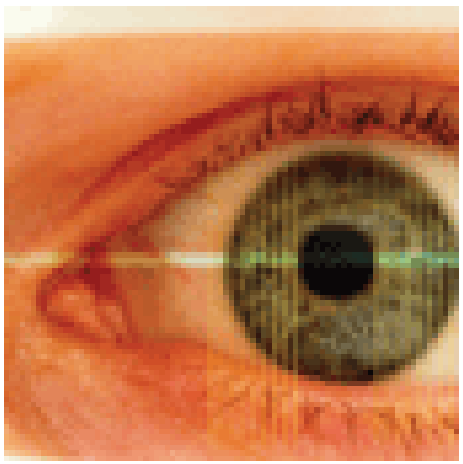


USB Keys

Magnetic Card - Smart Card

Fingerprint – Impronta Digitale

Retinal Scan



Autorizzazioni

- Il problema dell'autenticazione è soprattutto tecnico
- Il problema dell'autorizzazione è di decidere una politica sensata di protezione

Autorizzazione a files

- I files sono protetti dal sistema operativo
  - In relazione altri utenti
  - In relazione alle operazioni che si possono fare sui files

Protezione dagli utenti

- Il proprietario del file (owner)
- Utenti appartenenti a certi gruppi (group)
- Tutti gli altri utenti (world)

Esempio Unix/Linux

- Tre tipi di protezione
  - Lettura
  - Scrittura/Cancellazione/Modifica
  - Esecuzione

Esempi di protezione

- La mia mailbox
  - Io sono l'owner e posso fare tutto
  - Quelli nel mio gruppo e il resto del mondo non deve poter fare nulla
- Un altro mio documento
  - Io posso fare tutto
  - Tutti gli possono solo leggerlo

Esempi di protezione

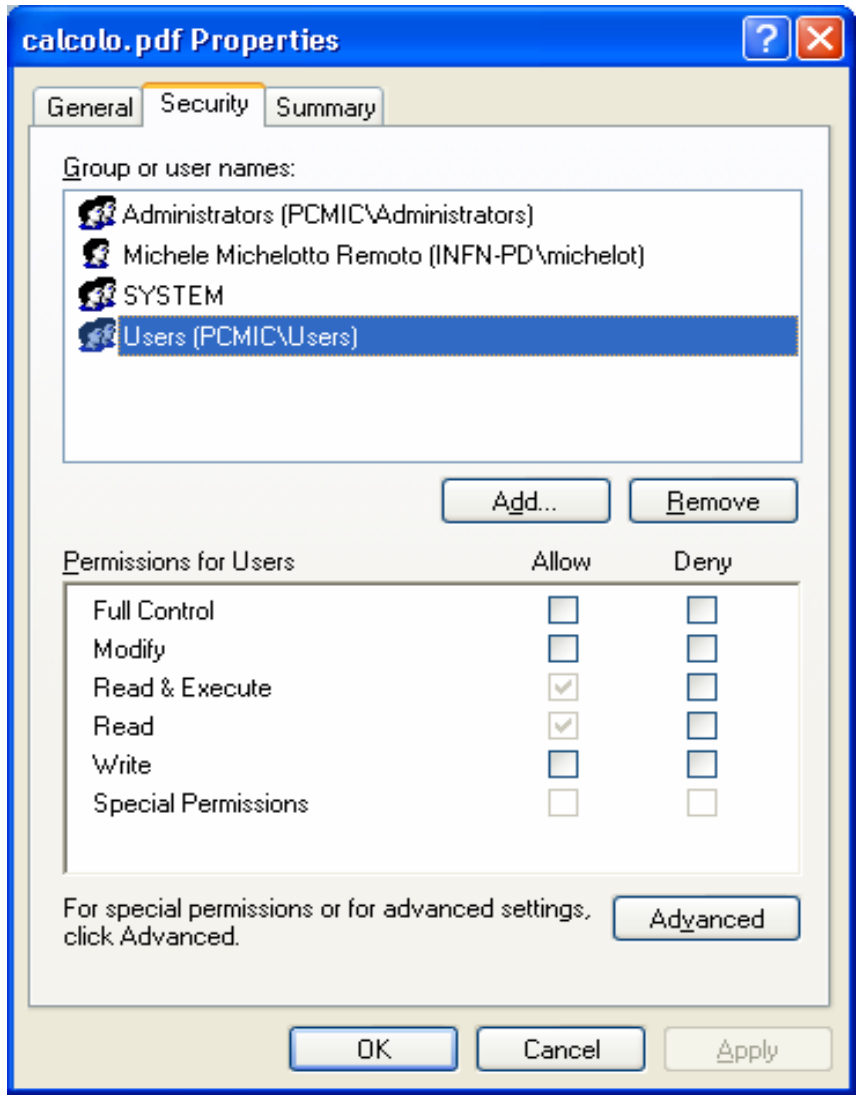
- Un documento del mio ufficio
  - Io posso fare tutto
  - Quelli del mio ufficio possono cambiarlo
  - Tutti gli altri possono leggerlo
- Altro documento
  - Io posso fare tutto
  - Quelli del mio ufficio possono solo leggerlo
  - Tutti gli altri non lo possono leggere

Access Contro List

- Le protezioni di Unix sono relativamente semplici ma in alcuni casi limitate
- Le ACL (Access Control List sono uno strumento più potente anche se spesso più complesso

Es Windows

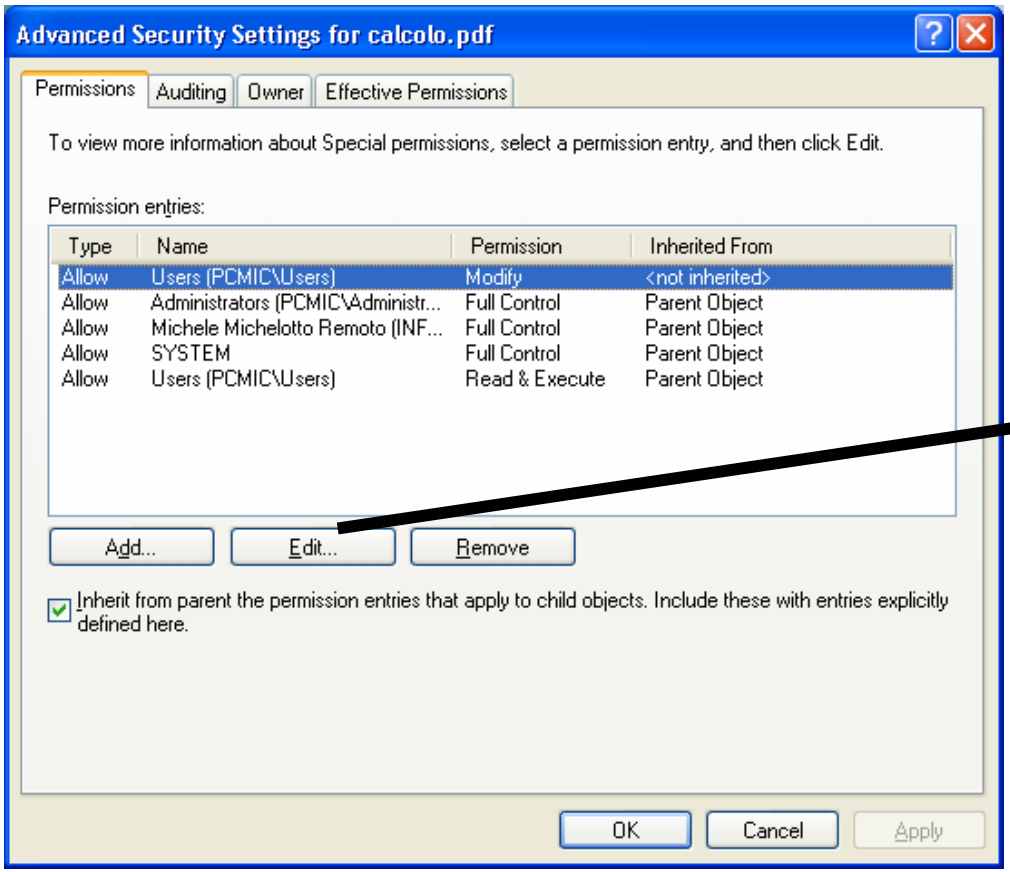
- Chi (dopo essere stato autenticato) può fare qualcosa
- Cosa può fare

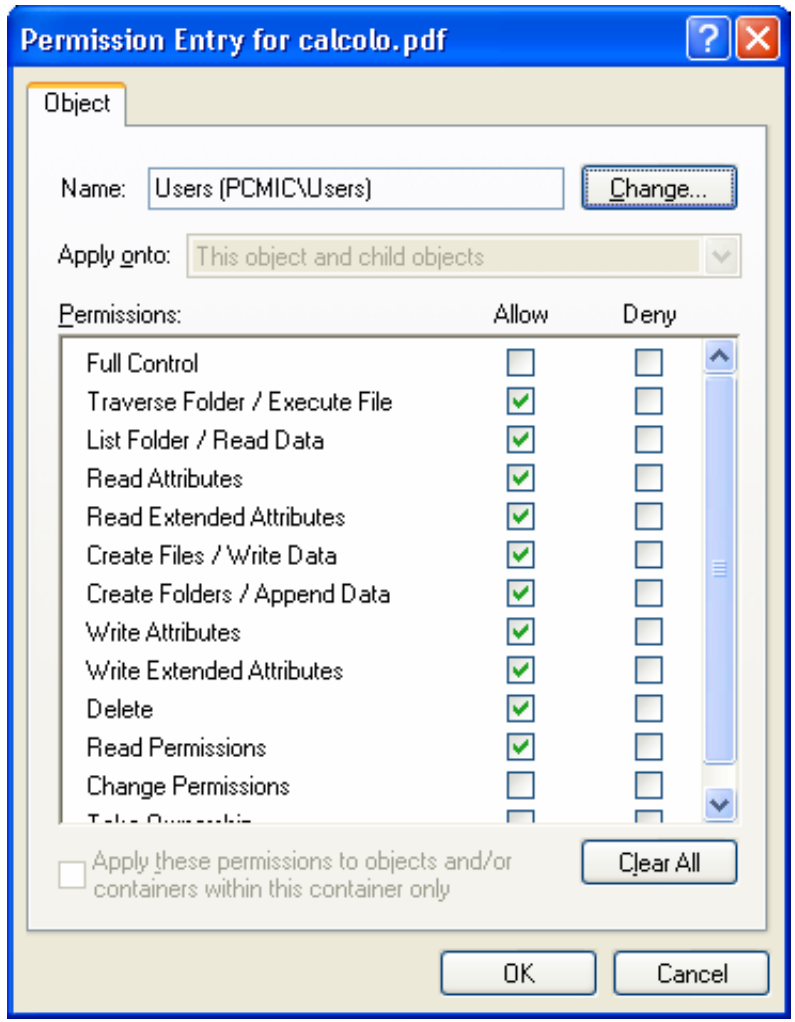


Permessi degli utenti

- Full Control: Qualsiasi cosa, compreso la modifica dei permessi stessi e cambiare l'owner
- Modify: Modificare il file ma non lo cancella
- Write: Qualsiasi modifica
- Read: Leggere il file senza modificarlo
- Read&Execute: Legge il file e lo esegue

Dettagli possibili





Utenti autorizzabili

- Amministratore Locale
- Gli amministratori del dominio
- Gli utenti locali
- Gli utenti del dominio
- Gli utenti del dominio di un certo gruppo
- Un ben definito utente locale
- Un ben definito utente del dominio
- Il mio account quando accedo remotamente
- Un utente qualsiasi via rete, anche anonimo

Troppo controllo?

- Troppe Combinazioni?
  - Abbiamo visto che si possono autorizzare diversi tipi di utenti
  - e che per ognuno di questi utenti possiamo dare una grande varietà di azioni
- Attenzione.
  - Si rischia di tagliarsi fuori dall'accesso dei propri stessi files.
  - Fate delle prove
  - Fatevi consigliare dagli amministratori locali

Protezione di pagine web

- Es: Stiamo pubblicando diverse pagine web, con diversi livelli di riservatezza
  - Pagine che vorremmo che tutti vedessero
  - Pagine che non ci interessa se tutti le vedono, basta che le vedano gli interessati
  - Pagine che solo i dipendenti INFN o solo i dipendenti della mia struttura possono vedere
  - Pagine che solo alcune persone possono vedere
  - Pagine che devono essere viste solo dal proprietario

Come proteggere?

- Non divulgando la pagina
  - Troppo debole
- Si possono impedire gli accessi da tutti i nodi che non siano *.infn.it oppure *.*struttura*.infn.it
  - Se un nostro utente vuole accedere da casa o da un altro laboratorio?

Come proteggere?

- Con elenchi di username/password
  - Una password da distribuire a tutti gli interessati?
  - Una password diversa per ogni interessato?

Password del server

- Dove accedo
- Username:
- Password oscurata dai puntini
- Ricordati la password la prossima volta che cerco di accedere a questa pagina

Pagine attive

- Un programma perl gestisce questa form
- Il programma accede ad un file o database con gli account
- Complicato, richiede programmazione, ma posso personalizzare il risultato

Protezione web

- Abbiamo visto come proteggere pagine web
- Autenticazione con username/password o tramite l'indirizzo IP del richiedente
- Autorizzazioni Accedi/Non Accedi o Autorizzazioni Complesse/Personalizzate

Protezioni di Applicativi

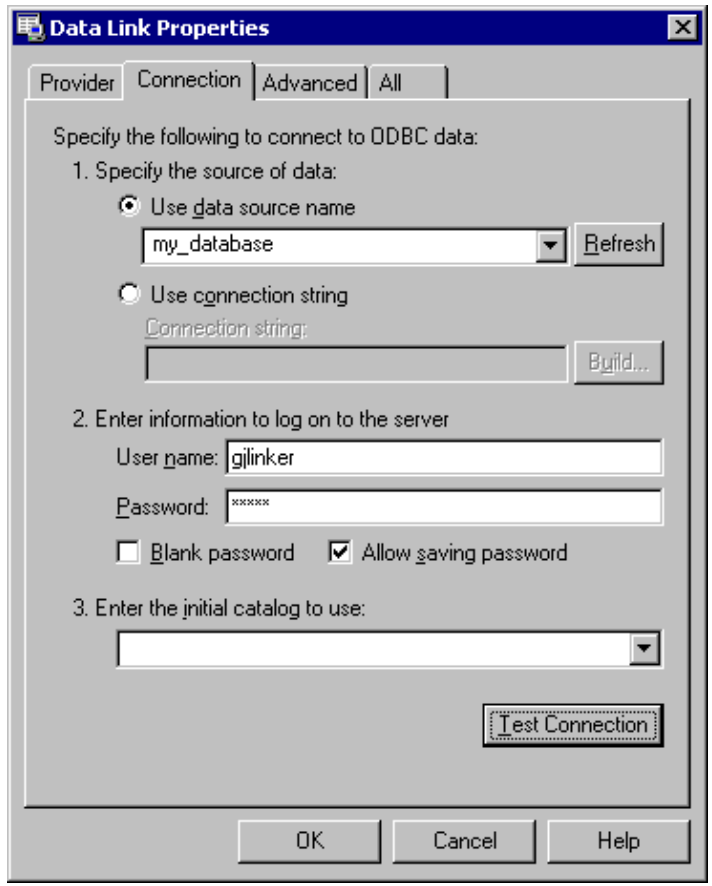
- Anche programmi applicativi possono aver bisogno di livelli di protezione differenziati
- I Database
  - Sono files particolari, o insiemi di files, con una struttura interna, a cui si accede con programmi appositi
  - Nei casi semplici (tipo MS Access, Claris FileMaker Pro) sono single-user quindi si proteggono come i files semplici o i documenti Excel
  - A volte ai databases devono accedere diverse persone con diversi ruoli

Esempio: Preventivi

- Utente non INFN: **nessun accesso**
- Utente normale INFN: **sola consultazione via web**
- Coordinatore di un gruppo X: **Accesso in modifica di alcuni campi relativi al gruppo X**
- Direttore (o suo delegato) di una sezione: **modifica di tutti (quasi) i campi relativi alla sezione ma non al formato dei campi**
- Responsabile del progetto: **Accesso a tutti i campi**

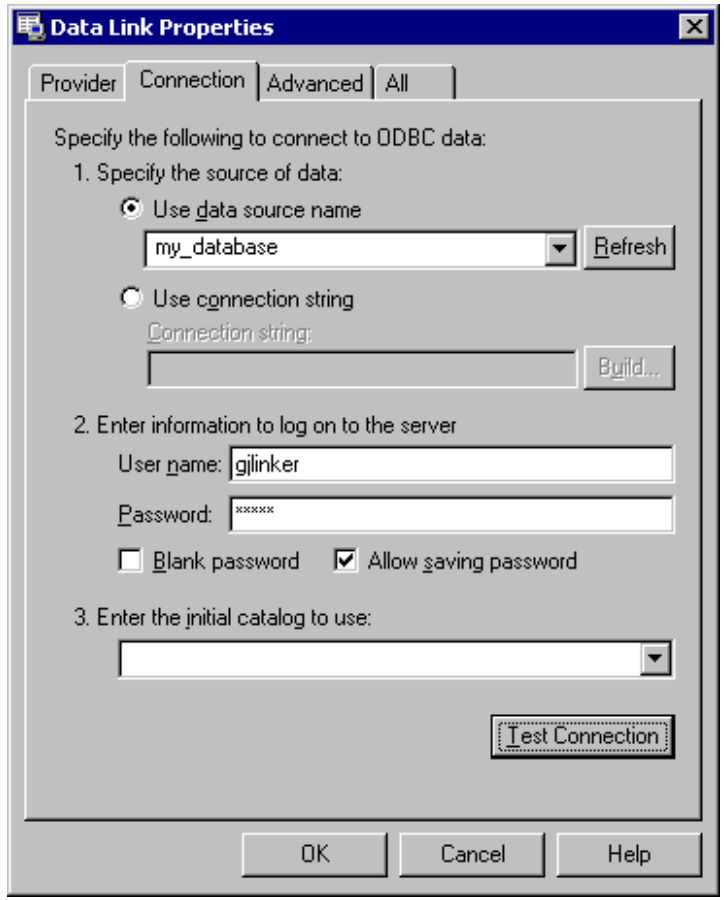
Password del database

- Il database contiene diverse tabelle
- Autenticazione:
  - Diversi utenti possono accedere contemporaneamente
- Autorizzazioni diverse
  - Leggere una tabella
  - Modificare un campo di un record in una tabella
  - Modificare la struttura della tabella aggiungendo campi o relazione



Amministratore del DB

- Aggiungere nuovi utenti, o toglierli
- Cambiare la loro password
- Aggiungere o togliere tabelle



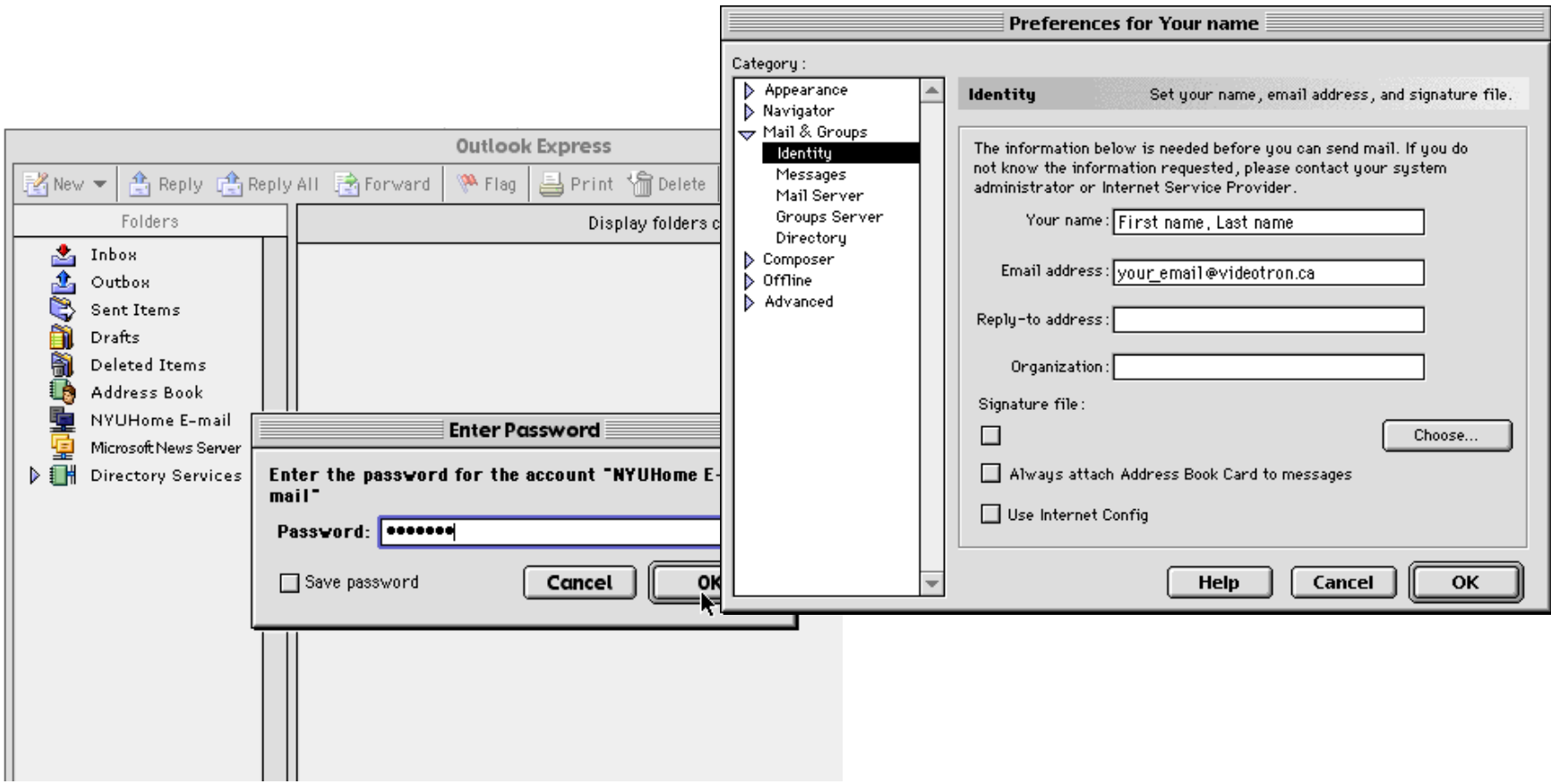
Password relative all'accesso web

- Accanto all'accesso diretto al database usando i protocolli specifici (ODBC) viene spesso dato un accesso via web
- In questo caso il database viene acceduto da un utente "web server" che poi gestisce all'interno del "frontend" web i diversi ruoli

Password del mail

- I mail stanno in files accessibili solo dal proprietario e dall'amministratore
- Quando i mail vengono scaricati su di un PC locale, devono finire in files/folder protetti da occhi indiscreti
- Attenzione. Non è, di solito, la stessa password che si usa per accedere al computer.

Password mail



Riservatezza dei mail

- I mail vengono gestiti in modo automatico dalla ricezione, alla ricerca di SPAM e virus, alla consegna all'utente finale
- Le persone che amministrano la macchina non devono leggere i mail per consegnarli (ma tecnicamente lo possono fare)
- Solo raramente alcuni mail si incastrano per cui gli amministratori devono "accendere" i loro superpoteri per leggere il mail e consegnarlo "a mano".

Autenticazione del mittente

- Il mittente può, senza grossi sforzi, cambiare il campo “From”
- Quindi non c’è modo di capire se chi la manda è veramente quello che afferma di essere
- Insomma il mittente (sia come utente che come computer) non è autenticato

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

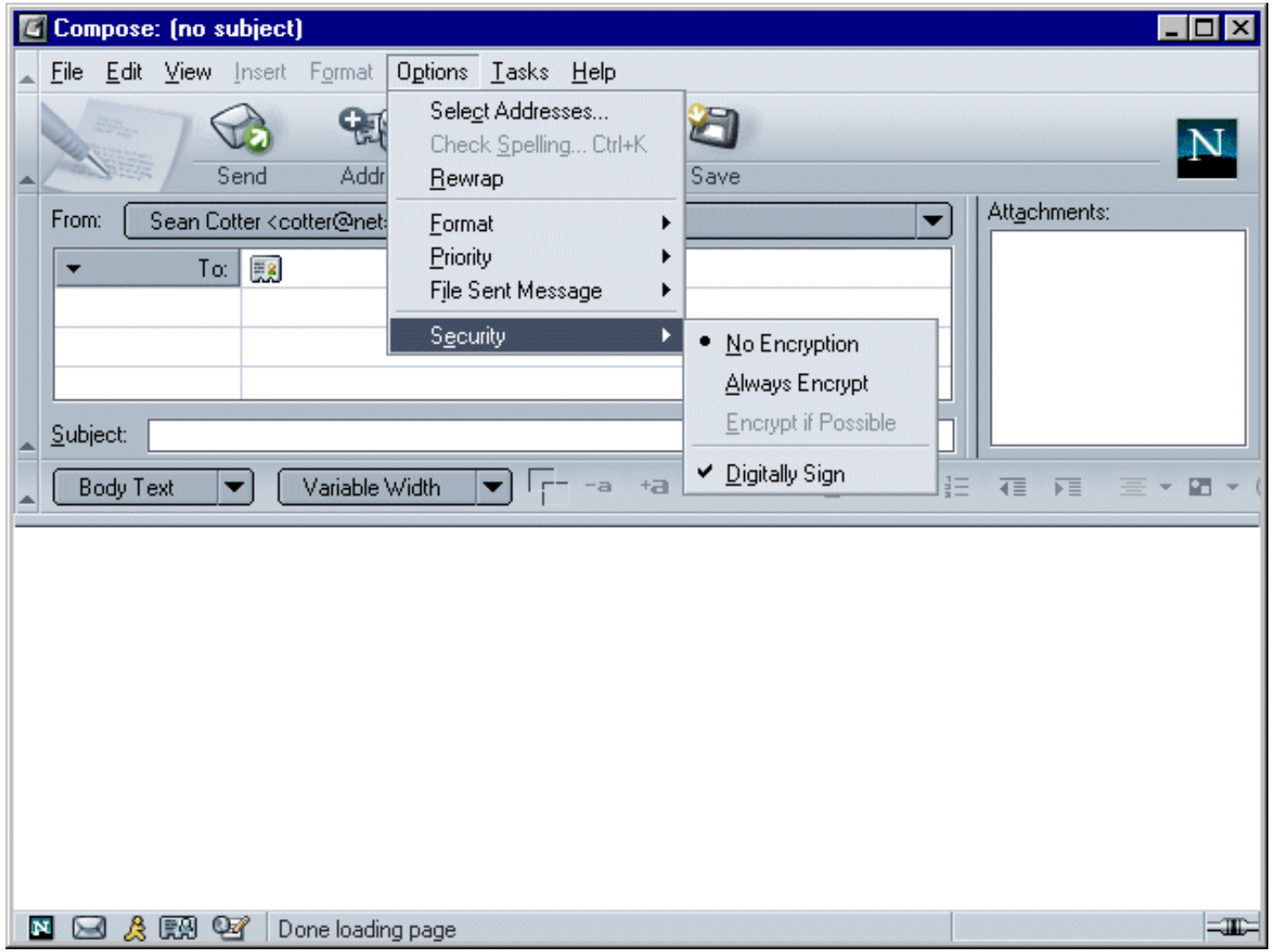
Mail firmate

- Anche nella posta cartacea il mittente è non autenticato
- Ci fidiamo dal contesto, presenza di un marchio o un logo, o riconoscendo una firma
- Anche per la posta elettronica c'è la firma di tipo digitale

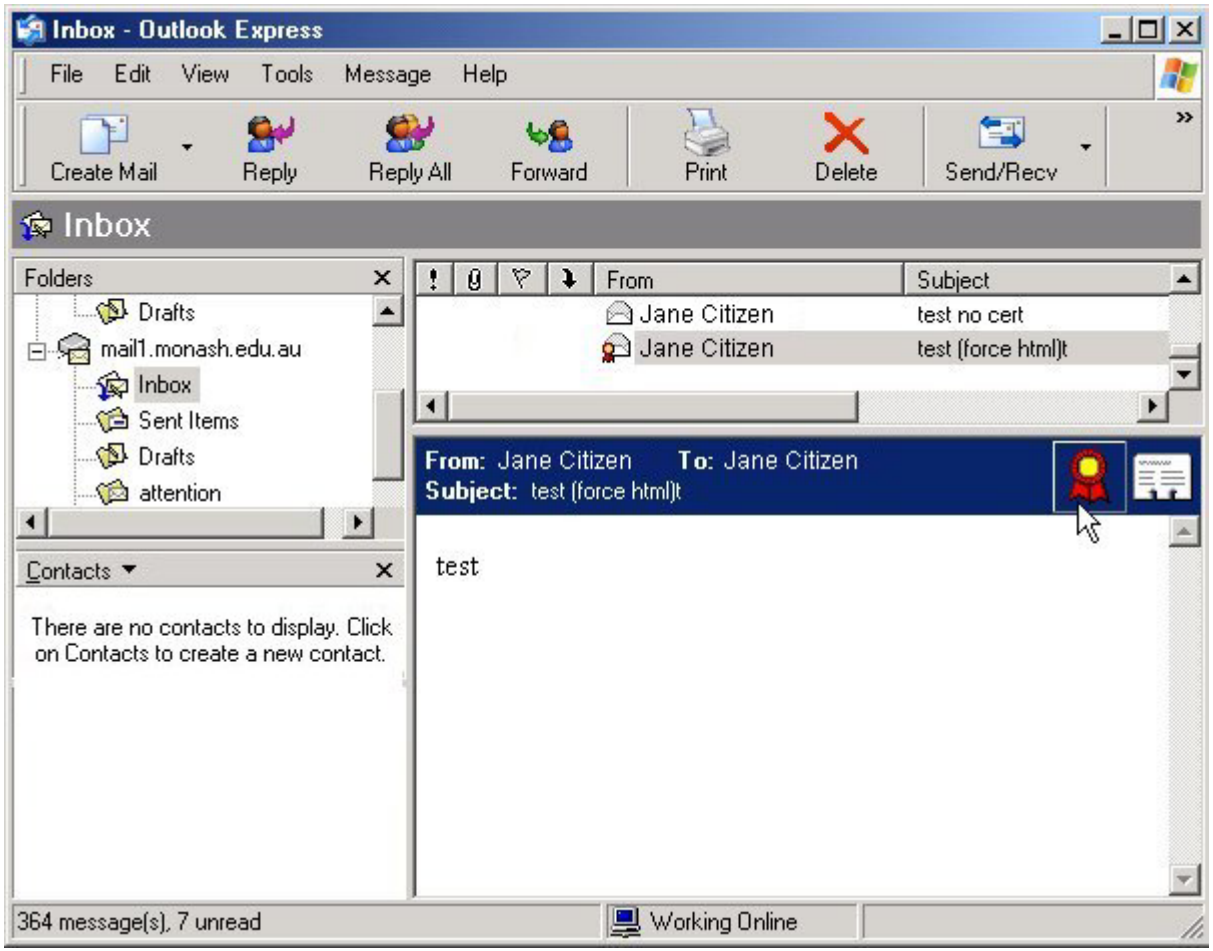
Cosa garantisce?

- Se il mio programma di posta verifica che la firma digitale è corretta
  - So che il mittente apparente è veramente quello che mi ha mandato il mail
  - So che il mail non è stato modificato nel percorso tra mittente e destinatario

Come si firma



Mail Firmato (Outlook)



Mail Firmato (Mozilla)

[tb-grid] Problemi con VOMS e MyProxy - 0--TECBRD-grid for michele.michelotto@pd.infn.it - Mozilla

File Edit View Go Message Tools Window Help

Get Msgs | Compose | Reply | Reply All | Forward | Next | Junk | Delete

Subject: [tb-grid] Problemi con VOMS e MyProxy
From: Roberto Barbera <roberto.barbera@ct.infn.it>
Date: 21/9/2004 11:43
To: tb-grid@infn.it
Cc: 'Vincenzo Ciaschini' <Vincenzo.Ciaschini@cnaf.infn.it>, grid-prod@ct.infn.it

Ciao a tutti,

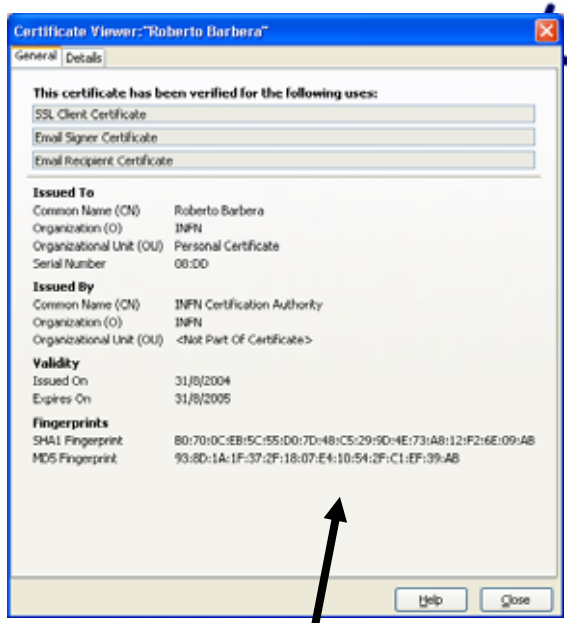
con la creazione dei primi VOMS abbiamo iniziato a rendere GENIUS compatibile ma ci stiamo scontrando con i primi (grossi) problemi. Da una analisi pare che il comando myproxy-init eseguito dopo un voms-proxy-init crei un delegatore sul MyProxy server che rilascia ***comunque*** (con il comando myproxy-get-delegation) proxy di tipo VO e ***NON*** di tipo VOMS.
Per risolvere il problema ci occorrerebbero i comandi:

voms-myproxy-init
voms-myproxy-info
voms-myproxy-get-delegation
voms-myproxt-destroy

che permettano il management di myproxy creati a partire da un VOMS proxy. Esistono ? Qualcuno ci sta lavorando su ? Come e' gestita l'interazione tra VOMS e MyProxy attualmente ?
Una risposta rapida sarebbe estremamente gradita dato che il problema si porra' immediatamente con il VOMS compchem dei chimici.
Grazie 1000 in anticipo.

Roberto

--
Roberto Barbera (mailto:roberto.barbera@ct.infn.it)
Phone Catania: ++.39.095.378.5313 | Phone CERN: ++.41.22.76.79739
Fax Catania: ++.39.095.378.5231 | Fax CERN: ++.41.22.76.79480
WWW: http://alipc1.ct.infn.it | Office CERN: 23-1-016



Quanto sono sicuri i miei dati?

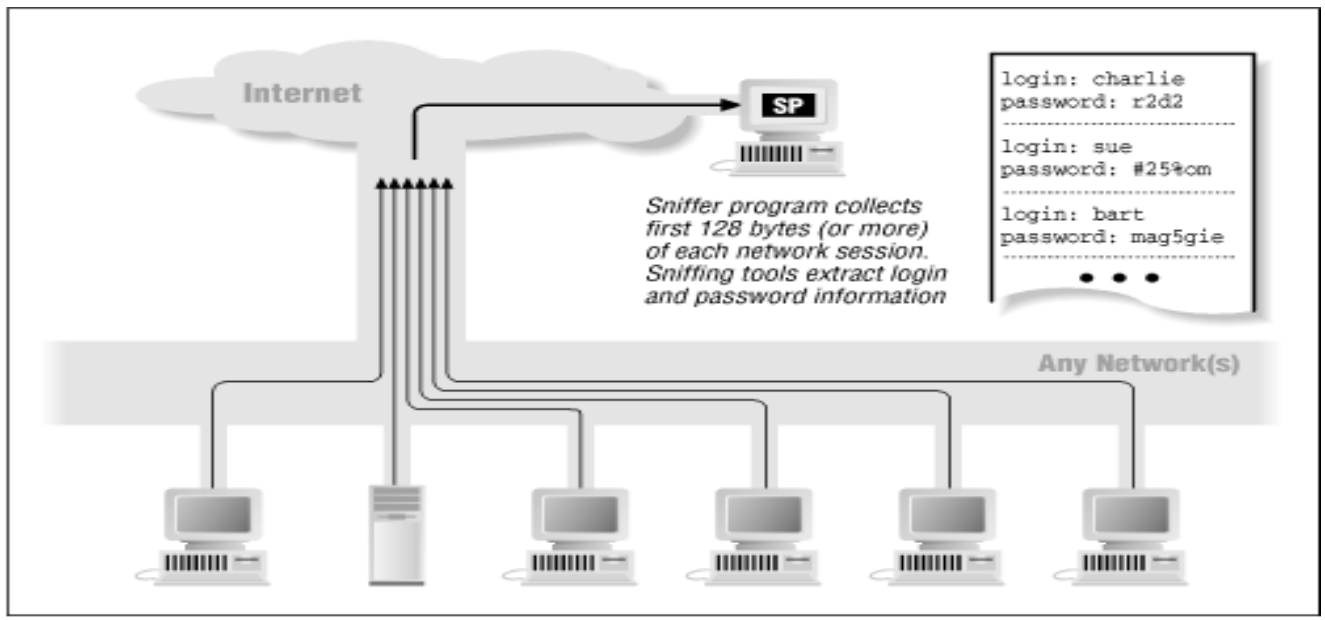
- Abbiamo deciso una policy di authorization
- Abbiamo un valido strumento di authentication
- Quindi solo chi è autorizzato può accedere ai miei dati?
- In teoria SI

In pratica

- Nella pratica i miei dati possono essere trafugati e/o modificati
  - Da uno che mi indovina la password
  - Da un amministratore curioso
  - Da uno che intercetta il traffico di rete (sniffer)
  - Da qualcuno che mi ruba il computer o il disco del computer o una cassetta di backup

Sniffer

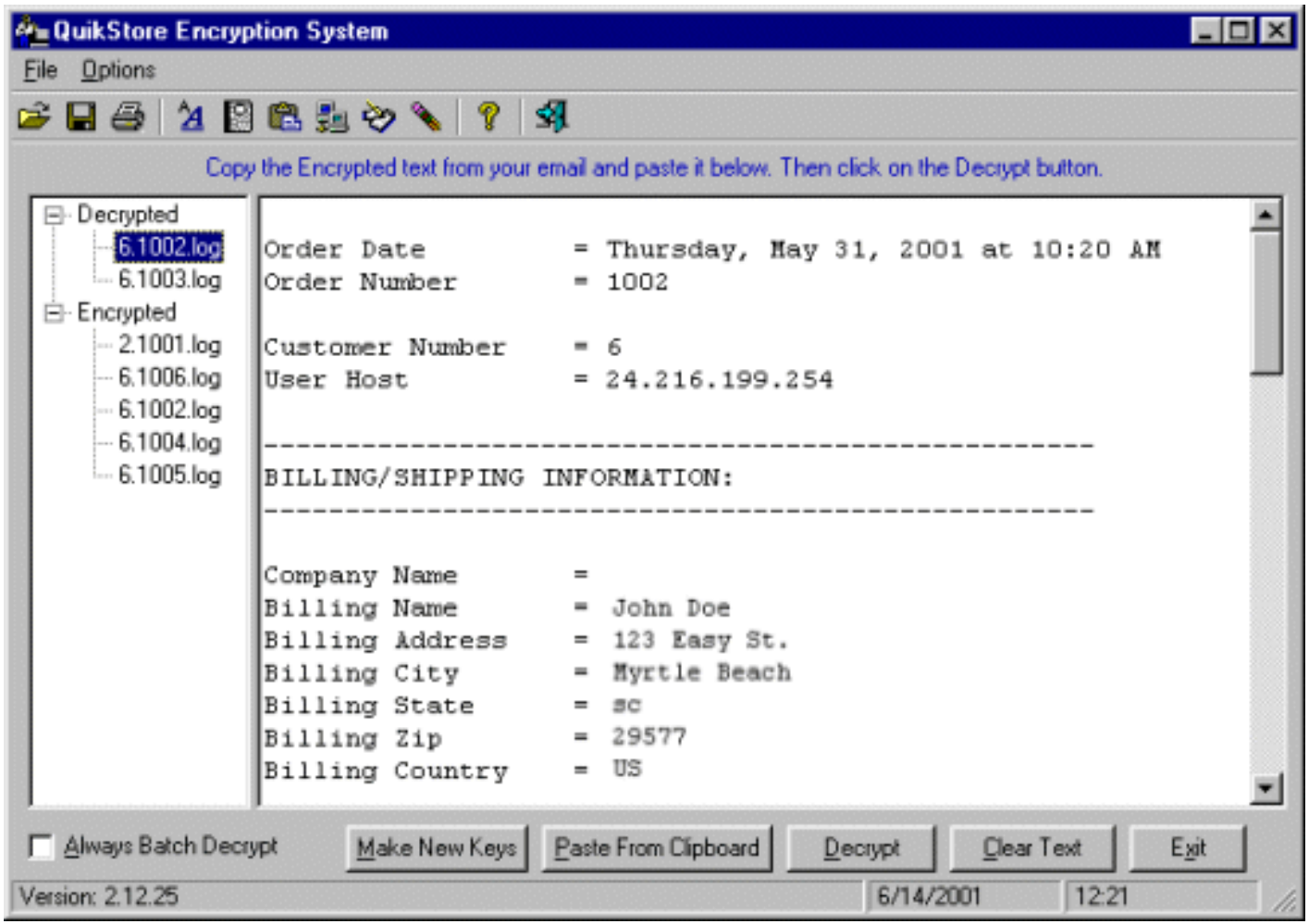
- Chi controlla la rete localmente o nei punti intermedi riesce a leggere i dati o le password che passano non criptate



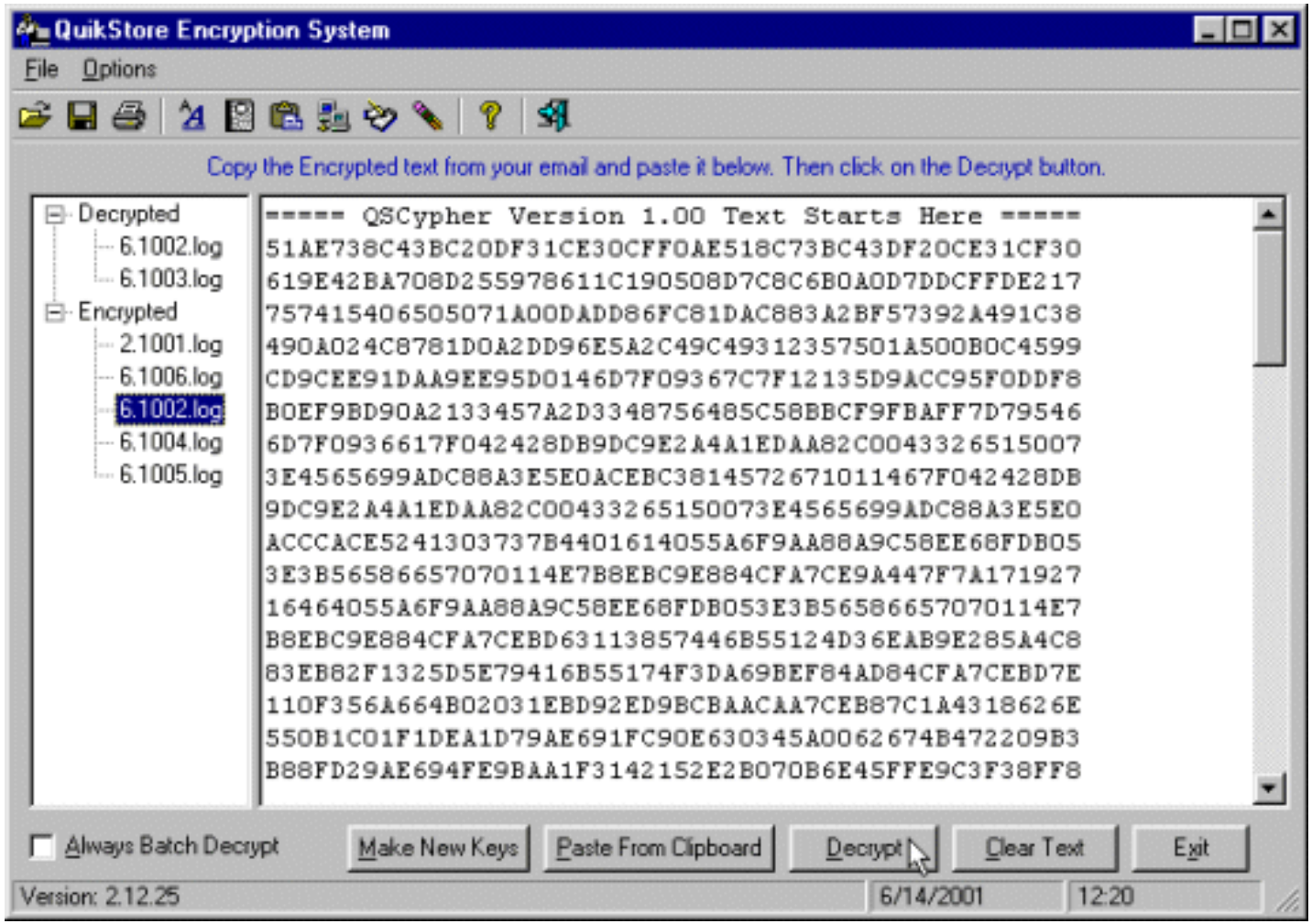
Encryption

- Si possono criptare (**to encrypt**) i dati in modo da renderli leggibili ma non intelleggibili
  - Le password sono quasi sempre immagazzinate in forma criptata.
  - Si possono criptare anche i campi in un database
  - Si possono criptare singoli files
  - Si possono inviare mail criptate
  - Esistono anche file system criptati

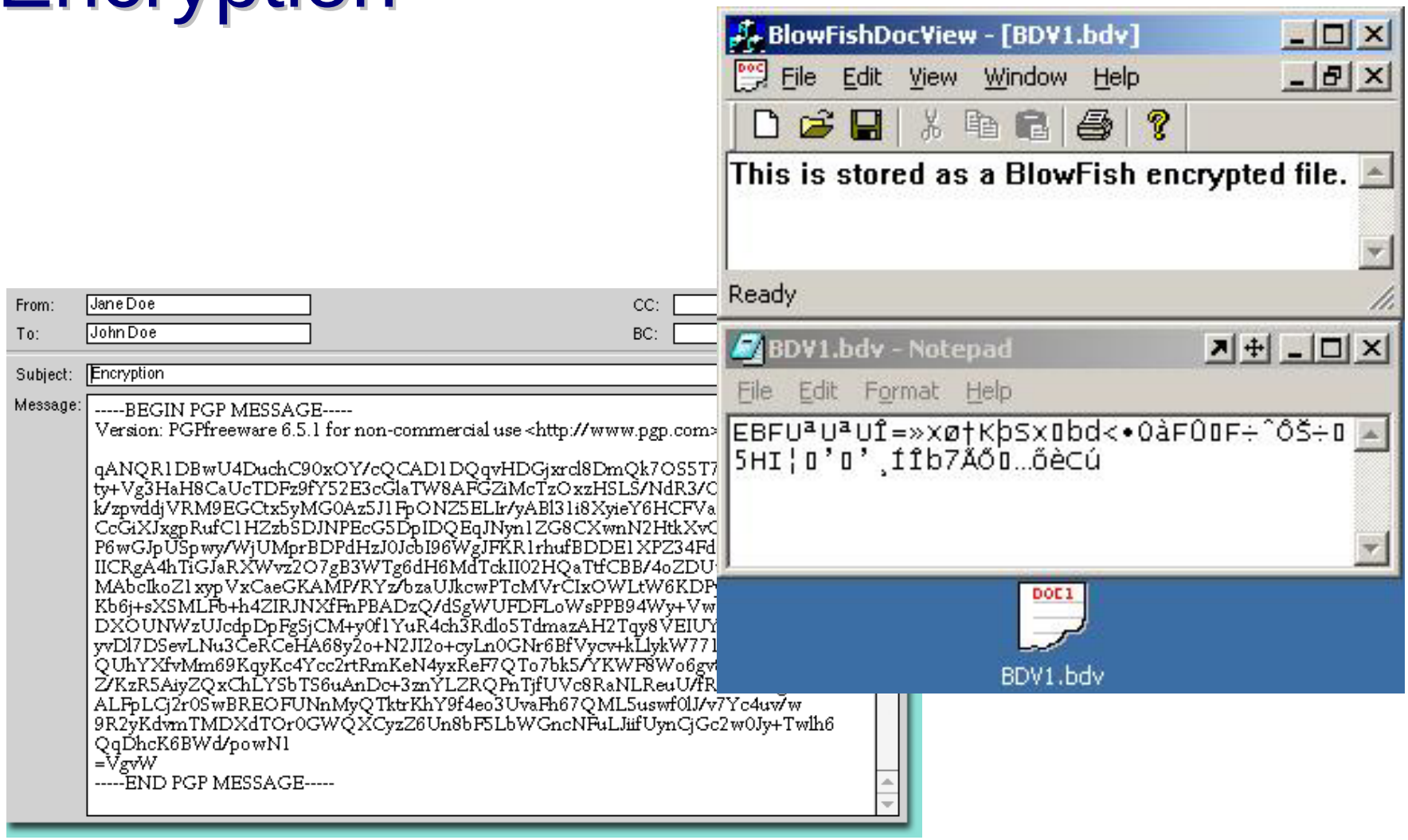
Testo in chiaro



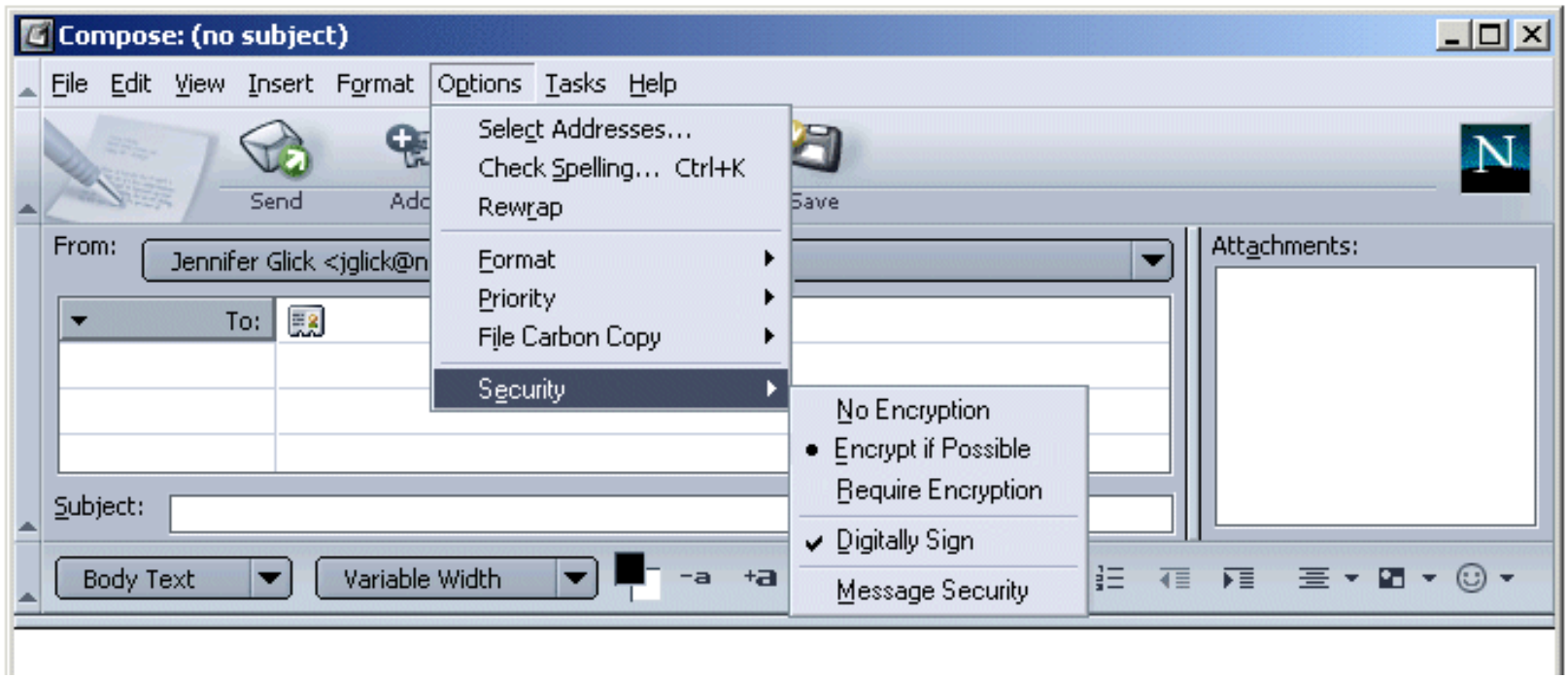
Testo criptato



Encryption


BlowFishDocView - [BDV1.bdv]
File Edit View Window Help
This is stored as a BlowFish encrypted file.
Ready
BDV1.bdv - Notepad
File Edit Format Help
BDV1.bdv
From: Jane Doe
To: John Doe
CC:
BC:
Subject: Encryption
Message:
-----BEGIN PGP MESSAGE-----
Version: PGPfreeware 6.5.1 for non-commercial use <http://www.pgp.com>
-----END PGP MESSAGE-----

Mail Encryption



Vantaggi della criptatura

- Il messaggio arriva a destinazione anche attraverso un canale insicuro
- Il documento viene letto solo da chi possiede la chiave
  - Quindi sono protetto da furti
  - Colleghi curiosi
  - Amministratori curiosi

Svantaggi della criptatura

- Non possiamo accedere al nostro file senza la conoscenza della password
  - Es password dimenticata, segretaria che si licenzia
  - Non si può chiedere all'amministratore di creare una nuova password.

Protocolli criptati

- Per rendere difficile la vita agli sniffatori si cerca di usare protocolli criptati
  - Es nel web usando **https** invece che **http**
  - Es nell'emulazione di terminale usando **ssh** invece che **telnet**
  - Es posta elettronica **imaps** invece che **imap**

L’anello debole

- Una catena è forte quanto il suo anello più debole
- Se mandata la vostra carta di credito ad un sito web dovete richiedere di farlo via **https** e non **http**
- Ma non basta
  - Se nel vostro PC c’è un programma spia che registra tutto quello che digitate
  - Se l’hacker riesce a entrare nel server web e si copia tutte i codici delle carte di credito
  - Se un impiegato del sito in cui acquistate si ricopia i codici

Domande e Risposte