Sicurezza nelle reti

Sicurezza: molti significati

- Crittografia
- Autenticazione
- Integrità dei messaggi
- Certificazione e distribuzione delle chiavi
- Altro?

Alcuni esempi:

- applicazioni: e-mail sicure, e-business
- trasporto: SSL, SET
- network: IP security
- Operational security: firewall, intrusion detection

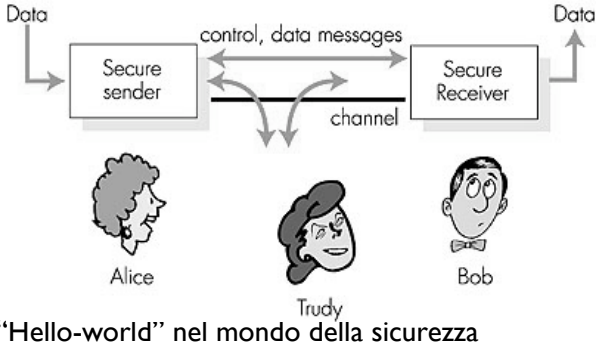
Sicurezza

- Sicurezza non si caratterizza in modo semplice
  - Valori (non facili da determinare)
  - Determinare la presenza di attacchi (non sempre è possibile)
  - Affrontare e risolvere gli attacchi (a volte in tempo reale)

Ingegneria del Software e Sicurezza

- Sistemi Software
  - Specifica (che cosa fa)
  - Implementazione (come lo fa)
  - Correttezza (cosa effettivamente fa)
- Sicurezza dei sistemi software
  - Specifica: politica
  - Implementazione: meccanismi
  - Correttezza: assurance

Alice, Bob, e … Trudy



- "Hello-world" nel mondo della sicurezza
- Bob e Alice hanno la necessità di comunicare tra loro in modo sicuro
- Trudy, "intruder" è in grado di intercettare e modificare i messaggi

Alice, Bob … nel mondo reale

- Web browser/server nel caso di applicazioni di e-commerce (pagamenti on-line)
- on-line banking
- DNS server
- routers che si scambiamo informazioni sullo loro routing table (OSPF)

Chi sono i cattivi?

D: Cosa puo' fare un "cattivo" digitale?

R:una valanga di cose (dal sito CERT)

- *eavesdrop:* intercept messages
- actively *insert* messages into connection
- *impersonation:* can fake (spoof) source address in packet (or any field in packet)
- *hijacking:* "take over" ongoing connection by removing sender or receiver, inserting himself in place
- *denial of service*: prevent service from being used by others (by overloading resources)

Proprietà: CIA

Confidentiality - Secrecy -- segretezza: solo il sender ed il receiver designato dovrebbero essere in grado di comprendere il contenuto di un msg

- Sender: cifra (encrypt) il msg
- Receiver: decifra (decrypt) il msg

Message Integrity – integrità del messaggio: sendere receiver vogliono avere la sicurezza che il contenuto del msg non sia stato alterato

Authentication -- autenticazione: sender e receiver sono in grado di confermare l'identità dell'altra componente coinvolta nella comunicazione

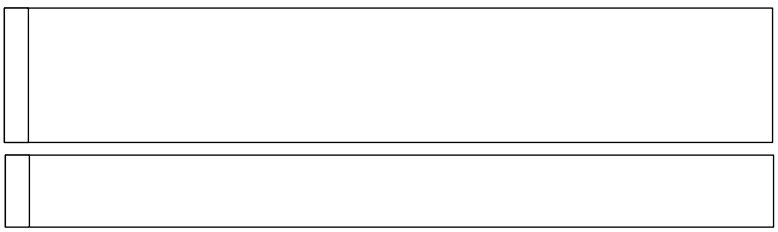
Politica di sicurezza

- Insieme di proprietà di sicurezza = politica di sicurezza
- Esempio: una banca on line
  - Autenticazione dei clienti
  - Segretezza dei dati dei clienti e di tutti ali altri dati interni al sistema
  - Integrità del sistema di interazione
  - Ma anche "non repudiation" delle transazioni e altre proprietà

Politiche

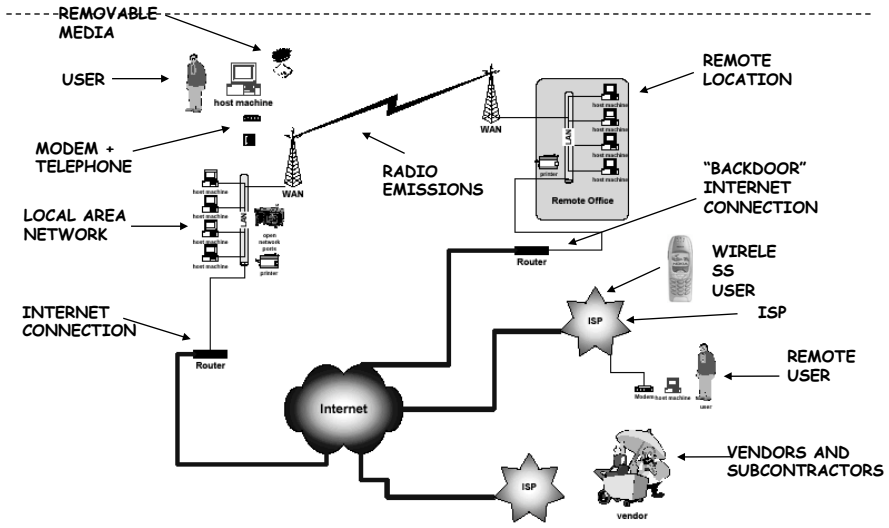
- Non esiste una unica nozione di sicurezza che si applica in tutte le situazioni
  - Sistemi differenti richiedono politiche di sicurezza differenti
  - Le capacità di interazione con l'ambiente possono portare a politiche di sicurezza tra loro in conflitto (e.g. non repudiation e deniability)

Sicurezza e Internet

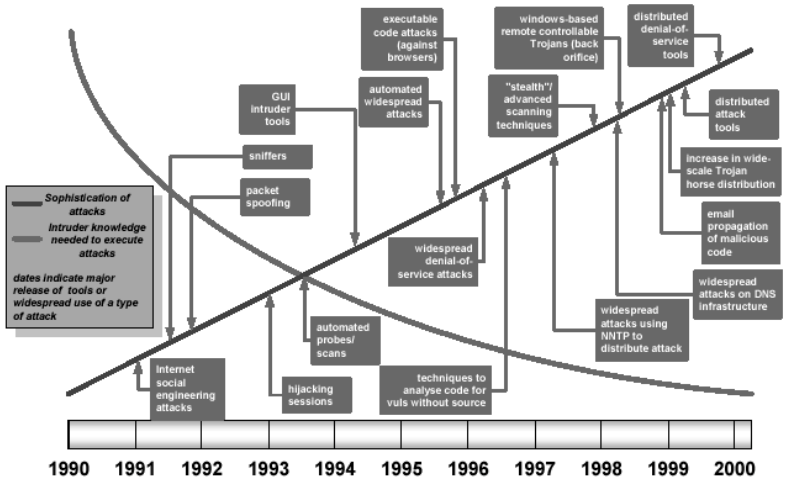


Sicurezza delle applicazioni di rete

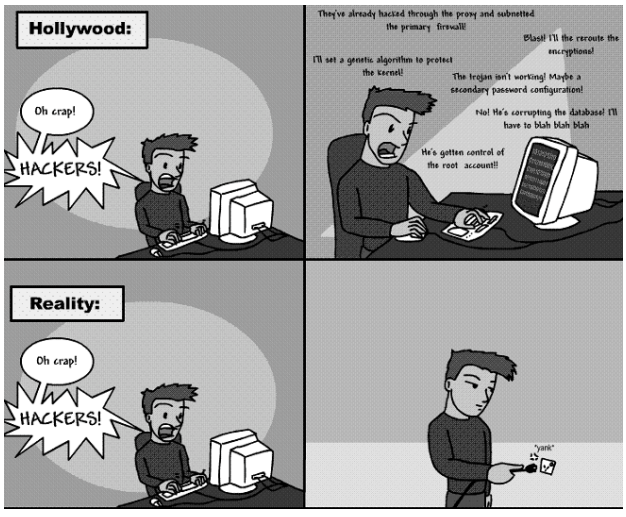
- I sistemi software (pre-internet) erano isolati.
  - Amministratore gestiva tutti i programmi e gli aggiornamenti
  - Entita' eseguibili, i programmi, erano poche e bene identificate.
  - Accesso "fisico" ai sistemi
- Internet …. Una rivoluzione
  - Software e' aggiornato costantemente spesso anche di nascosto dall'utente.
  - Cosa fanno i programmi presenti sul sistema? Boh!!
  - La distanza fisica non e'un problema: un hacker in australia e' il vostro vicino piu' prossimo.
  - Ogni cosa e' eseguibile (i.e., pagine web, email, mms, …).
  - Dipendiamo costantemente dalla infrastruttura di rete.



Solo hackers??



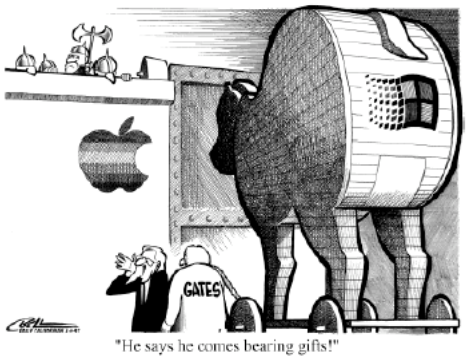
Fonte: CERT (Computer Emergency Response Team)



Trends

- Sofware innovativo
  - Codice mobile (contenuti eseguibili)
  - Indipendente dalla piattaforma
  - Estendibile dinamicamente
- Fantastico!!! (anche per gli hackers)
  - Write (an attack once) and run everywhere …
  - Sistemi sono vulnerabili: attacchi non facilmente predicibili

Mobile Trojan Horses



"He says he comes bearing gifts!"

Attacchi innovativi

- Applet attack: programmi eseguibili all'interno browser web
- ActiveX Controls: componenti che attaccano il sistema via OS
  - Accesso ai dati
- Dispositivi mobili con codice mobile
- Mobile networks

L'Internet Security Threat Report di Symantec rivela che l'Italia è al t...cted": Cagliari, Roma e Milano le città in cui il fenomeno è più diffuso 13-05-2008 21:46

symantec. Confidence in a connected world.

Italia | Acquisti | Cerca

Norton | Aziende | Partner | Negozio on-line | Informazioni su Symantec

Benvenuti | Profilo aziendale | Notizie e media | Relazioni con gli investitori | Analisti di settore | Offerte di lavoro

Notizie
Risorse per i media
Contatti PR

Symantec.com > Informazioni su Symantec > Notizie e media > Notizie > Comunicati stampa

Notizie

L'Internet Security Threat Report di Symantec rivela che l'Italia è al terzo posto in Europa per numero di computer "bot infected": Cagliari, Roma e Milano le città in cui il fenomeno è più diffuso

La nuova edizione del Report evidenzia la formazione di una vera e propria "economia sommersa": i criminali informatici comprano, vendono e scambiano le informazioni personali sottratte e usano i siti Web più visitati per lanciare gli attacchi

Cupertino, Calif. – 08 aprile 2008 – L'Italia è al terzo posto in Europa per numero di computer "bot infected", ossia computer nei quali i criminali informatici si sono insinuati per assumerne il controllo e usarli come "ponte" per lanciare attacchi informatici di vario tipo. Cagliari, Roma e Milano, le città più colpite, si collocano rispettivamente al 3°, 6° e 8° posto tra le dieci città europee che presentano il maggio numero di computer infettati.

Sono alcuni dei dati che emergono dall'ultima edizione dell'Internet Security Threat Report (ISTR), Volume XIII, presentata da Symantec Corp. (Nasdaq: SYMC). Il Report giunge alla conclusione che oggi il Web rappresenta il principale veicolo per condurre attività di attacco e che gli utenti online sono sempre più esposti a contagio semplicemente cliccando e collegandosi ai siti Web tradizionalmente visitati tutti i giorni. Lo studio raccoglie i dati provenienti da milioni di sensori Internet, ricerche e monitoraggio attivo delle comunicazioni degli hacker, fornendo una panoramica globale dello stato attuale della sicurezza Internet.

In passato accadeva che per "diventare una vittima" di un attacco l'utente dovesse visitare intenzionalmente un sito illegale o cliccare coscientemente su un allegato pericoloso. Oggi non è più così: gli hacker riescono a compromettere siti Web leciti e ad utilizzarli come mezzi per la diffusione di attacchi a computer aziendali e privati. Symantec ha evidenziato come i cyber-criminali prediligano i siti che infondono maggiore fiducia negli utenti, come ad esempio quelli di social networking.

Gli hacker fanno, inoltre, leva sulle vulnerabilità di un sito specifico che possono essere sfruttate per sferrare altri attacchi. Negli ultimi sei mesi del 2007 sono state rilevate 11.253 vulnerabilità di siti specifici di scripting multi-sito; si tratta di vulnerabilità presenti solo in singoli siti Web. Ciò nonostante, per sole 473 (circa il 4%) di queste vulnerabilità sono state messe a punto delle patch da parte degli amministratori IT dei siti colpiti, offrendo così agli hacker una notevole finestra di opportunità.

In maniera analoga, il phishing continua a rappresentare un problema. Nell'ultimo semestre del 2007 Symantec ha rilevato 87.963 host di phishing – computer che possono ospitare uno o più siti Web preposti a tecniche di phishing – segnando in tal modo un incremento del 167% rispetto alla prima metà dell'anno. L'80% dei brand presi di mira da fenomeni di phishing durante il periodo in oggetto appartengono al settore finanziario.

Dal report è emerso anche che i cyber-criminali sono sempre più alla ricerca di informazioni confidenziali da utilizzare poi per scopi fraudolenti a fini di profitto, anziché focalizzarsi sui computer o sui dispositivi che contengono tali dati. Negli ultimi sei mesi del 2007 il 68% delle maggiori minacce riportate da Symantec era costituito da tentativi di sottrazione di dati sensibili.

Infine, gli hacker comprano, vendono e scambiano le informazioni violate avvalendosi di un mercato sommerso ben consolidato. Un commercio che assume sempre più le sembianze delle economie tradizionali. Ad esempio, la legge della domanda e dell'offerta ha un impatto diretto sulla definizione del prezzo. Le informazioni relative a carte di credito si sono aggiudicate il secondo posto in

In ginocchio l'internet italiana tutta colpa dei virus sui computer – Scienza & Tecnologia – Repubblica.it 12/13/2006 09:28 AM

Repubblica.it L'Espresso Kataweb
XL Dweb mixjab Quotidiani Espresso Trovacinema
DEEJAY Capital m2o Repubblica TV All Music Fantacalcio

la Repubblica.it

Cerca
Web
Immagini
Video
News
Annunci
Shopping
Repubblica.it

Cerca
Pagine Gialle
Pagine Bianche
Mappe

Ultimo aggiornamento **mercoledì 13.12.2006 ore 09.10**

SCIENZA & TECNOLOGIA

Da alcuni giorni irraggiungibili alcuni siti, si naviga a singhiozzo
Interessati i principali operatori. Ecco perché accade. Come agire

In ginocchio l'internet italiana tutta colpa dei virus sui computer

È la Telecom mette a disposizione il numero 19122 per l'assistenza
di *ALESSANDRO LONGO*

ROMA - L'internet italiana è in ginocchio: sono giorni di malcontento, di proteste che affollano forum e gruppi di discussione. Problemi a navigare sui siti, pagine che non si aprono o lo fanno dopo minuti di attesa. Decine di tentativi prima di inviare una e-mail. Il tutto sembra avvenire ovunque in Italia e con i principali operatori. "È vero, ma non è colpa nostra: la causa è un'epidemia di malware, spyware e adware che sta colpendo i server Dns di tutti gli operatori", dicono da Telecom Italia. Tradotto: molti utenti hanno computer infetti da file cattivi, parenti dei virus informatici: spyware e adware, appunto. File che generano traffico all'insaputa degli stessi utenti, aprendo connessioni con altri computer, inviando e-mail. Lo fanno di solito a scopi di marketing, per monitorare le abitudini di navigazione degli utenti o per inondarli di pubblicità. In questo moto, intasano con un surplus di richieste i server Dns degli operatori.

I Dns sono come le rubriche telefoniche del web. I computer le consultano ogni volta che l'utente digita l'indirizzo di un sito web su un browser o usa un altro servizio internet basato su un nome a dominio, come la posta elettronica. I Dns danno al computer la direzione giusta per raggiungere il computer che può fornire quel servizio, in base al nome a dominio digitato (per esempio si raggiunge così il computer dove è collocato il sito web richiesto). Ma se ci sono troppi computer che vogliono consultare queste rubriche, perché manipolati da spyware e adware, è ovvio che il traffico sul web diventa come sulle autostrade durante l'esodo di agosto: a niente, a passo d'uomo o proprio bloccato.

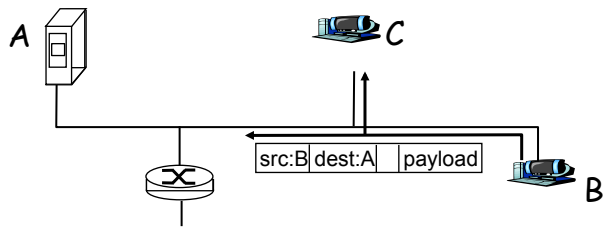
Per citare solo le proteste di ieri e di oggi: "E' il quarto giorno che l'Adsl è collassata. Per mandare un e-mail occorrono 20 tentativi e tutto il resto è fermo come un sasso. Il problema interessa un intero Paese e perfino le banche hanno problemi con le linee dati", scrive su un gruppo di discussione un utente umbro. "Da qualche giorno fatico a navigare, due volte su tre non apre le pagine e anche la posta ha problemi", aggiunge Andrea S. "Sembra un problema nazionale perché ho lo stesso a Napoli", conferma un utente che si firma Samanta. "Da un paio di giorni ho enormi problemi con la connessione... a volte lentissima, a volte non apre neppure i siti più comuni (Google)", scrive un utente da Genova.

La cosa sta dando parecchio fastidio, quindi, a utenti e aziende. "Siamo già intervenuti con contromisure sui nostri server, ma potrebbero esserci ancora problemi in alcune zone", dicono da Telecom. È ancora allarme, quindi, tanto che Telecom ha reso disponibile un numero di assistenza tecnico dedicato: 19122.

▷ 1

Packet sniffing:

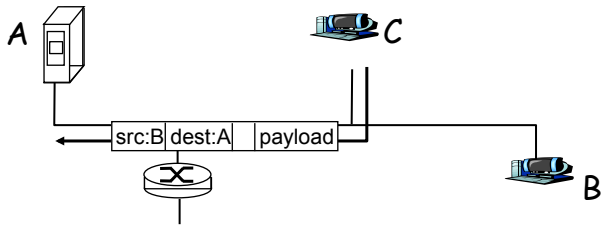
- LAN di tipo broadcast
- Le schede di rete sono in grado di leggere tutti i pacchetti inviati sulla LAN ed in particolare tutti i dati "in chiaro" (e.g. passwords)



▷ 20

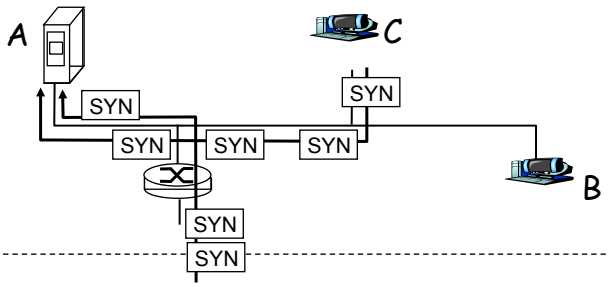
IP Spoofing:

- Un utente non educato potrebbe generare pacchetti IP con un valoro qualsiasi dei campi previsti dalla struttura di IP
- e.g.: C si fa passare per B



Denial of service (DOS):

- Creazione di un carico di lavoro elevato tale che il sistema non è in grado di funziuonare
- e.g., C: SYN-attack su A



Determinare i servizi attivi

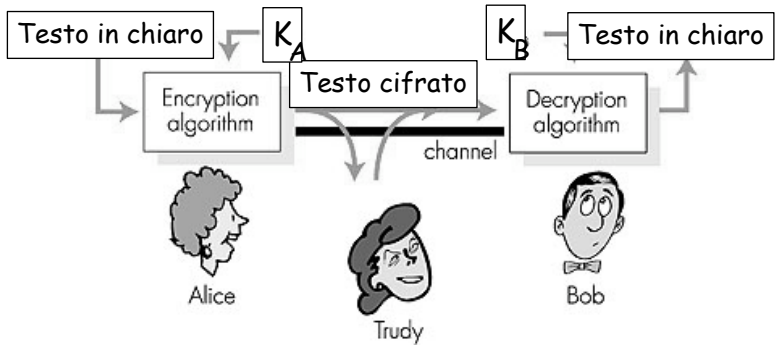
port	type	name	port	type	name
7	TCP/UDP	echo	513	UDP	who
9	TCP/UDP	discard	514	UDP	syslog
13	TCP/UDP	daytime	517	UDP	talk
19	TCP/UDP	chargen	2049	TCP/UDP	NFS
21	TCP	ftp ◯	512	TCP	exec ◯
23	TCP	telnet ◯	513	TCP	login ◯
37	TCP/UDP	time	514	TCP	shell ◯
53	TCP/UDP	domain			
69	UDP	tftp			
110	TCP	pop3 ◯			
113	TCP/UDP	auth			
161	UDP	snmp			

services marked with ◯
use cleartext passwords

Il gergo della sicurezza

- Principali
  - Utente
  - Sistema
  - Servizio
- La nozione di principale dipende dal livello di astrazione
  - Indirizzo IP
  - Gli host delle sottorete IP
  - Le persone che utilizzano gli host

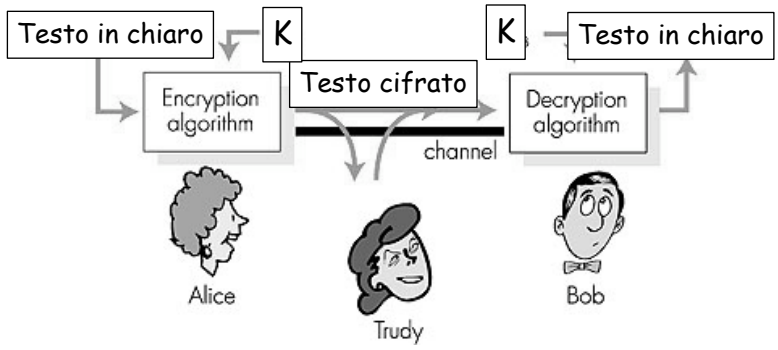
Crittografia



Chiave simmetrica: le chiave del sender e del receiver sono identiche

Chiave pubblica: chiave di cifratura: *public*, chiave di decifratura:*secret*

Crittografia: chiave simmetrica



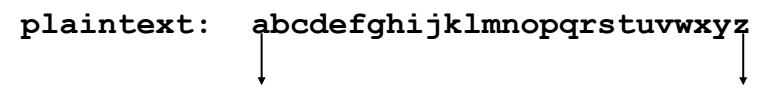
A: E(K,M) = C

B: D(K,C) = M

Chiave simmetrica

Alfabeto di cifratura: sostituzione di caratteri secondo uno schema

- monoalfabetico: sostituzione di un carattere per un altro



E.g.: `Plaintext: bob. i love you. alice`

`ciphertext: nkn. s gktc wky. mgsbc`

Algoritmo DES

DES: Data Encryption Standard

- Standard [NIST 1993]
- Chiave simmetrica a 54 bit
- Testo in chiaro 64 bit
- Cosa si ottiene?
  - Decifrare è computazionalmente costoso

AES
Advanced Encryption Standard

- new (Nov. 2001) symmetric-key NIST standard, replacing DES
- processes data in 128 bit blocks
- 128, 192, or 256 bit keys
- brute force decryption (try each key) taking 1 sec on DES, takes 149 trillion years for AES

Crittografia a chiave pubblica

Chiave simmetrica

- Sender e receiver devono conoscere la chiave
- Come si fa in rete ad incontrarsi?

Chiave Pubblica

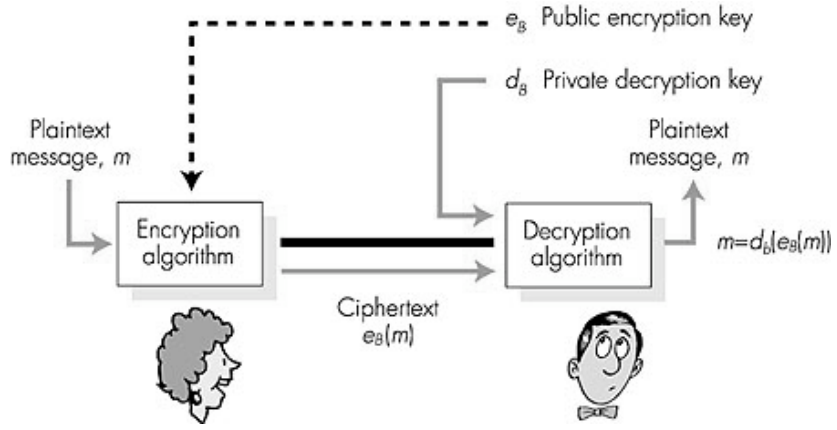
Sender e receiver non condividono alcun segreto

encryption key: *public*

decryption key: private

[Diffie-Hellman76, RSA78]

Public key cryptography



Public key encryption algorithms

Requirements:

1. Public&private keys

$$K_B^-(K_B^+(m)) = m$$

2. given public key K_B^+, it should be impossible to compute private key

RSA: Rivest, Shamir, Adelson algorithm

RSA

$$\underbrace{K_B^-(K_B^+(m))}_{\text{use public key first, followed by private key}} = m = \underbrace{K_B^+(K_B^-(m))}_{\text{use private key first, followed by public key}}$$

Result is the same!

Funzioni Hash

- Funzioni di cifratura H che hanno la caratteristica
  - Dal punto di vista computazionale e' difficile trovare due messaggi m e m' tali che H(m) = H(m')

Codice di autenticazione

- Sender
  - Calcola H(m)
  - Cre il messaggio (m, H(m))
- Receiver
  - Riceve (m, h)
  - If H(m) = h then OK

Problema

- Intruder
  - Intruder si fa passare per il sender
  - Invia (m', H(m'))
  - …

Soluzione

- Sender
  - Calcolo H(m+s) dove s e' il codice di autenticazione
  - Invia (m, H(m+s))
- Receiver
  - Riceve (m, h)
  - If H(m+s) = h then OK

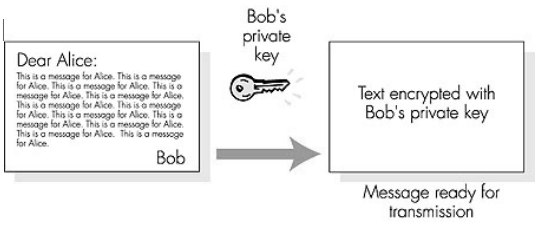
Firma digitale

Tecniche di crittografia = generazione della firma digitale

- Sender firma in modo digitale un documento.
- Verificabile: receiver deve essere in grado di verificare che solamente il sender ha firmato.

Esempio:

- Bob cifra m con la sua chiave privata d_B, ottenendo il msg $d_B(m)$.
- Bob invia ad Alice m e $d_B(m)$



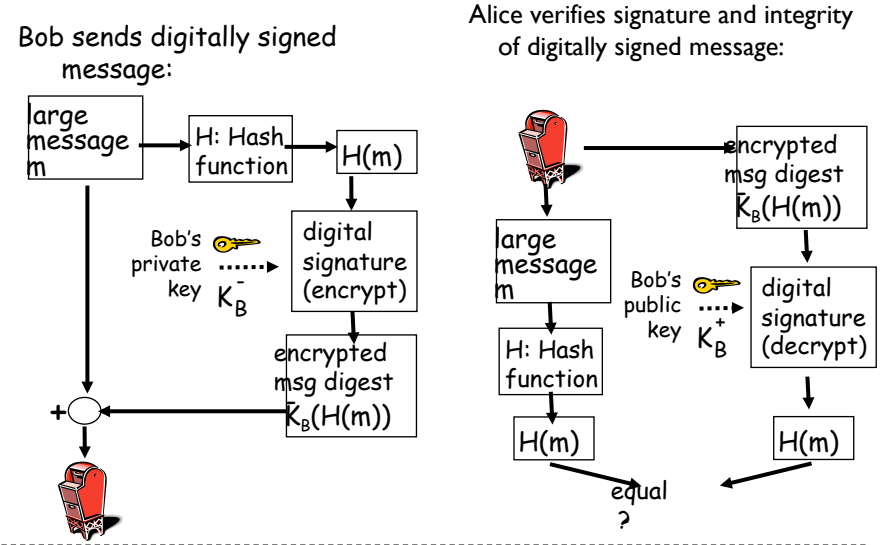
Firma digitale

- Alice verifica la firma di Bob tramite la chiave pubblica
- Se $e_B(d_B(m)) = m$, allora Bob ha firmato con la sua chiave privata.

Non-repudiation:

- Alice può provare che Bob ha effettivamente firmato

Digital signature = signed message digest



Hash Function Algorithms

- MD5 hash function (RFC 1321)
  - computes 128-bit message digest in 4-step process.
  - arbitrary 128-bit string x, appears difficult to construct msg m whose MD5 hash is equal to x.
- SHA-1
  - US standard [NIST, FIPS PUB 180-1]
  - 160-bit message digest

Intermediazione Trusted

Symmetric key problem:

- How do two entities establish shared secret key over network?

Solution:

- trusted key distribution center (KDC) acting as intermediary between entities

Public key problem:

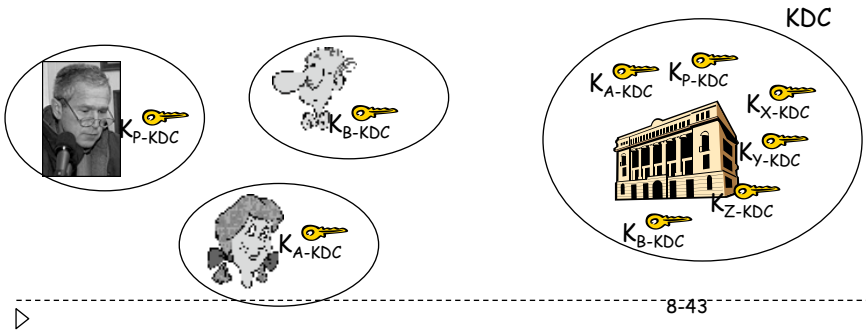
- When Alice obtains Bob's public key (from web site, e-mail, diskette), how does she know it is Bob's public key, not Trudy's?

Solution:

- trusted certification authority (CA)

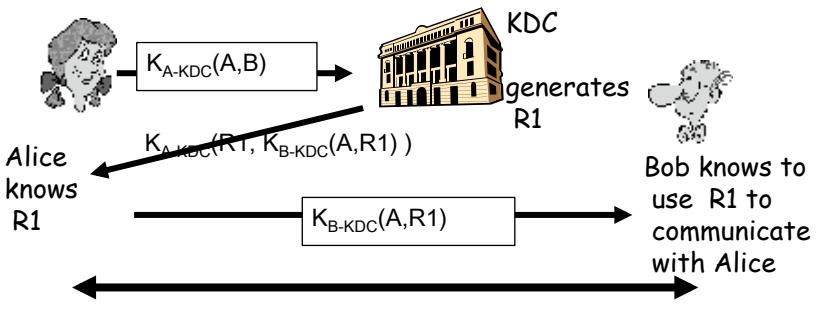
Key Distribution Center (KDC)

- Alice, Bob need shared symmetric key.
- KDC: server shares different secret key with *each* registered user (many users)
- Alice, Bob know own symmetric keys, $K_{A\text{-}KDC}$ $K_{B\text{-}KDC}$, for communicating with KDC.



Key Distribution Center (KDC)

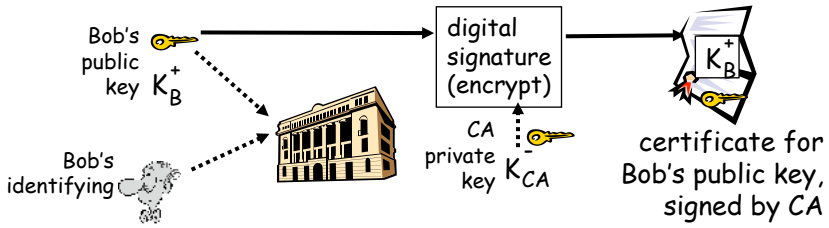
How does KDC allow Bob, Alice to determine shared symmetric secret key to communicate with each other?



Alice and Bob communicate: using R1 as *session key* for shared symmetric encryption

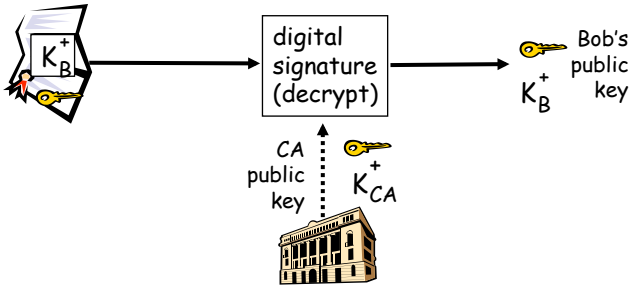
Certification Authorities

- Certification authority (CA): binds public key to particular entity, E.
- E (person, router) registers its public key with CA.
  - E provides "proof of identity" to CA.
  - CA creates certificate binding E to its public key.
  - certificate containing E's public key digitally signed by CA – CA says "this is E's public key"



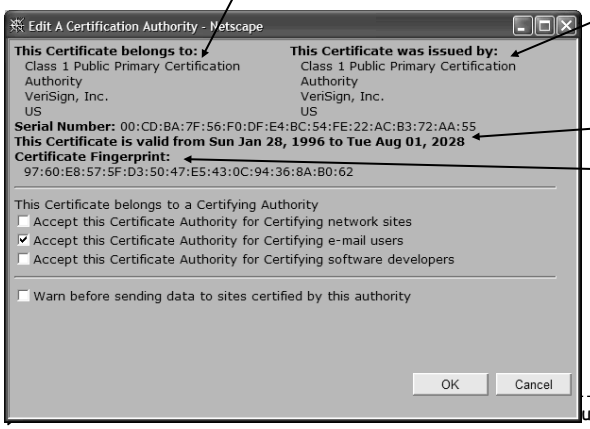
Certification Authorities

- When Alice wants Bob's public key:
  - gets Bob's certificate (Bob or elsewhere).
  - apply CA's public key to Bob's certificate, get Bob's public key



A certificate contains:

- Serial number (unique to issuer)
- info about certificate owner, including algorithm and key value itself (not shown)



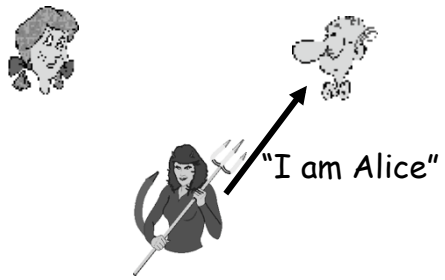
- info about certificate issuer
- valid dates
- digital signature by issuer

urity

Authentication

Goal: Bob wants Alice to "prove" her identity to him

Protocol ap1.0: Alice says "I am Alice"



in a network,
Bob can not "see"
Alice, so Trudy simply
declares
herself to be Alice

48

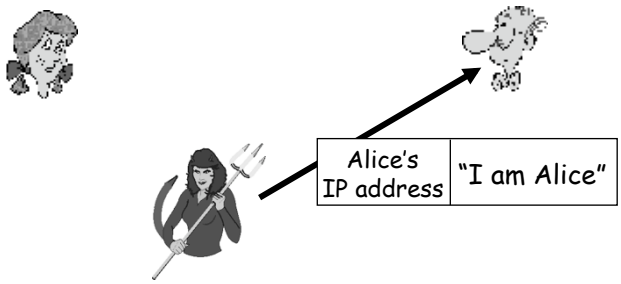
Authentication: another try

Protocol ap2.0: Alice says "I am Alice" in an IP packet containing her source IP address

Failure scenario??

Authentication: another try

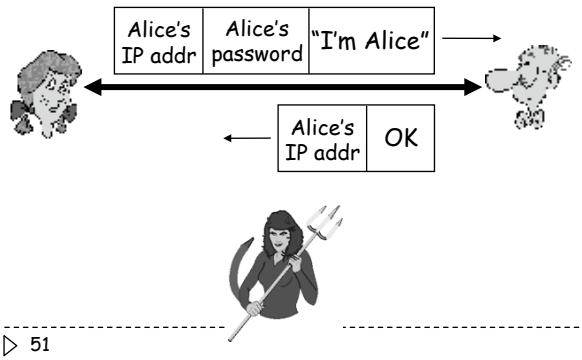
Protocol ap2.0: Alice says "I am Alice" in an IP packet containing her source IP address



Trudy can create a packet "spoofing" Alice's address

Authentication:

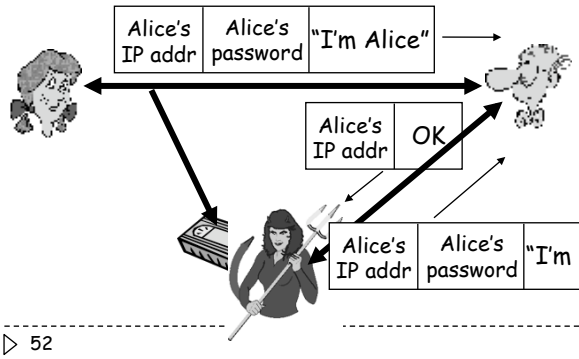
Protocol ap3.0: Alice says "I am Alice" and sends her secret password to "prove" it.



Failure scenario??

Authentication: another try

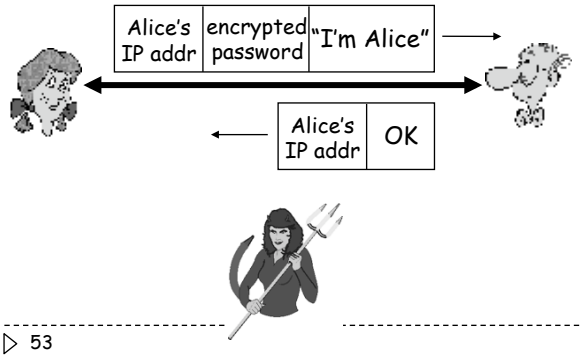
Protocol ap3.0: Alice says "I am Alice" and sends her secret password to "prove" it.



playback attack: Trudy records Alice's packet and later plays it back to Bob

Authentication: yet another try

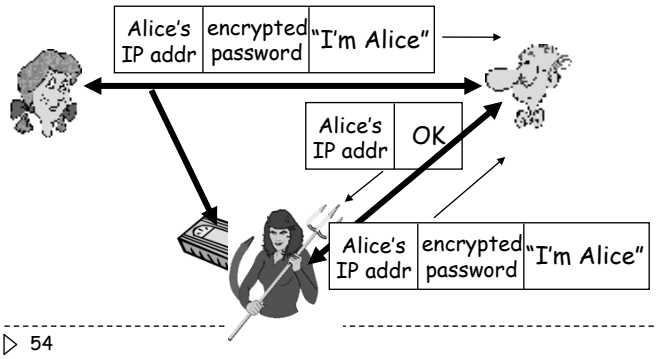
Protocol ap3.1: Alice says "I am Alice" and sends her *encrypted* secret password to "prove" it.



Failure scenario??

Authentication: another try

Protocol ap3.1: Alice says "I am Alice" and sends her *encrypted* secret password to "prove" it.



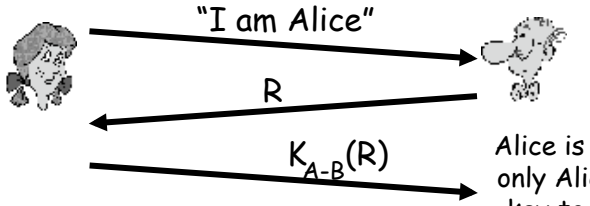
record and playback still works!

Authentication

Goal: avoid playback attack

Nonce: number (R) used only *once –in-a-lifetime*

ap4.0: to prove Alice "live", Bob sends Alice nonce, R. Alice must return R, encrypted with shared secret key



Alice is live, and only Alice knows key to encrypt nonce, so it must be Alice!

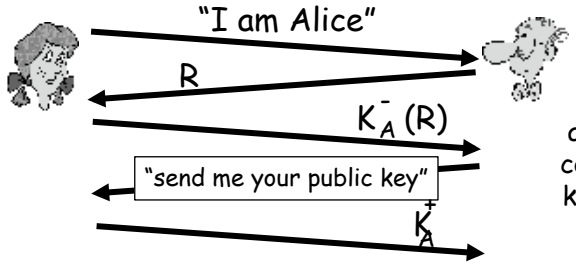
Failures, drawbacks?

Authentication: ap5.0

ap4.0 requires shared symmetric key

- can we authenticate using public key techniques?

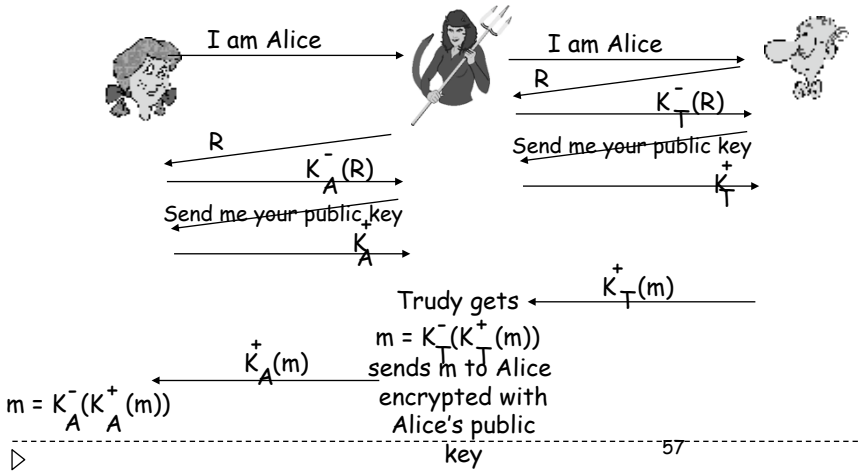
ap5.0: use nonce, public key cryptography



Bob computes $K_A^+(K_A^-(R)) = R$ and knows only Alice could have the private key, that encrypted R such that $K_A^+(K_A^-(R)) = R$

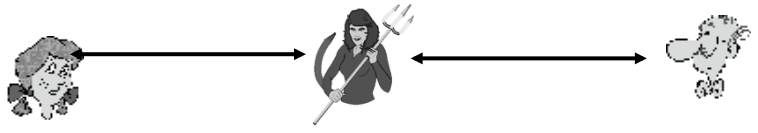
ap5.0: security hole

Man (woman) in the middle attack: Trudy poses as Alice (to Bob) and as Bob (to Alice)



ap5.0: security hole

Man (woman) in the middle attack: Trudy poses as Alice (to Bob) and as Bob (to Alice)

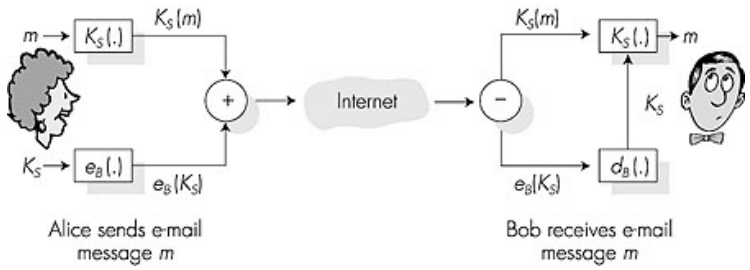


Difficult to detect:

- Bob receives everything that Alice sends, and vice versa. (e.g., so Bob, Alice can meet one week later and recall conversation)
- problem is that Trudy receives all messages as well!

e-mail sicure

- Alice vuole inviare una mail sicura a Bob.



- genera una chiave simmetrica K_S.
- cifra il messaggio con K_S
- cifra K_S con la chiave pubblica di Bob.
- invia a Bob $K_S(m)$ e $e_B(K_S)$.

Pretty good privacy (PGP)

- Standard per la cifratura di e-mail.
- Basato su chiavi pubbliche, simmetriche, firma digitale, funzioni hash.

Messaggio Cifrato:

```
---BEGIN PGP SIGNED
  MESSAGE---
Hash: SHA1

Bob:My husband is out of
  town tonight.Passionately
  yours, Alice

---BEGIN PGP SIGNATURE---
Version: PGP 5.0
Charset: noconv
yhHJRHhGJGhgg/12EpJ
  +lo8gE4vB3mqJhFEvZP9t6n7G
  6m5Gw2
---END PGP SIGNATURE---
```

IPsec: Network Layer Security

- Network-layer secrecy:
  - Il sender cifra i dati inviati
    - TCP - UDP segments;
    - ICMP messages.
- Network-layer authentication
  - Host di destinazione e' in grado di autenticare il mittente
- Due protocollo:
  - authentication header (AH) protocol
  - encapsulation security payload (ESP) protocol
- AH and ESP, richiedono esplicitamente una fase di handshake:
  - Si crea un canale logico sicuro a livello network denominato security association (SA)
- SA unidirezionale.
- SA determina in modo univoco:
  - security protocol (AH or ESP)
  - source IP address
  - 32-bit connection ID

Security Association

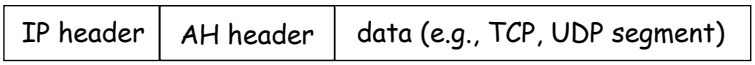
- Specifica i meccanismi di cifratura (chiavi, mac, hashing)
- Security parameter (SPI)
- Definito
  - Manualmente
  - Automaticamente (IKE)
- Database delle politiche
  - Identifica la coppia mittente destinatorio via SPI

Authentication Header (AH) Protocol

- Caratteristiche
  - source authentication,
  - data integrity,
  - no confidentiality
- AH header inserito tra IP header, data field.
- protocol field: 51
- Router intermedi fanno il loro lavoro

AH header:

- identificatore connessione
- authentication data: calcolato a partire dal datagram IP originario.
- next header field: type of data (e.g., TCP, UDP, ICMP)



ESP Protocol

- Caratteristiche
  - secrecy,
  - host authentication,
  - data integrity.
- data, ESP trailer cifrati.
- next header field is in ESP trailer.
- ESP authentication field = AH authentication field.
- Protocol = 50.