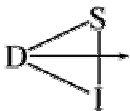


**La Gestione della Sicurezza Informatica
nelle Aziende
Firenze 29 Gennaio 2003**

Soluzioni Tecnologiche per Garantire la Sicurezza

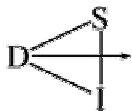
Autori

Ing. I. Bruno, Prof. P. Nesi, Ing. D. Rogai



Sommario

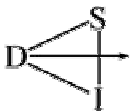
- λ Protezione locale di un computer (il bene materiale e l'informazione contenuta)
 - ♣ VIRUS
- λ Protezione e riservatezza dei dati (l'informazione e l'identità)
 - ♣ Crittografia, Firma Elettronica, Certificati, Comunicazione sicure
- λ Protezione del sistema da attacchi di intrusione (l'informazione, l'identità e la struttura)
 - ♣ Firewall



Protezione Locale

λ Virus

- ♣ Dalle statistiche risulta il primo fattore di rischio
- ♣ Sono programmi in grado di:
 - Replicarsi
 - Nascondersi
 - Attivarsi
- ♣ Sono presenti numerosi virus ognuno con diverse proprietà di azione, di replicamento, di occultamento e distruzione.
- ♣ Vengono individuati e creati nuovi tipi continuamente
- ♣ Colpiscono i dati e il software



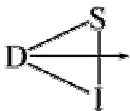
Tipologie di Virus

λ MACRO Virus

- ♣ Scritti in VBA (Visual Basic for Application).
- ♣ Multi-piattaforma (Windows & Macintosh) e non dipendono dal sistema operativo,
- ♣ Caratteristici di applicazione che consente l'uso di macro, cioè di comandi automatici.
- ♣ Programmi tipici a rischio:
 - Microsoft Office (Word, Excel, Power Point, Outlook...)
 - LOTUS AMIPRO File di tipo SAM, SMM
- ♣ Ricordate Melissa?

λ Hoaxes

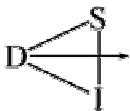
A chi non è capitato un messaggio del tipo "*...diffondete a più persone possibile: se trovate il messaggio PINCOPALLINO non apritelo perché vi formatterà il PC.*". Ebbene, si tratta di una burla al solo scopo di intasare le caselle e-mail di chiunque con un'inutile catena di S. Antonio a valanga.



Tipologie di Virus

λ Worms

- ♣ virus scritti in VBS (Visual Basic Script) o in JS (Java Script)
- ♣ viaggia e si riproduce lungo le reti
- ♣ Si instaura solo nella memoria fisica scompare allo spegnimento del computer
- ♣ Infetta i files sul disco (rendendoli inutilizzabili o in grado di riattivare il virus al riavvio del PC)
- ♣ È un mezzo per individuare informazioni sulla macchina e divulgarle sulla rete
- ♣ Es: Vampire Worms
 - ➔ silente quando il computer è utilizzato e attivo quando il computer è in stato di attesa
- ♣ Es: IRC (Internet Relay Communication) worms
 - ➔ Infetta tutti gli utenti che usano la chat mIRC
 - ➔ Consente di prendere il controllo del PC



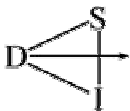
Tipologie di Virus

λ Trojan Horse

- ♣ Nasconde un'azione dannosa dietro un programma apparentemente innocuo
- ♣ Opera durante l'esecuzione dell'applicazione che lo contiene
- ♣ Il codice dannoso ha accesso alle risorse (dati, dischi, periferiche,...) senza alcuna restrizione
- ♣ Può funzionare da programma spia (Spyware)

λ Java / ActiveX

- ♣ Nuova tipologia di virus ancora poco diffusa, ma che presto diventerà una realtà
- ♣ Si contraggono dalle pagine web
- ♣ Sono programmi che vengono eseguiti automaticamente e che se non controllati possono risultare dannosi



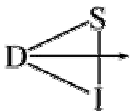
Veicoli di trasmissione

λ Supporti la memorizzazione dei dati

- ♣ Floppy Disk
- ♣ CD Rom

λ La rete Internet

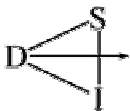
- ♣ Posta elettronica
 - Allegati
- ♣ Navigazione in rete
 - Download di file non garantiti
 - Installazione software attraverso la rete
 - Scripts o controlli ActiveX interni alla pagina web



Protegersi dai Virus

λ I Programmi Antivirus

- ♣ Software in grado di effettuare:
 - Controllo della memoria del PC alla ricerca di virus in essa residenti (es: Worms)
 - Ricerca di virus noti su supporti di memoria di massa (hard disk, floppy, etc...)
 - Ricerca di macro virus all'apertura di documenti
- ♣ Offrono:
 - Protezione in tempo reale (Real Time Protector)
 - Controllo periodico o a richiesta (On-Demand Scanning)
- ♣ Necessitano:
 - Aggiornamenti mensili dei virus conosciuti
- ♣ Possono essere
 - **locali** - installati su singola macchina
 - **centralizzati** - gestiti dal server



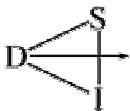
Protegersi dai Virus

λ I vantaggi di un controllo antivirus centralizzato

- ♣ L'aggiornamento avviene in modo automatico e trasparente all'utente.
- ♣ Il controllo avviene anche su traffici tra sottoreti interne e non solo su internet.
- ♣ Vengono controllati in modo automatico E-mail, FTP, HTTP, Java, ActiveX.
- ♣ Vengono anche fornite statistiche sul tipo di traffico all'interno della rete aziendale.

λ I programmi per difendersi ed eliminare i trojans

- ♣ Esistono specifici programmi in grado di identificare la presenza di un trojan horse e di rimuoverlo dalla macchina.



Futuro dei Virus

λ Multifunzionali

- ♣ È possibile assegnare al virus più funzioni distinte che si attivano in maniera "intelligente" a seconda delle caratteristiche del sistema operativo in cui si è insediato e dell'utilizzo prevalente che ne viene fatto.

λ Polimorfi e interattivi

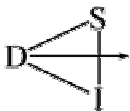
- ♣ I virus possono essere in grado di contattare il loro creatore automaticamente via internet durante la fase di diffusione, per essere aggiornati e dotarsi di caratteristiche e funzioni differenti.

λ Rapidi nella diffusione

- ♣ Virus sempre nuovi e più frequenti per mettere in difficoltà chi produce antivirus.

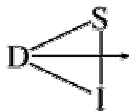
λ Invisibili

- ♣ “Worms” via posta elettronica in grado di attivarsi senza evidenziare la minima traccia della presenza del relativo programma e **senza bisogno di interazione da parte dell'utente del computer**



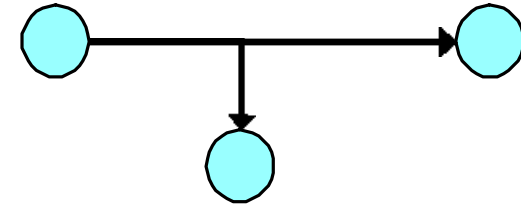
Protezione e riservatezza dei dati

- λ Internet per sua natura è un ambiente insicuro
 - ♣ Quando è stato concepito la sicurezza non appariva un problema di primaria importanza
 - ♣ Le debolezze di Internet sono presenti in deversi livelli del suo protocollo di comunicazione (TCP/IP)
- λ L'informazione è un bene prezioso e deve essere protetta
- λ L'informazione che può essere trasmessa attraverso la rete è di varia natura:
 - ♣ Dati anagrafici e personali
 - ♣ Dati fiscali (conti correnti, codici delle carte di credito)
 - ♣ Dati aziendali (accordi, contratti, preventivi)
 - ♣ Dati medici (cartelle cliniche elettroniche, risultati di esami)

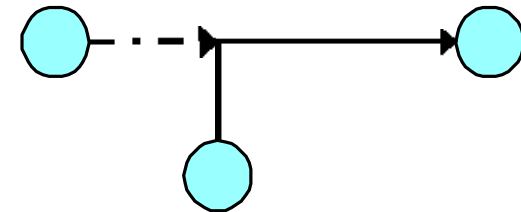


Cosa succede se i dati non sono protetti

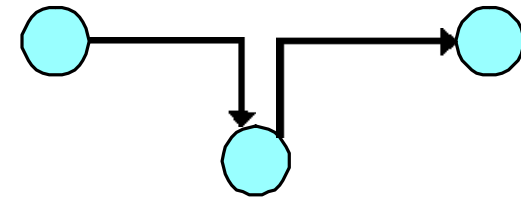
λ L'informazione può essere letta da terzi
(Sniffing o Eavesdropping)



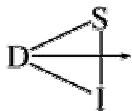
λ Una terza entità può sostituirsi al mittente o al destinatario
(Spoofing o Masquerading)



λ L'informazione può essere alterata oppure trattenuta e ritrasmessa in ritardo (Hijacking)



λ L'intercettazione dell'informazione può rivelare importanti proprietà sul tipo di sistema e di comunicazione usato



Strumenti per la sicurezza dei dati

λ Crittografia

- ♣ Confidenzialità

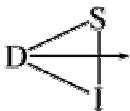
λ Firma elettronica

- ♣ Integrità
- ♣ Autenticità
- ♣ Non ripudio

λ Certificati (X.509 v3) e Certification Authority

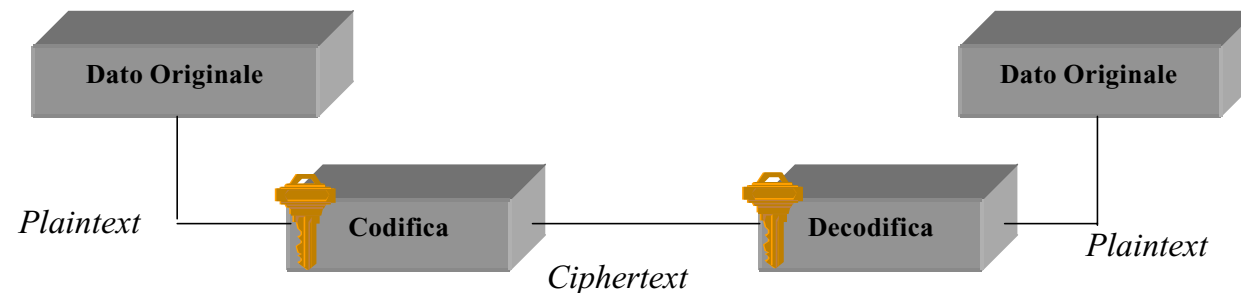
λ Steganografia (watermark)

λ Protocolli per la comunicazione sicura



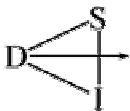
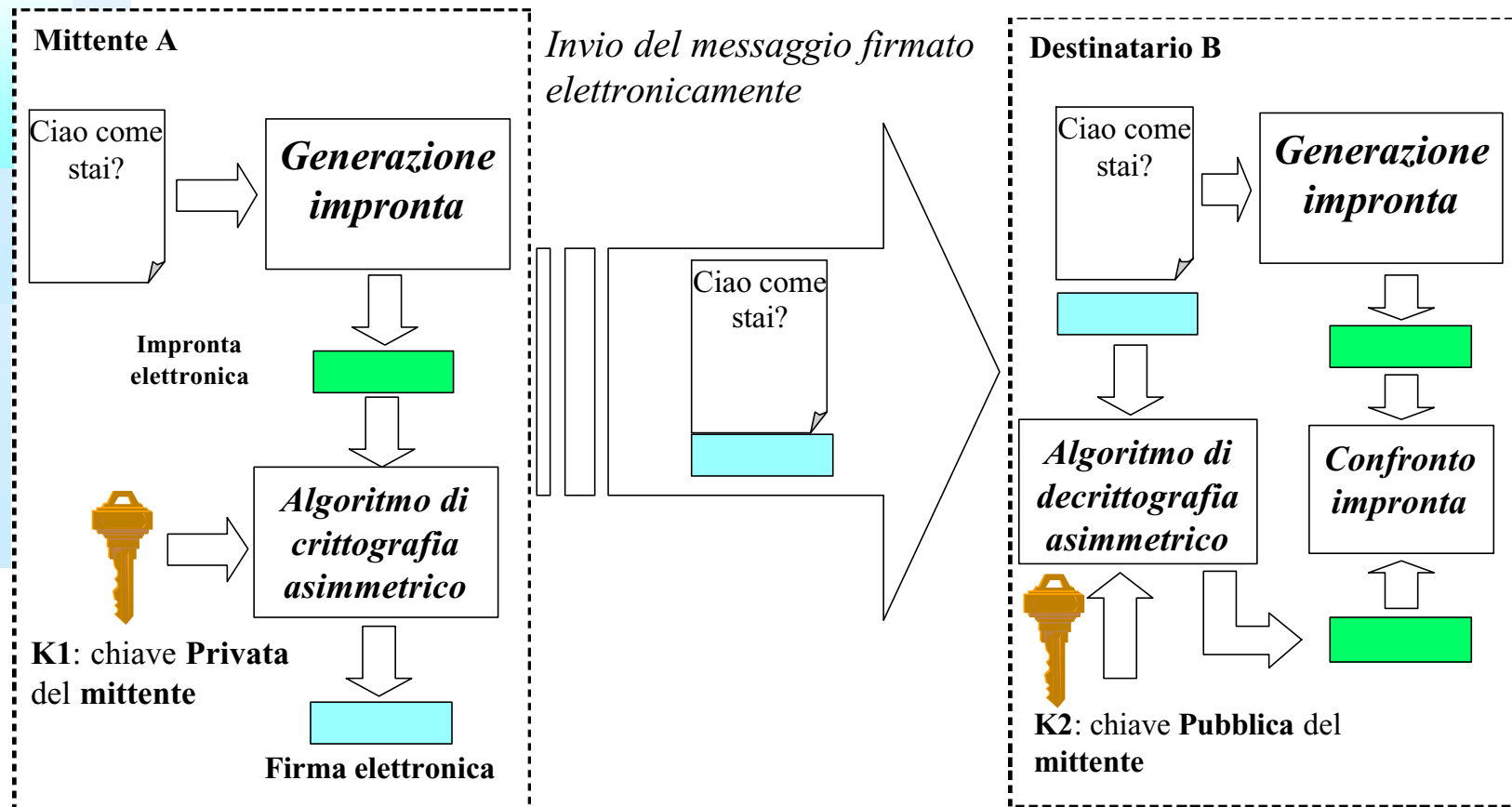
Utilizzo della crittografia

- λ Encryption è il processo che codifica un messaggio in modo da nascondere il contenuto
- λ Si basano sull'uso di parametri segreti chiamati *chiavi*
- λ Si dividono in due classi fondamentali
 - ♣ Chiavi *segrete* condivise (*simmetrico*)
 - *DES, TripleDES, IDEA, AES (o Rijndael).*
 - ♣ Coppie di chiavi *pubblica/privata* (*asimmetrico*)
 - *RSA, Diffie Helman, EL Gamal, Curve Ellittiche.*



Schema di crittografia

Firma Elettronica

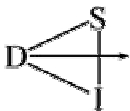





Certificati

- λ Documento (breve) che attesta dati di un utente (o di un sistema)
- λ Firmati elettronicamente dall'ente emettitore: la Certification Authority (CA)
- λ Verificati mediante la chiave pubblica della CA
- λ Hanno una validità limitata e sono revocabili sia dall'utente che dall'emettitore

1. <i>Certificate type</i>	Account number
2. <i>Name</i>	Alice
3. <i>Account</i>	6262626
4. <i>Certifying authority</i>	Bob's Bank
5. <i>Signature</i>	$\{ \text{Digest}(\text{field 2} + \text{field 3}) \}_{K_{Bpriv}}$



Protocolli per la comunicazione sicura

λ Tecnologie disponibili

♣ IPsec

- Supportato in IPv6 – nuova versione del protocollo IP attuale IPv4, consente la crittografia al livello più basso del protocollo
- Ideale per la configurazione di Virtual Private Network (sotto reti molto distanti tra loro connesse tramite linee della rete Internet)

♣ SSL

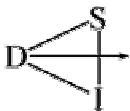
- Per la comunicazione remota attraverso canali sicuri (trasmissione crittografata)

♣ S-MIME

- Per la riservatezza della posta elettronica e degli allegati

♣ S-HTTP

- Accesso sicuro a pagine web

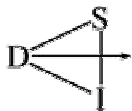


Protezione da intrusione esterna

λ La connessione continua (esempio tramite linea ADSL, Fastweb) ad Internet espone il sistema ad attacchi di tipo intrusivo

λ Tali attacchi hanno lo scopo di:

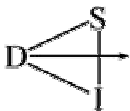
- ♣ Prendere in ostaggio un computer per “camuffare” il proprio indirizzo IP
- ♣ Interrompere un servizio sovraccaricandolo di richieste (Denial of Service)
- ♣ Leggere dati senza autorizzazione (Spionaggio)
- ♣ Inserire virus (trojan horses o backdoors)
- ♣ Prendere il possesso della macchina per fini illeciti (perpetrazione di attacchi verso altre reti)



Strumenti per la difesa perimetrale

λ Firewall

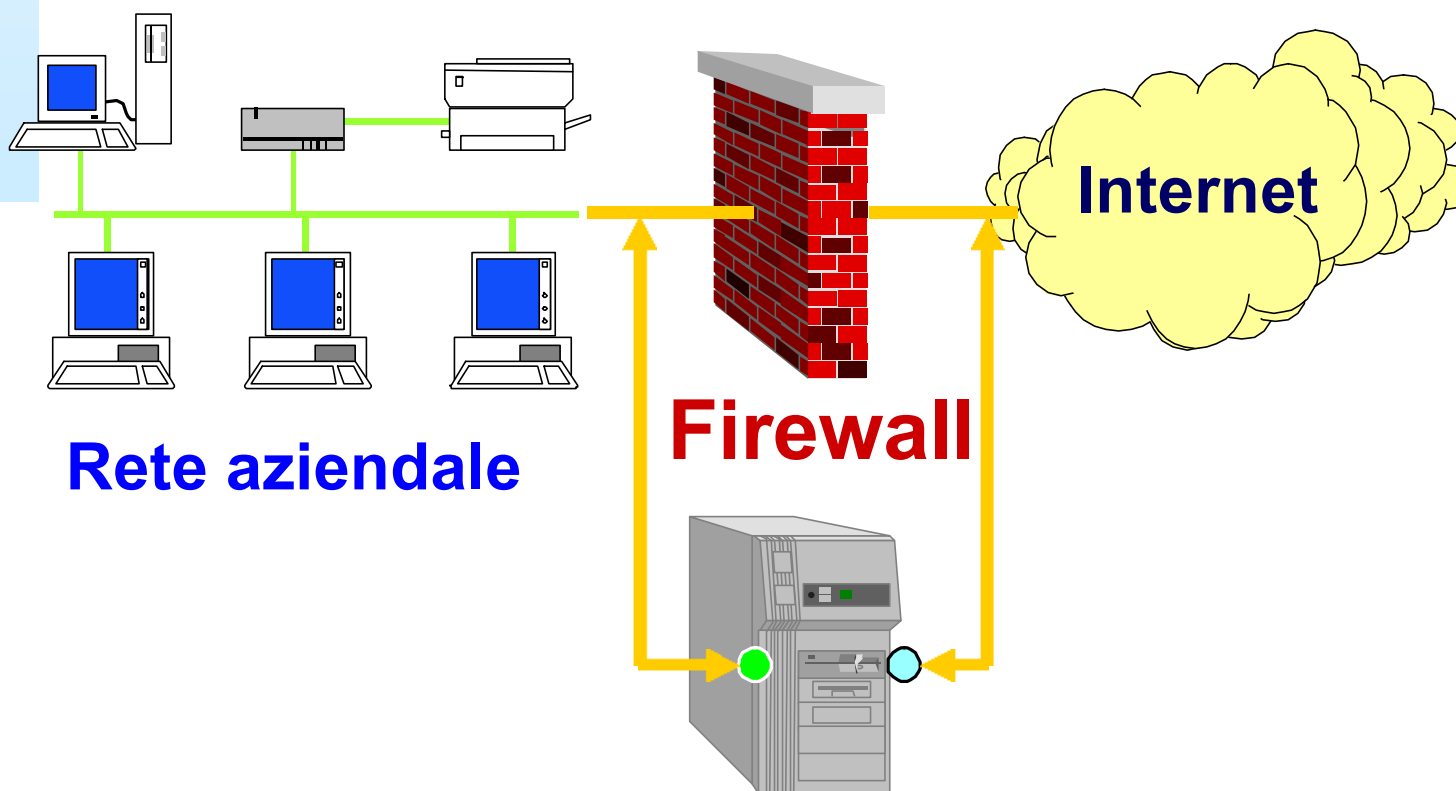
- ♣ Insieme di hardware e software posto nel punto di connessione tra la rete aziendale e la rete internet
- ♣ Ha il compito di monitorare e filtrare il traffico in ingresso e in uscita dalla rete
- ♣ Attua politiche di sicurezza relative ai servizi offerti dalla rete Internet
 - ➔ l'utente può navigare su internet e scaricare la posta, ma non può ricevere allegati di determinati tipi
 - ➔ solo alcuni indirizzi IP della rete esterna possono accedere al servizio di trasferimento file della rete locale
- ♣ Consente filtraggi con diversi livelli di protezione e resistenza agli attacchi
 - ➔ Static Filtering (possibile anche attraverso il router)
 - ➔ Dynamic Filtering / Proxy (a livello di applicazione)



Utilizzo del firewall

λ Filtraggio del traffico:

- ❖ Ogni informazione è controllata e, solo se è autorizzata dalla politica di sicurezza, può attraversare il firewall



Grazie per l'attenzione

