La sicurezza informatica

Antonio Lioy
< lioy @ polito.it >

Politecnico di Torino
Dip. Automatica e Informatica

Bibliografia (in Inglese)

- **B.Schneier: "Applied cryptography"**
- **W.Stallings:**
  "Cryptography and network security"
- **S.Garfinkel, G.Spafford:**
  "Practical Unix and Internet security"
- **W.R.Cheswick, S.M.Bellovin:**
  "Firewalls and Internet security" (2nd ed.)
- **C.P.Pfleeger, S.Pfleeger:**
  "Security in computing"

Bibliografia (in Italiano)

- **W.Stallings**
  "Sicurezza delle reti - applicazioni e standard"
  Addison-Wesley Italia
- **C.Pfleeger, S.Pfleeger**
  "Sicurezza in informatica"
  Pearson Education Italia
- **Fugini, Maio, Plebani**
  "Sicurezza dei sistemi informativi"
  Apogeo, 2001
- **S.Singh**
  "Codici e segreti"
  BUR saggi, 2001

© Antonio Lioy - Politecnico di Torino (2005-09)

Agenda

- **introduzione alla sicurezza dei sistemi informatici**
- **organizzazione e tecnologie della sicurezza**
- **risvolti legali**
- **analisi costi-benefici**

Agenda (I)

- **introduzione alla sicurezza dei sistemi informatici:**
  - l'evoluzione dei SI ed il problema sicurezza
  - i problemi ed il lessico della sicurezza informatica
  - gli attacchi tecnologici (sniffing, spoofing, …)
  - gli attacchi non tecnologici (social eng.)
- **organizzazione e tecnologie della sicurezza**
- **risvolti legali**
- **analisi costi-benefici**

Una definizione di sicurezza informatica

E' l'insieme dei prodotti, dei servizi, delle regole organizzative e dei comportamenti individuali che proteggono i sistemi informatici di un'azienda.

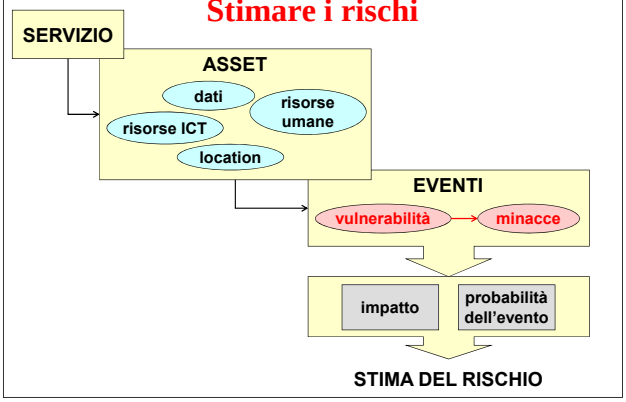
Ha il compito di proteggere le risorse da accessi indesiderati, garantire la riservatezza delle informazioni, assicurare il funzionamento e la disponibilità dei servizi a fronte di eventi imprevedibili (C.I.A.).

L'obiettivo è custodire le informazioni con la stessa professionalità ed attenzione con cui ci si prende cura di gioielli o certificati azionari depositati nel caveau.

Il sistema informatico è la cassaforte delle nostre informazioni più preziose; la sicurezza informatica è l'equivalente delle serrature, combinazioni e chiavi che servono a proteggerla.

© Antonio Lioy - Politecnico di Torino (2005-09)

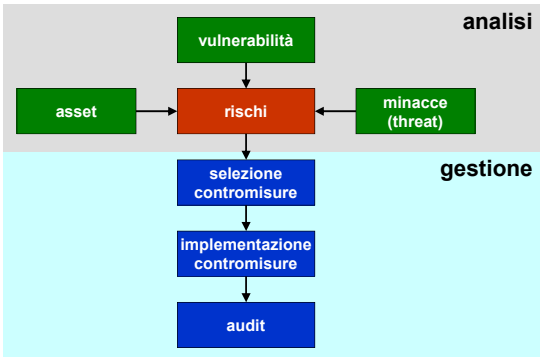
Stimare i rischi



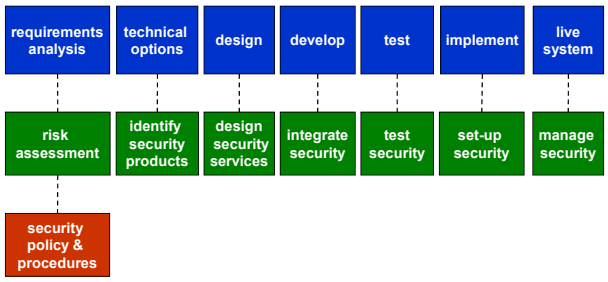
Terminologia

- **ASSET = l'insieme di beni, dati e persone necessarie all'erogazione di un servizio IT**
- **VULNERABILITA' = debolezza di un asset**
  - es. pwd = login; sensibile alle inondazioni
- **MINACCIA = atto volontario o evento accidentale che può causare la perdita di una proprietà di sicurezza**
- **ATTACCO = realizzazione pratica di una minaccia (di tipo "atto volontario")**
- **EVENTO (NEGATIVO) = realizzazione pratica di una minaccia (di tipo "evento accidentale")**

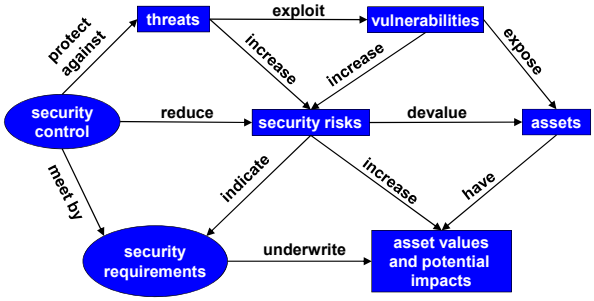
Analisi e gestione della sicurezza



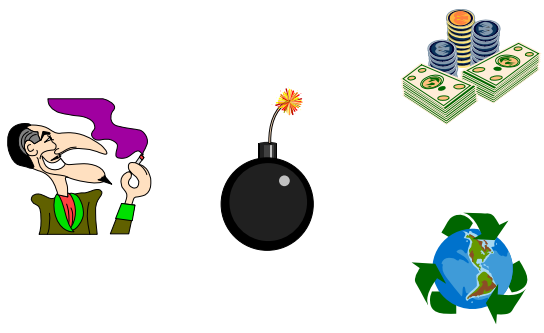
La sicurezza nel ciclo di vita di un sistema



Relazioni nel campo della sicurezza

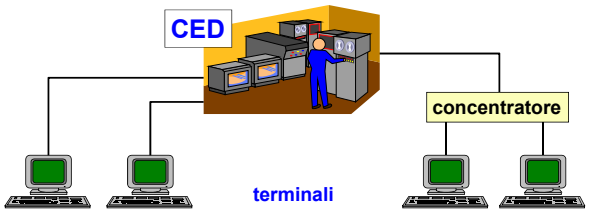


Perché è esploso il problema "sicurezza" ?



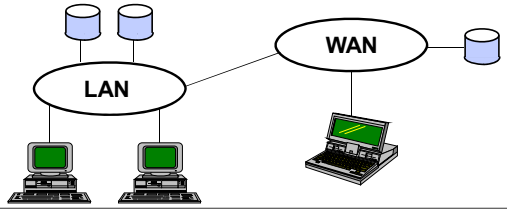
Vecchi paradigmi

- informazioni ed elaborazione centralizzate
- accesso tramite postazioni "stupide"
- comunicazione "unicast" tramite linee dedicate

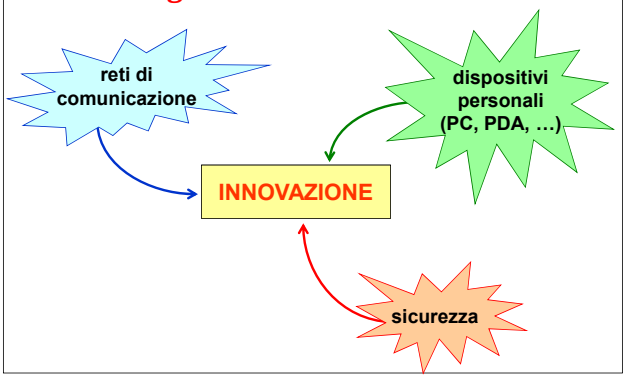


Nuovi paradigmi

- informazioni ed elaborazione distribuite
- accesso tramite postazioni distribuite intelligenti
- comunicazioni "broadcast" e/o linee condivise
- nuovi paradigmi applicativi (web, P2P, SMS, …)



La tecnologia come motore di innovazione

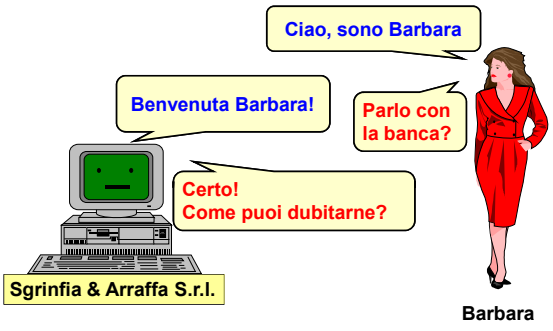


Proprietà (astratte) di sicurezza

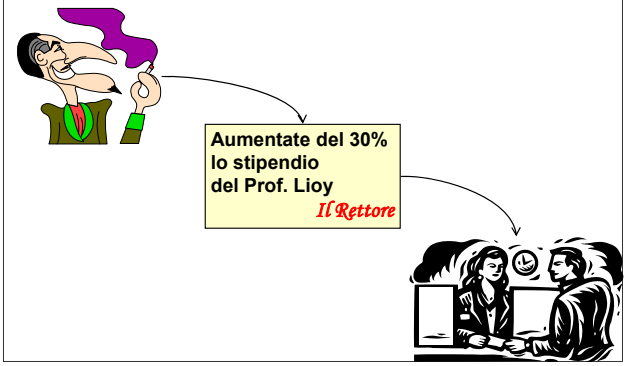
autenticazione (semplice / mutua)	*authentication (simple / mutual)*
autenticazione della controparte	*peer authentication*
autenticazione dei dati	*data / origin authentication*
autorizzazione, controllo accessi	*authorization, access control*
integrità	*integrity*
riservatezza, confidenzialità	*confidentiality, privacy, secrecy*
non ripudio	*non repudiation*
disponibilità	*availability*
tracciabilità	*accountability*

Autenticazione (della controparte)

Mutua autenticazione (delle controparti)



Autenticazione (dei dati)



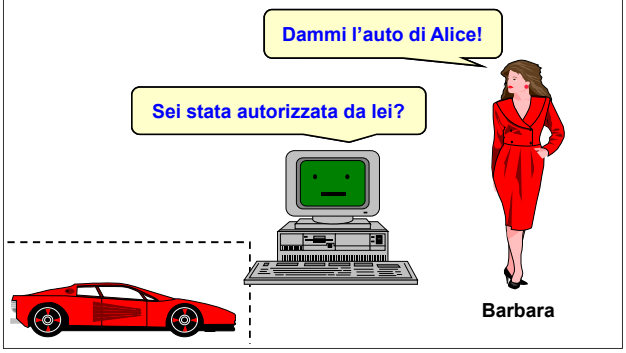
Non ripudio

- **prova formale - usabile in tribunale - che dimostra in modo innegabile l'autore dei dati**
- **molti aspetti da considerare:**
  - autenticazione (del mittente)
  - integrità
  - identificazione (del mittente)
  - . . .

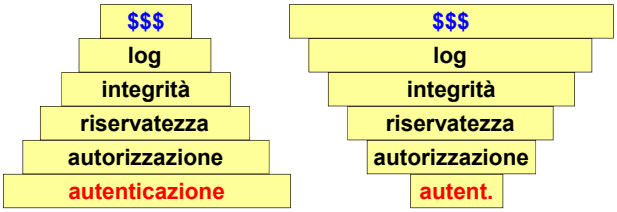
Non ripudio - esempio

- **consideriamo il non ripudio di una firma elettronica:**
  - sintassi (è la tua firma?)
  - semantica (hai capito ciò che stavi firmando?)
  - volontà (hai firmato volontariamente?)
  - identificazione (sei stato tu a firmare?)
  - tempo (quando hai firmato?)
  - luogo (dove hai firmato?)

Autorizzazione (controllo accessi)

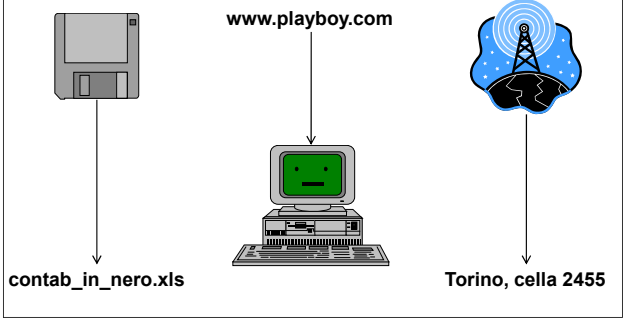


La piramide della sicurezza

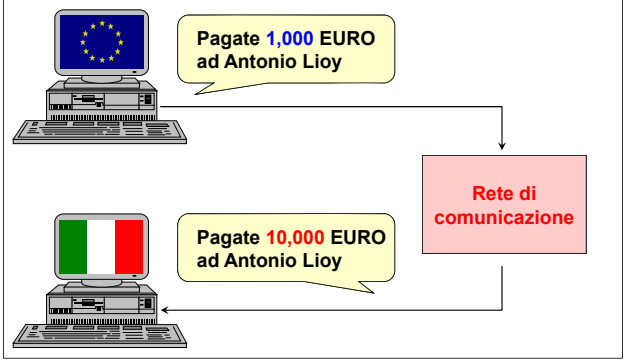


Riservatezza

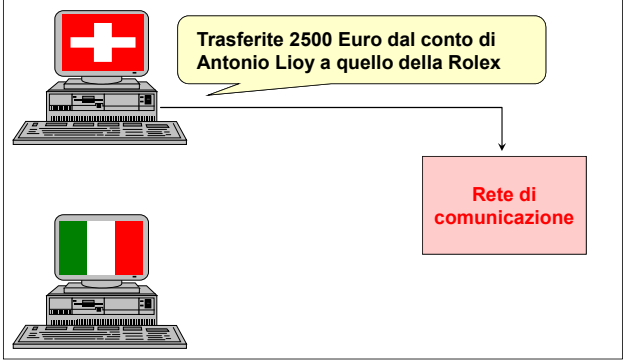
Riservatezza (dati, azioni, posizione)



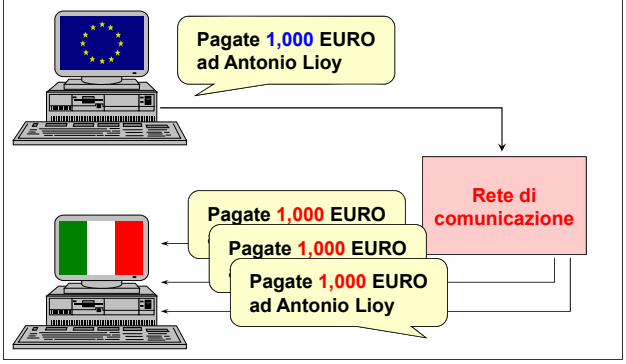
Integrità (modifica)



Integrità (cancellazione)

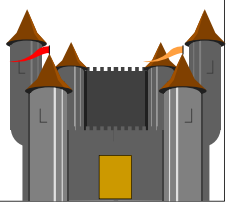


Attacchi di tipo “replay”



Sicurezza: dove è il nemico?

- **fuori dalla nostra organizzazione**
  - difesa del perimetro (firewall)
- **fuori dalla nostra organizzazione, con l’eccezione dei nostri partner**
  - protezione dell’Extranet (VPN)
- **dentro la nostra organizzazione**
  - protezione della Intranet (?!)
- **ovunque !**
  - protezione delle applicazioni



Da dove parte l’attacco? (2006)

- **Internet (50% del campione)**
- **internal system (50%)**

(da un’analisi condotta nel 2006 da CSI/FBI su un campione di 536 aziende USA)

Conseguenze di un attacco (2006)

- virus (65% del campione)
- furto di laptop/PDA (47%)
- abuso nell'uso delle reti da insider (42%)
- accessi non autorizzati ai dati da insider (32%)
- denial-of-service (25%)
- penetrazione nei sistemi (15%)
- abuso di reti wireless (14%)
- furti di informazioni riservate (9%)
- frodi finanziarie (9%)
- frodi TLC (8%)
- web defacement / web app misuse (6%)

Insicurezza: le cause profonde (I)

- "Attack technology is developing in a open-source environment and is evolving rapidly"
- "Defensive strategies are reactionary"
- "Thousands - perhaps millions - of system with weak security are connected to the Internet"
- "The explosion in use of the Internet is straining our scarse technical talent. The average level of system administrators … has decreased dramatically in the last 5 years"

Insicurezza: le cause profonde (II)

- "Increasingly complex sw is being written by programmers who have no training in writing secure code"
- "Attacks and attack tools trascend geography and national boundaries"
- "The difficulty of criminal investigation of cybercrime coupled with the complexity of international law means that … prosecution of computer crime is unlikely"

da "Roadmap for defeating DDOS attacks"
(feb. 2000, after Clinton meeting at White House)
aggiornamenti su www.sans.org/dosstep/roadmap.php

Problemi base (tecnologici)

- **le reti sono insicure:**
  - le comunicazioni avvengono in chiaro
  - le reti locali funzionano in broadcast
  - le connessioni geografiche non avvengono tramite linee punto-punto ma:
    - attraverso linee condivise
    - tramite router di terzi
- **autenticazione debole degli utenti (normalmente basata su password)**
- **non c'è autenticazione dei server**
- **il software contiene molti bachi!**

Alcune tipologie di attacco

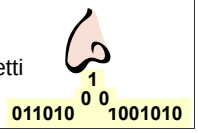
- **IP spoofing / shadow server**
  qualcuno si sostituisce ad un host
- **packet sniffing**
  si leggono password di accesso e/o dati riservati
- **connection hijacking / data spoofing**
  si inseriscono / modificano dati durante il loro transito in rete
- **denial-of-service (distributed DoS)**
  si impedisce il funzionamento di un servizio (es. la guerra dei ping)

IP spoofing

- **falsificazione dell'indirizzo di rete del mittente**
- **solitamente si falsifica l'indirizzo di livello 3 (IP) ma nulla vieta di falsificare anche quello di livello 2 (ETH, TR, ...)**
- **meglio chiamarlo *source address spoofing***
- **attacchi:**
  - falsificazione di dati
  - accesso (non autorizzato) a sistemi
- **contromisure:**
  - NON usare mai autenticazione basata sugli indirizzi di rete

Packet sniffing

- **lettura dei pacchetti destinati ad un altro nodo della rete**
- **facile da fare in reti broadcast (es. LAN) o nei nodi di smistamento (es. switch, router)**
- **attacchi:**
  - permette di intercettare qualunque cosa (password, dati, ...)
- **contromisure:**
  - reti non broadcast (!?)
  - crittografia del payload dei pacchetti



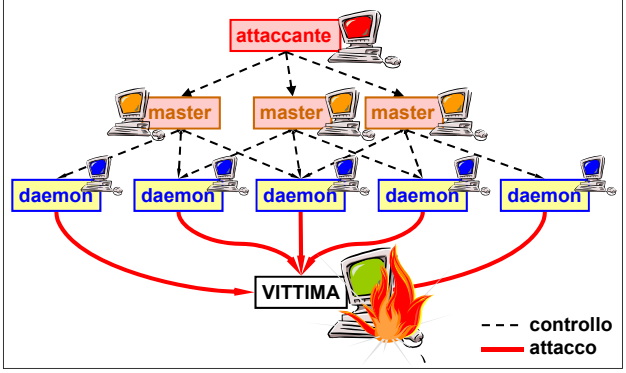
Denial-of-service (DoS)

- **si tiene impegnato un host in modo che non possa fornire i suoi servizi**
- **esempi:**
  - saturazione della posta / log
  - ping flooding (“guerra dei ping”)
  - SYN attack
- **attacchi:**
  - impedisce l’uso di un sistema / servizio
- **contromisure:**
  - nessuna definitiva, solo palliativi quantitativi

Distributed denial-of-service (DDOS)

- **software di attacco DOS installato su molte macchine (chiamate daemon o zombie)**
- **daemon controllati remotamente da un master (spesso tramite canali cifrati) e con capacità di auto-aggiornamento**
- **effetto dell’attacco base moltiplicato per il numero di daemon**
- **esempi:**
  - TrinOO
  - TFN (Tribe Flood Network)
  - Stacheldraht (=filo spinato)

DDoS attack



Feb 8th 2000, 10.30am (PST) @ Yahoo Server Farm

- "the initial flood of packets, which we later realized was in excess of 1G bits/sec, took down one of our routers …"
- "… after the router recovered we lost all routing to our upstream ISP …"
- "… it was somewhat difficult to tell what was going on, but at the very least we noticed lots of ICMP traffic …"
- "… at 1.30pm we got basic routing back up and then realized that we were under a DDoS attack"

http://packetstorm.decepticons.org/distributed/yahoo.txt

The lawyer said ...

"There is a distinct probability that if your site has been hijacked for a denial of service attack, then you could be liable for damages.

I would definitely advise clients they have grounds to sue."

Nick Lockett, e-commerce lawyer at Sidley & Austin

"Be Secure or Be Sued"
Silicon.com, 16 Nov 2000

http://www.silicon.com/a40900

Che cosa fa la polizia? (1ª parte)

"The strange tale of the attacks against GRC.COM"
by Steve Gibson, Gibson Research Corporation

http://grc.com/dos/grcdos.htm

- **"Both FBI guys said similar things …"**
- **"They explained that until $5,000 of damage had been done, no crime had even been committed. That's the law. And due to the peculiar nature of GRC.COM's business model (such as it is :), these attacks were stirring up interest in my forthcoming research and it wasn't even clear that we were going to be economically damaged in any way."**

Che cosa fa la polizia? (2ª parte)

- **"Secondly, they said that even if we did manage to meet the $5,000 minimum required for "Wicked's" activities to qualify as criminal, their staffs were overloaded and swamped with cases involving companies that had lost huge sums of money to Internet crime.**
  Furthermore, since the cost of an FBI prosecution was in the neighborhood of $200,000, they needed to prioritize their cases based upon prosecuting criminals who were responsible for causing large dollar losses.
  "Wicked's" attacks, no matter how annoying, failed to qualify."

Che cosa fa la polizia? (3ª parte)

- **"And finally, they said that since "Wicked" was only 13 years old, nothing much would happen to him, even if the preponderance of evidence demonstrated that he was behind these attacks. They said that a couple of agents might go out to his home and have a talk with his parents, but in this country his youth was an impenetrable shield. This, of course, further discouraged the costs which would be incurred through any investigation."**

© Antonio Lioy - Politecnico di Torino (2005-09)

DDoS references

- **il prof. Dave Dittrich è uno dei massimi esperti:**

  http://staff.washington.edu/dittrich/misc/ddos/

- **il caso di Steve Gibson ha suscitato molte discussioni:**

  http://grc.com/dos/grcdos.htm

Shadow server

- **elaboratore che si pone come fornitore di un servizio senza averne il diritto**
- **richiede address spoofing e packet sniffing**
- **il server ombra deve essere più veloce di quello reale, oppure questo non deve essere in grado di rispondere (guasto o sotto attacco, es. DoS)**
- **attacchi:**
  - fornitura di un servizio sbagliato
  - cattura di dati forniti al servizio sbagliato
- **contromisure:**
  - autenticazione del server

Connection hijacking

- **anche detto *data spoofing***
- **si prende il controllo di un canale di comunicazione e si inseriscono, cancellano o manipolano dei pacchetti**
- **MITM (Man In The Middle) logico o fisico**
- **attacchi:**
  - lettura, falsificazione e manipolazione di dati
- **contromisure:**
  - autenticazione, integrità e serializzazione di ogni singolo pacchetto di rete

Software bug

- **anche il miglior software contiene dei bug che possono essere sfruttati per vari fini**
- **sfruttamento più semplice: DoS**
- **esempio: WinNT server (3.51, 4.0)**
  - telnet alla porta 135
  - 10 caratteri a caso, poi CR
  - server non disponibile!
    (CPU al 100% senza che venga svolto alcun lavoro)
  - soluzione: installare SP3

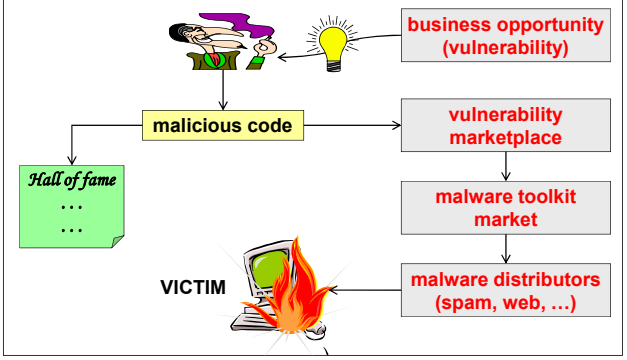
Alcuni tipici problemi applicativi

- **buffer overflow**
- **memorizzare nei cookie informazioni sensibili**
- **memorizzare le password in chiaro in un DB**
- **"inventare" un sistema di protezione**

Virus e worm (malware)

- **virus = provoca danni e si replica**
- **worm = provoca danni perché si replica**
- **richiede complicità (anche involontaria):**
  - dell'utente (gratis, free, urgente, importante, …)
  - del sistemista (malconfigurazione)
  - del produttore (esecuzione automatica, trusted, …)
- **contromisure:**
  - sensibilizzazione degli utenti
  - configurazioni corrette / sw sicuro
  - installazione (ed aggiornamento!) degli antivirus

Malware food chain



Problemi base (non tecnologici)

- scarsa comprensione del problema (awareness)
- fallibilità degli esseri umani (soprattutto in condizioni di sovraccarico, frustrazione, …)
- gli esseri umani hanno una naturale tendenza alla fiducia
- interfacce / architetture complesse che facilitano gli errori
- calo di prestazioni dovuto all'applicazione delle misure di sicurezza
- …

Social engineering

- si chiede la partecipazione (inconsapevole) dell'utente all'azione di attacco
- si sfruttano utenti ingenui ("per favore cambia subito la password con la seguente, perché il tuo PC è sotto attacco") …
- … ma si attaccano anche utenti esperti (es. copiando un mail autentico ma cambiandogli un allegato o una URL)
- via mail, telefono o anche comunicazioni cartacee

Esempi di social engineering

- **il Phishing (~ fishing = la pesca al gonzo)**
  - "gentile utente del servizio di Internet banking la preghiamo di compilare e spedirci il seguente modulo ai sensi della legge 675 …"
- **pressioni psicologiche:**
  - "se non mi aiuti sono nei pasticci …"
  - "se non fai quello che chiedo lo segnalerò al tuo responsabile …"
- **dimostrare di conoscere bene l'azienda, le persone, le procedure per far abbassare la guardia**

Un mail dalla CIA …

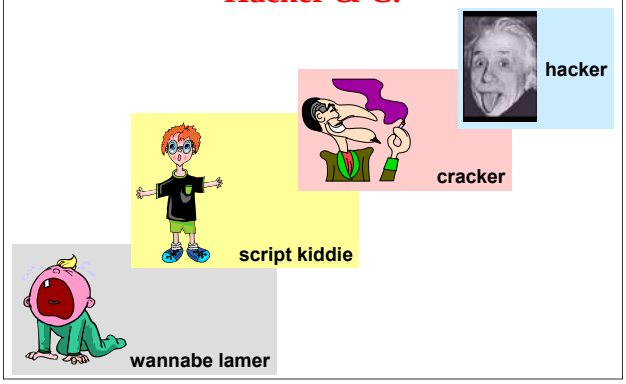
```
From: Post@cia.gov
Date: Tue, 22 Nov 2005 17:51:14 UTC
X-Original-Message-ID: <1e3c8.15d13bbb95@cia.gov>
Subject: You_visit_illegal_websites

Dear Sir/Madam,
we have logged your IP-address on more than 30 illegal Websites.
Important: Please answer our questions!
The list of questions are attached.

Yours faithfully,
Steven Allison

++++ Central Intelligence Agency -CIA-
++++ Office of Public Affairs
++++ Washington, D.C. 20505
++++ phone: (703) 482-0623
++++ 7:00 a.m. to 5:00 p.m., US Eastern time
```

Hacker & C.



Hacker (I)

hacker: /n./ [originally, someone who makes furniture with an axe]

1. A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary.

2. One who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming.

3. A person capable of appreciating {hack value}.

4. A person who is good at programming quickly.

Hacker (II)

5. An expert at a particular program, or one who frequently does work using it or on it; as in "a Unix hacker". (Definitions 1 through 5 are correlated, and people who fit them congregate.)

6. An expert or enthusiast of any kind. One might be an astronomy hacker, for example.

7. One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations.

8. [deprecated] A malicious meddler who tries to discover sensitive information by poking around. Hence "password hacker", "network hacker". The correct term for this sense is {cracker}.

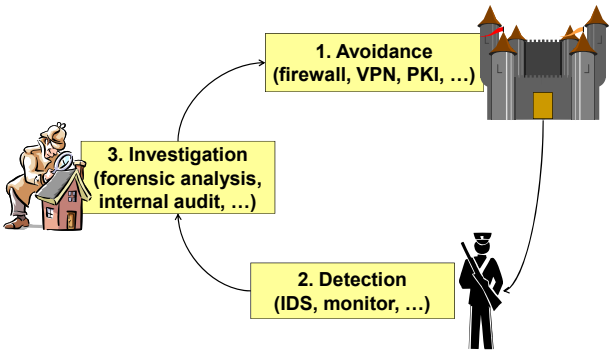
Cracker

cracker: /n./ One who breaks security on a system. Coined ca. 1985 by hackers in defense against journalistic misuse of {hacker} (q.v., sense 8). An earlier attempt to establish "worm" in this sense around 1981-82 on Usenet was largely a failure.

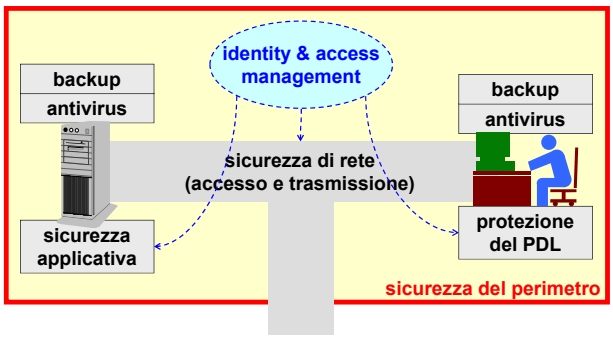
Agenda (II)

- introduzione alla sicurezza dei sistemi informatici
- **organizzazione e tecnologie della sicurezza:**
  - componenti base
  - tecnologie di autenticazione
  - tecnologie di sicurezza di rete
  - tecnologie di sicurezza applicativa
  - investigazione
- risvolti legali
- analisi costi-benefici

I tre pilastri della sicurezza

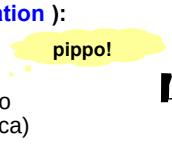


Componenti base



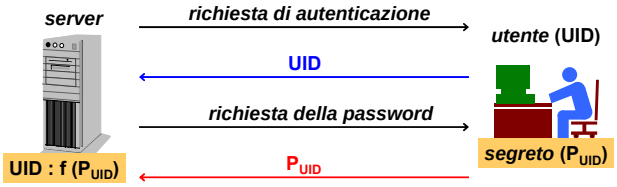
Metodologie di autenticazione

- **basate su meccanismi diversi (1/2/3-factors authentication):**
  - qualcosa che so (es. una password)
  - qualcosa che posseggo (es. una carta magnetica)
  - qualcosa che sono (es. impronta digitale)

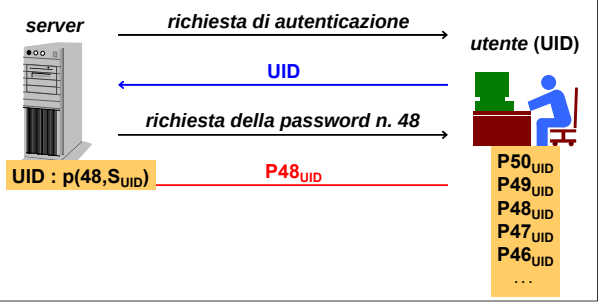


- **possibilità di combinare meccanismi diversi per identificazione personale**

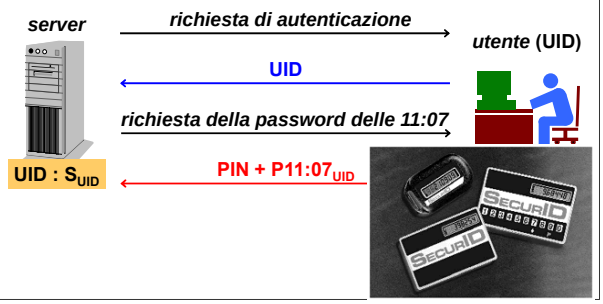
Password (ripetibili)



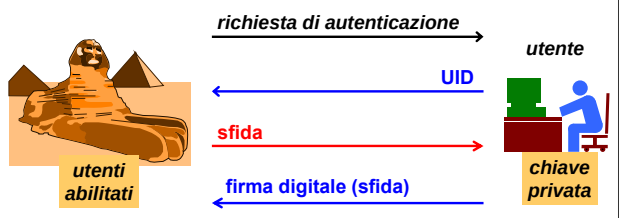
Password (usa-e-getta)



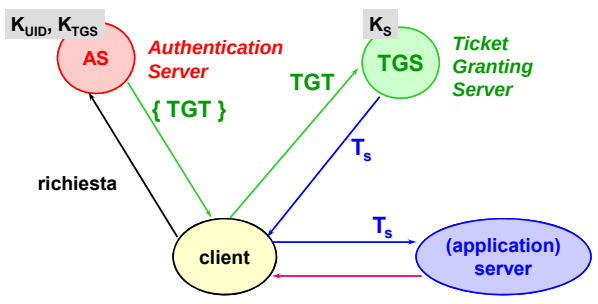
Password (usa-e-getta con autenticatore)



Autenticazione a sfida (asimmetrica)



Kerberos

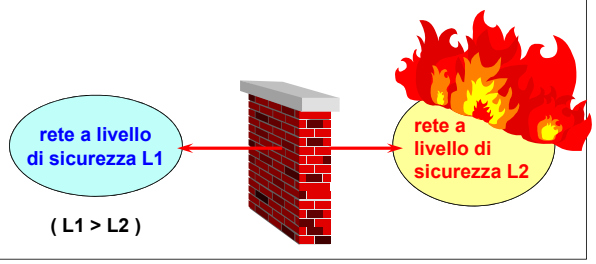


Autenticazione di esseri umani

- **come essere certi di stare interagendo con un essere umano e non con un programma (es. che invia una password memorizzata in un file)?**
- **due soluzioni:**
  - tecniche CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart)
    - es. immagini di caratteri distorti
  - tecniche biometriche
    - es. impronte digitali

Che cos'è un firewall?

- **firewall = muro tagliafuoco**
- **collegamento controllato tra reti a diverso livello di sicurezza = sicurezza del perimetro**

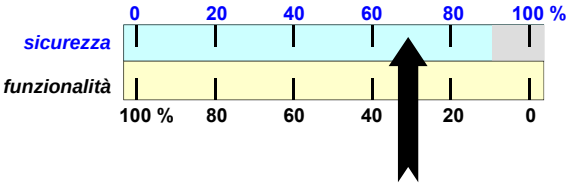


Progettazione di un FW

Un firewall non si "compra", si progetta (si comprano i suoi componenti)

- **si tratta di trovare il compromesso ottimale ...**
- **... tra sicurezza e funzionalità**
- **... col minimo costo**

L'indice della sicurezza



I TRE PRINCIPI INDEROGABILI DEI FIREWALL

I. il FW deve essere l'unico punto di contatto della rete interna con quella esterna

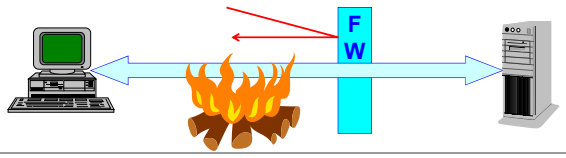
II. solo il traffico "autorizzato" può attraversare il FW

III. il FW deve essere un sistema altamente sicuro esso stesso

D.Cheswick
S.Bellovin

Ma non basta un firewall?

- un firewall impedisce gli accessi non conformi alla politica di sicurezza aziendale
- un firewall è inefficace contro gli attacchi condotti:
  - dalla zona interna al firewall
  - sui canali di accesso leciti
- occorre sicurizzare le singole applicazioni



Che cos'è una VPN?

- una tecnica (hardware e/o software) per realizzare una rete privata ...
- ... utilizzando canali e apparati di trasmissione condivisi

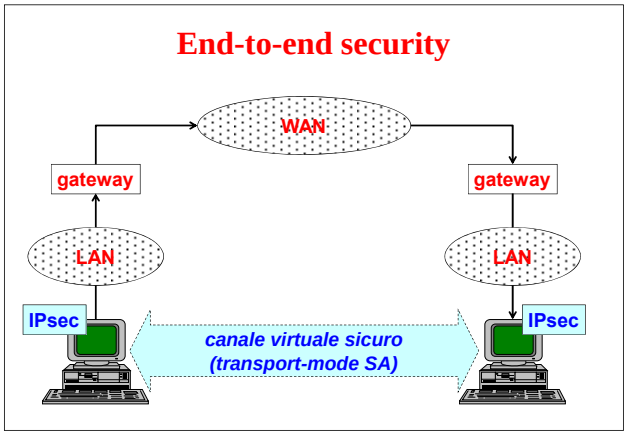
Dove si applica una VPN?

- quando si attraversa una rete pubblica e/o non fidata ...
- ... per comunicazioni intra-aziendali tra sedi remote (Intranet)
- ... per comunicazioni inter-aziendali chiuse tra aziende che si sono previamente accordate (Extranet)

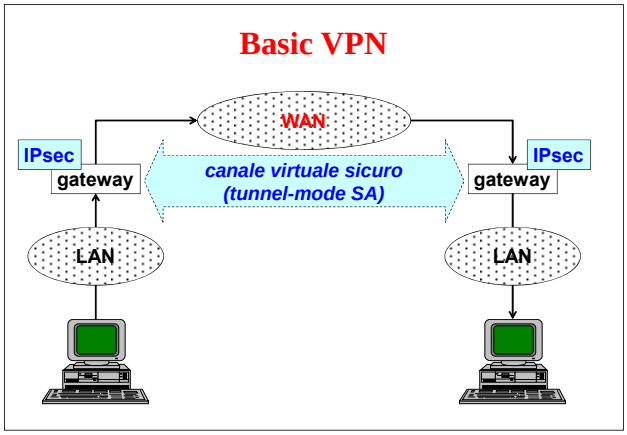
Dove NON si applica una VPN?

- quando si attraversa una rete pubblica e/o non fidata ...
- ... per comunicazioni inter-aziendali senza accordi precedenti
- ... per comunicazioni con clienti non noti a priori (commercio elettronico di tipo business-to-consumer)

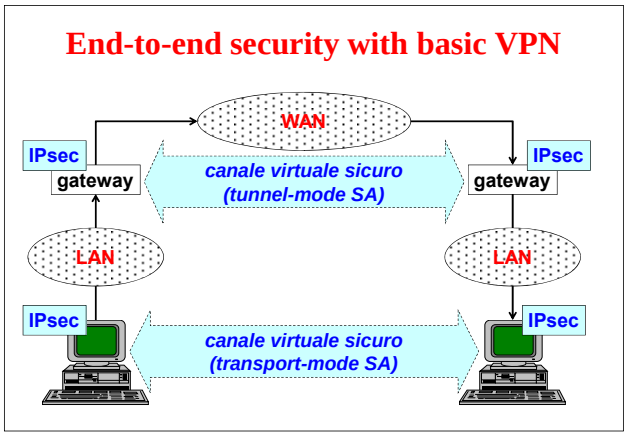
End-to-end security



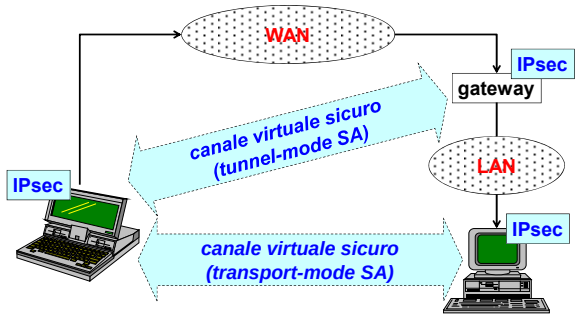
Basic VPN



End-to-end security with basic VPN



Secure remote access



Intrusion Detection System (IDS)

- **definizione:**
  - sistema per identificare individui che usano un computer o una rete senza autorizzazione
  - esteso anche all'identificazione di utenti autorizzati, ma che violano i loro privilegi
- **ipotesi:**
  - il comportamento degli utenti non autorizzati si differenzia da quello degli utenti autorizzati

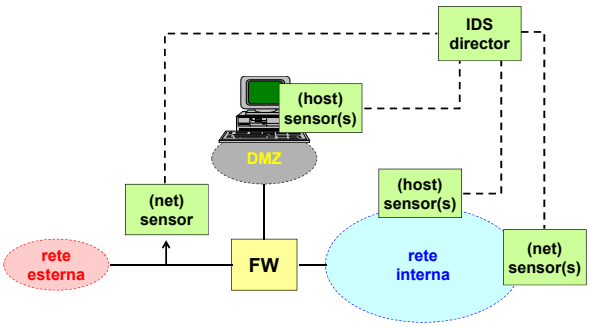
IDS: caratteristiche funzionali

- **IDS passivi:**
  - uso di checksum crittografiche
  - riconoscimento di pattern ("attack signature")
- **IDS attivi:**
  - "learning" = analisi statistica del funzionamento del sistema
  - "monitoring" = analisi attiva di traffico dati, sequenze, azioni
  - "reaction" = confronto con parametri statistici (reazione scatta al superamento di una soglia)

IDS: caratteristiche topologiche

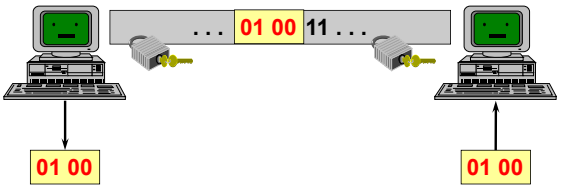
- **HIDS (Host-based IDS)**
  - analisi dei log (del S.O. o delle applicazioni)
  - attivazione di strumenti di monitoraggio interni al S.O.
- **NIDS (Network-based IDS)**
  - attivazione di strumenti di monitoraggio del traffico di rete

Architettura di un IDS



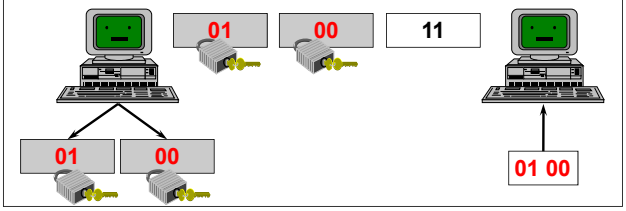
Sicurezza di canale

- **autenticazione (singola o mutua), integrità e segretezza solo durante il transito nel canale**
- **nessuna possibilità di non ripudio**
- **non richiede modifica alle applicazioni**

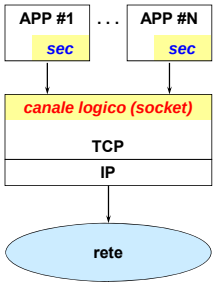


Sicurezza di messaggio (o dei dati)

- autenticazione (singola), integrità e segretezza auto-contenute nel messaggio
- possibilità di non ripudio
- richiede modifica alle applicazioni

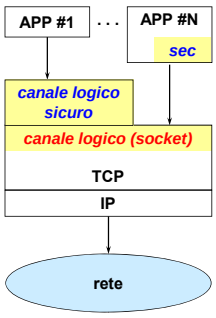


Sicurezza interna alle applicazioni



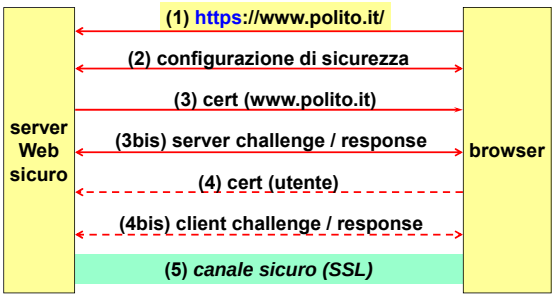
- ogni applicazione implementa la sicurezza al proprio interno
- la parte in comune si limita ai canali di comunicazione (socket)
- possibili errori di implementazione (inventare protocolli di sicurezza non è semplice!)
- non garantisce l'interoperabilità

Sicurezza esterna alle applicazioni



- il livello sessione sarebbe ideale per implementare molte funzioni di sicurezza
- … ma non esiste in TCP/IP!
- è stato proposto un livello "sessione sicura":
  - semplifica il lavoro degli sviluppatori applicativi
  - evita possibili errori di implementazione
  - a scelta dell'applicazione

SSL (Secure Socket Layer)



Autorizzazione / controllo accessi

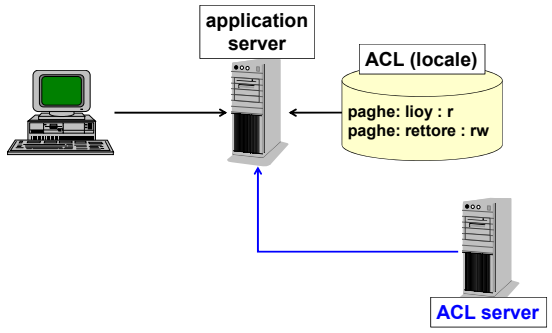
- **S = soggetto che desidera compiere un'azione**
- **O = oggetto dell'azione**
- **T = tipo di azione (access privilege)**
- **P = predicato (affermazione ausiliaria, es. ora)**
- **modello base per il controllo accessi:**

f : S x O x T x P → { vero, falso }

User-based authorization

- **S = utente del sistema**
- **controllo accessi tramite:**
  - ACL (Access Control List) impostate sugli oggetti
    - elenco di S x T x P permessi su un oggetto
  - Capability assegnate ai soggetti
    - elenco di O x T x P concessi ad un soggetto
- **difficilissima gestione in sistemi con molti utenti e/o molti oggetti**

Autorizzazione: ACL



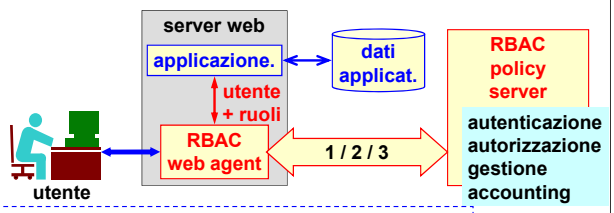
RBAC (Role-Based Access Control)

- **un framework concettuale per semplificare la gestione dei permessi di accesso**
  - permessi associati ai ruoli invece che agli utenti
  - ruoli associati agli utenti
- **ai ruoli possono essere:**
  - dati nuovi permessi quando si introducono in azienda nuove applicazioni o sistemi
  - tolti permessi quando cambiano le responsabilità
- **i ruoli sono più stabili perché le attività/funzioni in un'ente cambiano meno frequentemente rispetto alle persone che svolgono queste funzioni**

RBAC: estensioni

- **RBAC gerarchico**
  - se i ruoli sono organizzati gerarchicamente, allora chi possiede un ruolo possiede anche automaticamente tutti i ruoli inferiori (e quindi i relativi permessi)
  - es. direttore implica automaticamente capo-ufficio
- **RBAC con vincoli**
  - non tutti i permessi sono assegnabili perché esistono dei vincoli (constraint)
  - es. no manager ed auditor dello stesso servizio

RBAC: esempio con applicazione web



1. la risorsa è protetta?
   se si, richiedi le credenziali all'utente
2. l'utente è autenticato?
   se si, trovane i ruoli e verifica l'autorizzazione
3. l'utente è autorizzato?
   se si, concedi l'accesso alla risorsa

Sviluppo di applicazioni sicure

- **non implica necessariamente l'uso di tecniche di sicurezza (es. crittografia)**
- **richiede certamente:**
  - robustezza (es. prevedere tutti i possibili input)
  - comprensione dell'ambiente operativo (es. compatibilità con firewall e IDS)
  - integrazione coi meccanismi di sicurezza aziendali (es. I&AM)

Data recovery

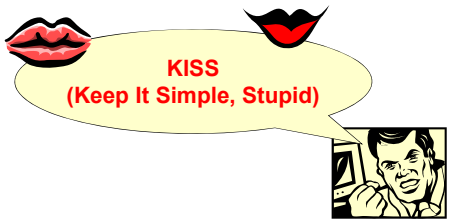
- **possibile recuperare i dati memorizzati su supporti magnetici dopo la loro cancellazione ed anche dopo la formattazione del disco**
- **programmi di recovery**
- **strumenti di recovery magnetico**
- **per cancellare veramente i dati:**
  - usare programmi di "secure erase"
  - riformattare il disco col comando ATA
  - distruggere fisicamente il disco

La complessità è nemica della sicurezza

PRIMO ASSIOMA DELL'INGEGNERIA
Più un sistema è complesso,
più è difficile verificarne la correttezza
(di implementazione, gestione, funzionamento)

- **esempio: il numero di bachi di un programma è proporzionale al numero di righe di codice**
- **la complessità degli attuali sistemi informativi gioca a favore degli attaccanti, che possono trovare soluzioni di attacco sempre più ingegnose e non previste**

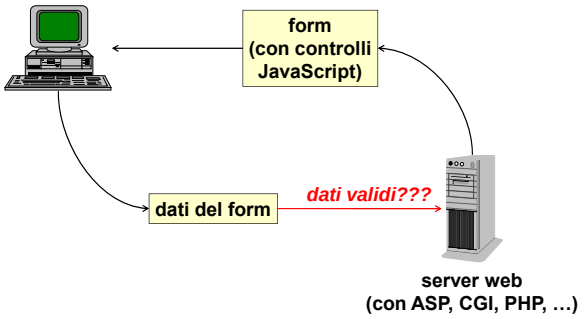
La regola del bacio



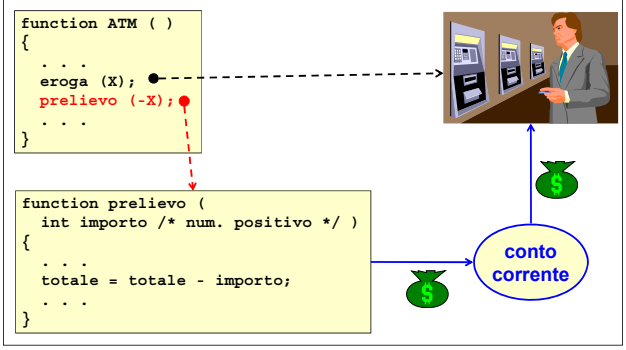
Duplicazione dei controlli (ovvero la cultura del sospetto)

- **è sempre meglio moltiplicare i controlli perché:**
  - possono fallire
  - possono essere aggirati
- **controlli da effettuare sul "perimetro":**
  - dell'applicazione
  - della rete
  - della libreria
  - del componente
  - …

Il sospetto: caso web



Il sospetto: programmazione tradizionale



Favorire il riuso

- fare sicurezza è un compito difficile
- se c'è qualcosa di disponibile e già provato è meglio usarlo

Combattere la sindrome NIH (Not Invented Here) che prima o poi colpisce qualunque tecnico

Usabilità

- **prestare molta attenzione agli aspetti usabilità**
- **soprattutto nei confronti dell'utente finale (può cambiare drasticamente il grado di accettabilità ed il livello risultante di sicurezza)**
- **considerare come esempio (negativo) il meccanismo di protezione delle chiavi private in Windows:**
  - basic (uso senza chiedere o segnalare niente)
  - medium (chiede il permesso ma non verifica l'identità)
  - high (chiede il permesso e verifica l'identità ad ogni singolo uso della chiave)

Costruire la sicurezza

- **tecnologia:**
  - indispensabile, ma da sola non basta
  - può essere mal progettata, configurata o gestita
- **addestramento:**
  - la sicurezza è un campo estremamente complesso ed in rapida evoluzione
  - addestramento generale e di prodotto
- **organizzazione:**
  - acquisire il background consolidato
  - definire le regole
  - … e soprattutto cosa capita in caso siano violate!

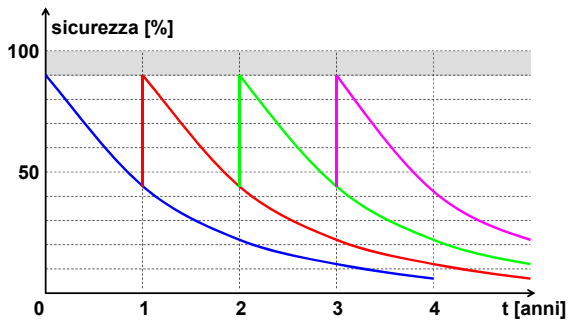
Spafford's first principle of security administration

If you have responsibility for security, but have no authority to set rules or punish violators, then your own role in the organization is to take the blame when something goes wrong.

Monitoraggio e revisioni

- **monitoraggio ordinario quotidiano**
- **revisioni periodiche programmate**
- **criticità:**
  - decine di nuovi attacchi scoperti ogni settimana
  - dare il tempo al personale di seguire gli sviluppi
  - necessità di reagire molto in fretta

Necessità di revisioni periodiche



Addestramento del personale

- **addestramento tecnico specifico:**
  - è più facile comprare hardware e software che non personale ben addestrato
  - ad ogni acquisto di un prodotto deve corrispondere un corso di formazione specifico su di esso
- **addestramento generale del personale:**
  - es. persona che ha cambiato 24 password per tornare a quella preferita
  - di chi è la responsabilità? (direzione sicurezza, altre direzioni, utenti finali)
- **checkpoint attivi (auto-hacking, ethical hacking)**

The 7 top-management errors that lead to computer security vulnerabilities (I)

- (n. 7) pretend the problem will go away if they ignore it
- (n. 6) authorize reactive, short-term fixes so problems re-emerge rapidly
- (n. 5) fail to realize how much money their information and organizational reputations are worth
- (n. 4) rely primarily on a firewall
- (n. 3) fail to deal with the operational aspects of security: make a few fixes and then not allow the follow through necessary to ensure the problems stay fixed

The 7 top-management errors that lead to computer security vulnerabilities (II)

- (n. 2) fail to understand the relationship of information security to the business problem - they understand physical security but do not see the consequences of poor information security
- (n. 1) assign untrained people to maintain security and provide neither the training nor the time to make it possible to do the job

As determined by the 1,850 computer security experts and managers meeting at the SANS99 and Federal Computer Security Conferences held in Baltimore May 7-14, 1999 (http://www.sans.org/resources/errors.php)

The 5 worst security mistakes end-users make

- (n. 1) failing to install anti-virus, keep its signatures up to date, and apply it to all files
- (n. 2) opening unsolicited e-mail attachments without verifying their source and checking their content first, or executing games or screen savers or other programs from untrusted sources
- (n. 3) failing to install security patches (especially for MS Office, MS IE/Outlook, and MS-Windows)
- (n. 4) not making (and testing!) backups
- (n. 5) using a modem while connected through a local area network

Agenda (III)

- introduzione alla sicurezza dei sistemi informatici
- organizzazione e tecnologie della sicurezza
- **risvolti legali:**
  - legge sulla protezione dei dati
  - legge sui crimini informatici
  - uso di Internet sul luogo di lavoro
- analisi costi-benefici

Leggi sulla protezione dei dati

- **legge 675/96 e DPR 318/99:**
  - misure minime
  - solo per dati sensibili
  - solo per reti "pubbliche"
- **TU 30/6/2003 sulla protezione dei dati personali:**
  - include anche i log (del traffico, dell'ubicazione, …)
  - generalizza (reti generiche) ed assegna responsabilità per le scelte effettuate
  - include personale esterno (tecnici, pulizia, …)
  - obbligatoria la formazione

T.U. protezione dati: responsabilità penale

- **il datore di lavoro può essere ritenuto in concorso con il dipendente a lui subordinato che ha commesso il crimine informatico se non ha posto in essere tutte le misure di prevenzione (a norma legge 547/93)**

mancata adozione di tutte le misure
=
agevolazione alla commissione del crimine

T.U. protezione dati: responsabilità civile

- **il trattamento dei dati è qualificato come attività pericolosa (art. 2050 c.c.)**
  - l'operatore è tenuto a fornire la prova di avere applicato le misure tecniche di sicurezza più idonee a garantire la sicurezza dei dati
- **responsabilità di padroni e committenti (art. 2049 c.c.)**
  - "padroni e committenti sono responsabili per i danni arrecati dal fatto illecito dei loro domestici e commessi nell'esercizio delle incombenze cui sono adibiti"

T.U. protezione dati: misure minime

- **le misure minime non necessariamente sono "idonee" o sufficienti:**
  - si è responsabili anche se si attuano le misure minime ma queste risultano inadeguate
- **normativa generale (e stabile) separata dai dettagli tecnici (e variabili):**
  - le misure minime variano nel tempo
  - allegato B del T.U.
  - aggiornamento periodico dell'allegato B (senza scadenza)

Allegato B: credenziali e password

- **trattamento dei dati solo da parte di persone autorizzate con "credenziali di autorizzazione"**
  - almeno identificativo + parola chiave
- **parola chiave:**
  - almeno 8 caratteri (o il massimo consentito se il sistema non ne permette 8)
  - NON deve contenere riferimenti all'incaricato
    - dictonary attack!
  - cambiata almeno ogni 6 mesi (3 per dati giudiziari)

Allegato B : credenziali e password

- **le "credenziali di autorizzazione" devono essere disattivate:**
  - dopo sei mesi di inattività
  - se non si possiede più il ruolo
- **non bisogna lasciare incustodita una sessione:**
  - screen saver con password
  - non allontanarsi dal PDL
- **possibile definire dei profili di autorizzazione:**
  - per ogni ruolo
  - deve esserne verificata la consistenza (almeno annualmente)

Allegato B: altre norme

- **controllo dell'ambito del trattamento per ogni singolo incaricato (annualmente)**
- **programmi anti-intrusione**
- **aggiornamento dei programmi (antivirus, patch, …) almeno annualmente**
  - per i dati sensibili almeno semestralmente
- **backup almeno settimanale**

Allegato B: documento programmatico

- **entro il 31/3 di ogni anno, con informazioni su:**
  - elenco dei trattamenti di dati personali
  - assegnazione di compiti e ruoli
  - analisi dei rischi che incombono sui dati
  - misure da adottare
  - backup e ripristino dati
  - formazione per gli incaricati
    - dal momento dell'ingresso in servizio
- **l'aggiornamento delle misure minime deve essere segnalato nella relazione accompagnatoria del bilancio d'esercizio (!)**

Legge 547/93 (crimini informatici)

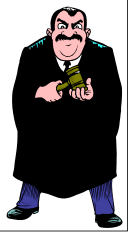
- **basata sull'inviolabilità del domicilio e dei segreti**
- **molti reati perseguibili solo su querela di parte**
- **sanziona ingresso, alterazione, cancellazione o soppressione ...**
- **... di dati o programmi informatici o qualsiasi altra ingerenza in un trattamento informatico**
- **frode informatica = per ottenere un vantaggio economico**
- **falso informatico = reato di falso se commesso su oggetto tradizionale**

Legge 547/93

- **danneggiamento**
- **sabotaggio**
- **accesso non autorizzato**
  - quale grado di affidabilità?
  - standard ufficiali?
  - basta una qualunque misura di sicurezza?
- **abusiva acquisizione di programmi**
- **detenzione e diffusione di virus**

Responsabilità oggettiva

- **il proprietario / fornitore / gestore di un sistema informativo deve controllare l'attività dei suoi utenti per segnalare alle autorità competenti violazioni di legge:**
  - pedofilia
  - scambio di materiale protetto dal diritto d'autore
  - …
- **possibile conflitto con la privacy**
- **garanzia dell'anonimato delle denunce (anche per evitare danno d'immagine)**



Agenda (IV)

- introduzione alla sicurezza dei sistemi informatici
- organizzazione e tecnologie della sicurezza
- risvolti legali
- **analisi costi-benefici:**
  - rischi e gestione dei rischi
  - costi e prestazioni

Rischi

monitoraggio + assicurazione

analisi costi - benefici

Rischi e gestione dei rischi

- **la sicurezza al 100% non esiste!**
- **occorre valutare e coprire il rischio residuo**
- **occorre accorgersi del danno**
  - il caso della videoteca di una TV
- **come minimo bisogna saper ripristinare l'oggetto ed i suoi dati:**
  - frequenza dei backup?
  - backup solo dei dati o dell'intero sistema?
- **analisi costi-benefici:**
  - costi per proteggere contro costi per ricostruire

Valutazione delle prestazioni

- **le prestazioni non dipendono dalla RAM ma dalla CPU e dalla sua cache**
- **le prestazioni non sono un problema sui client**
- **le prestazioni possono essere un problema sui server o sui nodi di rete (es. router):**
  - uso di acceleratori crittografici
  - acceleratori specifici (es. SSL, IPsec) o generici

Prestazioni (P4 @ 1.7 GHz)

	[64 B/packet]	[1024 B/packet]
hmac(md5)	31.5 MB/s	152.1 MB/s
des cbc	28.7 MB/s	28.9 MB/s
des ede3	10.8 MB/s	10.9 MB/s
aes-128	38.0 MB/s	37.8 MB/s
rc4-128	61.2 MB/s	62.0 MB/s
rsa 1024	133.7 firme/s	2472.1 verifiche/s

Conclusioni

- **la sicurezza non si compra … si progetta! (si comprano i componenti)**

- **la sicurezza non si aggiunge alla fine (come una ciliegina sulla torta) ma è uno dei requisiti base della specifica di un moderno sistema informativo**

- **la sicurezza non è una spesa ma … un risparmio!**

- **la sicurezza è un bersaglio … mobile!**