Metodologie Informatiche Applicate al Turismo

4. Aspetti di sicurezza nell reti

Paolo Milazzo

Dipartimento di Informatica, Università di Pisa
http://www.di.unipi.it/~milazzo/
milazzo@di.unipi.it

Corso di Laurea in Scienze del Turismo
A.A. 2012/2013

Importanza della sicurezza nelle reti (1)

- Gli aspeti di sicurezza giocano un ruolo chiave nelle reti di computer
- Sulle reti (tanto sulle reti locali che su Internet) vengono memorizzati e scambiati continuamente dati personali più o meno confidenziali
  - Messaggi privati (email, instant message, ecc....)
  - Dati sensibili (orientamento sessuale, religioso, ecc...)
  - Informazioni riservate o segrete (dati carta di credito, pin, ecc...)
- Inoltre tramite le reti si realizzano transazioni commerciali
  - Compravendita di beni e servizi (e-commerce, aste online, prenotazioni alberghiere, ecc...)

Importanza della sicurezza nelle reti (2)

- I messaggi che viaggiano sulla rete possono essere facilmente intercettati
  - Facile nel caso delle reti broadcast (es. molte reti locali e reti wireless)
  - Gli intermediari dei messaggi (server di posta elettronica, server web, ...) possono subire attacchi di “pirati informatici” (hackers)
- Sulla rete è facile spacciarsi per un’altra persona
  - Impersonificando un’altra persona si possono ottenere dati privati di quella persona

Attacchi alla sicurezza

- Un attacco alla sicurezza di un sistema informatico o una rete di computer è un'attività svolta da un soggetto (attacker, attaccante o avversario) volta a carpire, modificare o sfruttare informazioni riservate
  - Carpire: lo scopo è ottenere l'informazione senza modificare nulla (es. intercettazione messaggi privati)
  - Modificare: lo scopo è modificare l'informazione memorizzata (es. voto dell'esame)
  - Sfruttare: lo scopo è utilizzare un'informazione precedentemente carpita per trarre benefici (es. impersonificazione)

Attacchi alla sicurezza

- A seconda del tipo di attività che si svolge un attacco può essere passivo o attivo
  - Attacco passivo: l'attacker si limita ad osservare i messaggi scambiati sulla rete senza autorizzazione
  - Attacco attivo: l'attacker effettua operazioni che modificano i messaggi scambiati sulla rete o le informazioni memorizzate nei computer collegati
- Molte tecniche che consentono di proteggersi dagli attacchi si basano su crittografia (cifratura delle informazioni) che rendono i messaggi incomprensibili ai terzi

Attacchi alla sicurezza

Tipi di attacchi, dal più passivo al più attivo:

1. Analisi del traffico
2. Lettura del contenuto dei messaggi
3. Modifica dei messaggi
4. Cancellazione dei messaggi
5. Replicazione dei messaggi
6. Impersonificazione

Analisi del traffico

- I messaggi vengono scambiati tra mittente e destinatario, l'attaccante osserva (solo) il flusso dei messaggi
- I messaggi possono essere crittografati
- Un attacker (passivo) non decifra ne legge il contenuto dei messaggi, però viene a conoscenza di altre informazioni interessanti:
  - l'identità degli host comunicanti, la frequenza e la dimensione dei messaggi, ecc...

Lettura del contenuto dei messaggi

- Mittente e destinatario si scambiano messaggi in chiaro (non crittografati)
- Un attacker (passivo) viene a conoscenza del contenuto della comunicazione
- Terminologia: Sniffing dei messaggi

Modifica, cancellazione e replicazione dei messaggi

- Un utente utilizza un servizio in rete
- Invia una richiesta (esempio: richiesta effettuazione bonifico)
- L'attacker modifica porzioni del messaggio inviato (esempio: il codice IBAN del beneficiario)
- L'attacker fa sparire (cancella) il messaggio
- L'attacker lo invia nuovamente (replicazione) molte volte (esempio: il bonifico viene eseguito più volte)

Impersonificazione

- Un utente utilizza comunemente un servizio in rete (banca on-line, ad esempio)
- Un attacker (attivo) finge di essere un'entità (utente) diversa.
- Invia una sua richiesta come se fosse quella dell'utente originario
- Esempio: rispondendo a un email falsa un utente rivela la propria password per accedere a un servizio di home-banking. L'attacker può accedere così al conto "impersonificando" l'utente.

Elementi fondamentali di sicurezza dei sistemi informatici

Alcune proprietà o funzionalità che si vorrebbero poter garantire riguardo ai dati memorizzati e/o scambiati dai sistemi informatici sono:

- Confidenzialità (privacy, secrecy)
- Integrità dei dati
- Autenticazione
  - Identificazione
  - Provenienza dei messaggi
- Non-ripudio

Elementi fondamentali dei servizi di sicurezza (1)

- Autenticazione
  - Processo che permette di determinare l'identità dei partecipanti (nodo,persona, pacchetto IP) alla comunicazione con una "certa" sicurezza
  - L'autenticazione si basa sulla possibilità di dimostrare la conoscenza di un certo dato (es: password), o la proprietà di un certo oggetto (es: smartcard).

Elementi fondamentali dei servizi di sicurezza (2)

- Integrità
  - Proprietà che permette di garantire che non vengano effettuate modifiche non autorizzate dei dati
  - Si basa sul metodi di controllo degli accessi
    - Processo che permette di definire e controllare i diritti e i privilegi di accesso a risorse e servizi
    - Presuppone un meccanismo di autenticazione

Elementi fondamentali dei servizi di sicurezza (3)

- Confidenzialità
  - Proprietà che permette di garantire (con un certo margine di sicurezza) che l'accesso ai dati (sia in transito che memorizzati) sia consentito solo ad un ristretto numero di persone autorizzate
  - Presuppone l'esistenza di un meccanismo di autenticazione

Funzionalità fondamentali dei servizi di sicurezza (4)

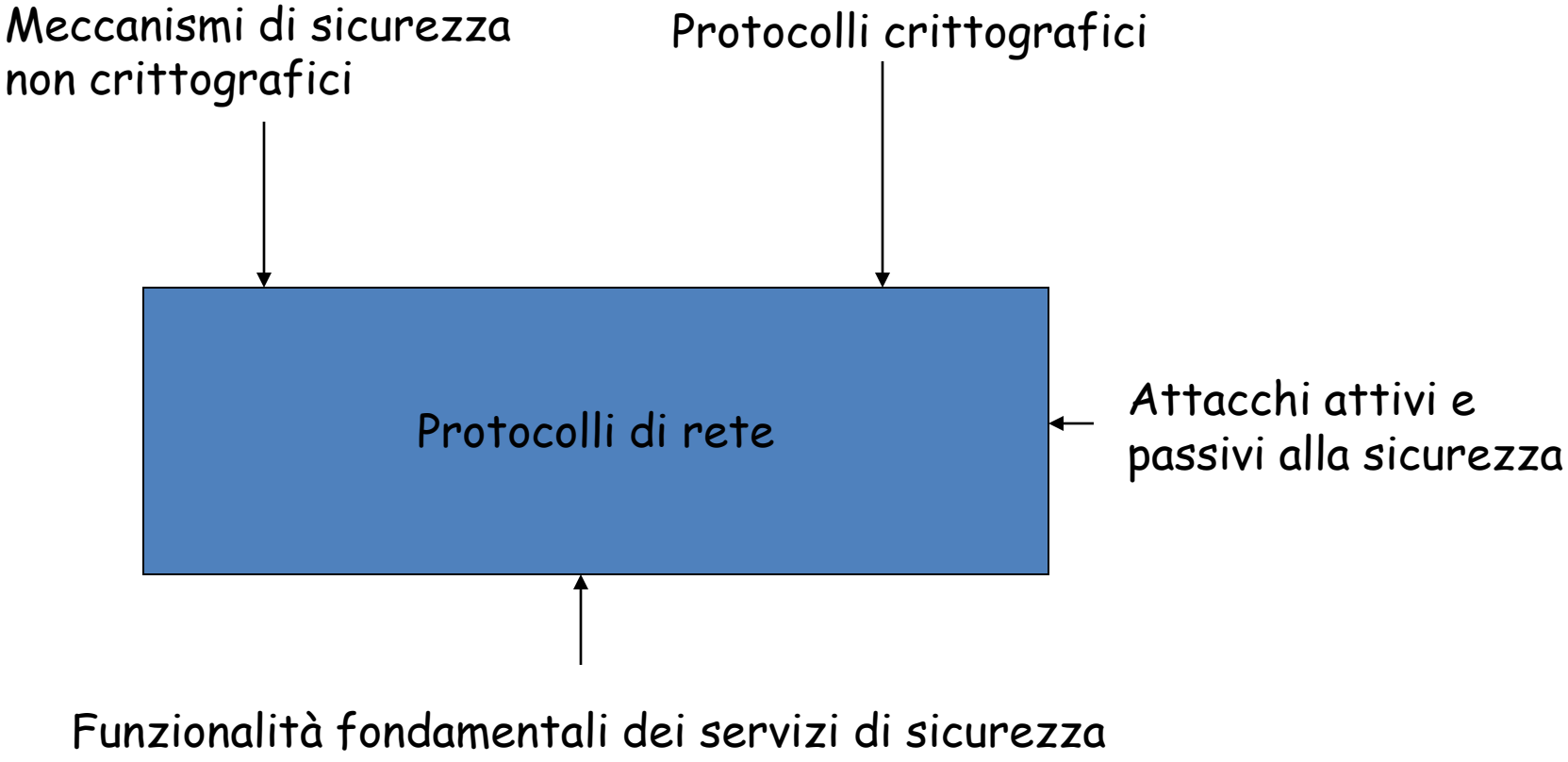
- Non ripudio
  - Proprietà che permette di assicurare che l'entità che ha generato i dati non possa in seguito negare di averlo fatto
  - Esempio: dopo aver sottoscritto un contratto tramite la rete (e.g. acquisto online) i contraenti non dovrebbero poter negare di averlo fatto

Sicurezza in ambito Web

- Rendere sicuri i canali (o i protocolli) di comunicazione
  - Come essere sicuri che informazioni critiche non vengano “sniffate”?
- Accertare l’identità dei server
  - Ci possiamo fidare che il server è chi dice di essere?
- Autenticazione dell’utente
  - Qual è il meccanismo offerto per identificare l’utente?
- Esecuzione controllata di applicazioni
  - L’esecuzione di programmi contenuti nei siti web all’interno del browser può danneggiare la mia macchina?

Problematiche della sicurezza

- I protocolli di rete devono occuparsi degli aspetti di sicurezza



Come fare a difendersi

- Meccanismi non crittografici (esempi)
  - Autenticazione debole (tramite indirizzo IP, ad esempio, cioè si riconosce il computer da cui partono i messaggi)
  - Controllo degli accessi mediante firewall: si bloccano (o filtrano) le connessioni in entrata ad un nodo della rete (tipicamente a livello TCP e/o applicazione)

Come fare a difendersi

- Una garanzia forte per le proprietà di autenticazione, confidenzialità, integrità e non ripudio si può avere tramite crittografia

Crittografia

- Crittologia:
  - scienza che ha lo scopo di studiare comunicazioni sicure
- Crittografia:
  - branca della crittologia che ha come scopo la progettazione di algoritmi di cifratura e decifratura, col fine di garantire la segretezza e l'autenticità dei messaggi.
  - Consiste nell'alterazione controllata di un messaggio (sequenza alfanumerica di caratteri) in maniera da renderlo non comprensibile a chi non dispone degli strumenti adeguati
  - La *crittografia* studia le **tecniche matematiche** relative alla sicurezza (confidenzialità, integrità dei dati, autenticazione e non-ripudio)
- Crittoanalsi:
  - branca della crittologia che ha come scopo l'analisi di messaggi cifrati per risalire all'informazione originaria, e/o la generazione di informazione cifrata contraffatta che possa essere accettata come autentica

Crittografia: terminologia di base

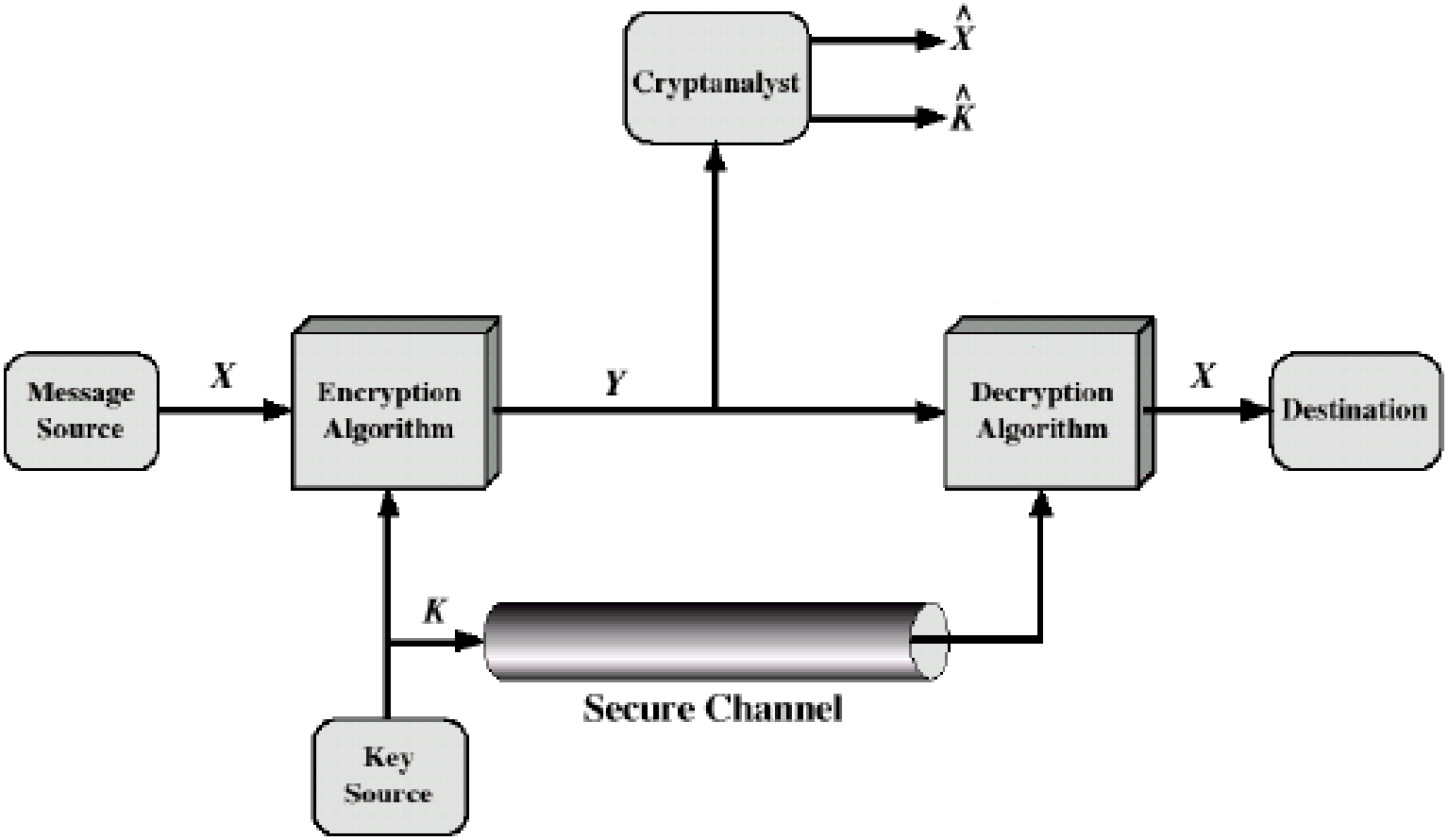
- Plaintext: messaggio originale
- Ciphertext: messaggio codificato
- Cipher (cifrario): algoritmo usato per trasformare il plaintext in ciphertext
- Key (chiave): informazione usata in cipher e nota solo a mittente e destinatario
- Encryption/Decryption: operazioni di codifica/decodifica

Crittografia

- Tipi di cifratura
  - Cifratura simmetrica (es. rotazione dell'alfabeto): la stessa chiave per cifrare e decifrare
  - Cifratura asimmetrica: chiave pubblica e chiave privata
    - Un messaggio cifrato usando la chiave pubblica si decifra (solo) con la chiave privata, e viceversa.
    - usata per messaggi segreti e per firma digitale
    - Messaggi segreti
      - Se A vuole inviare un messaggio segreto a B, usa la chiave pubblica di B. Solo B lo può leggere con la sua chiave privata
    - Firma digitale
      - A vuole dimostrare a B di essere veramente A. A firma il messaggio con la sua chiave privata; B può verificare la firma con la chiave pubblica di A.

Crittografia simmetrica

Modello di sistema crittografico tradizionale

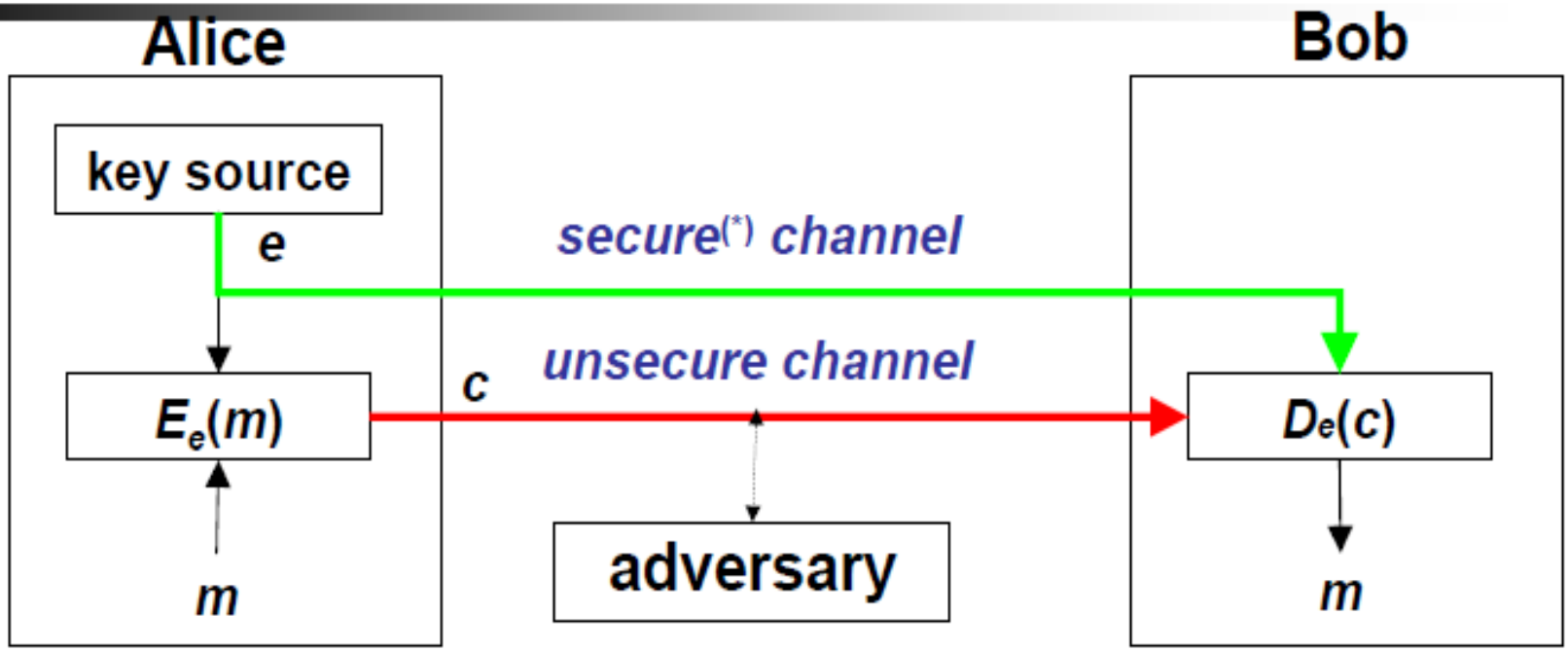


Crittografia simmetrica

- Siano E_e e D_e funzioni matematiche che rappresentano gli algoritmi di cifratura e decifratura usati con chiave *e*
- Siano $c = E_e(m)$ ed $m = D_e(c)$
- Il cipher simmetrico (E, D) è sicuro se e solo se:
  - Dato *c* è difficile determinare *m* senza conoscere *e*, e viceversa
  - Dati *c* e m è difficile determinare *e*

Come ci si accorda sulla chiave?

- La crittografia simmetrica consente di comunicare riservatamente usando un canale “insicuro” (ad esempio, Internet...)
- La prima cosa che devono fare mittente e destinatario è accordarsi sulla chiave
- Ma la chiave è un’infomazione riservata, quindi non possono usare lo stesso canale “insicuro” per accordarsi
- Serve un altro canale di comunicazione “sicuro” tramite cui scambiarsi la chiave... (ad esempio, la posta ordinaria...)



- Alice and Bob know ***E*** and ***D***
- Alice and Bob trust each other
- key ***e*** is a shared secret between Alice and Bob

(*) the channel is not ***physically*** accessible to the adversary and ensures both confidentiality and integrity

C’è una dose di fiducia

- Alice (Bob) confida che Bob (Alice) non rivelerà ***m***
- Alice (Bob) confida che Bob (Alice) terrà segreta la chiave ***e,*** cioè:
  - Alice (Bob) confida che Bob (Alice) sia competente nella gestione delle chiavi (key management)
  - Alice (Bob) confida che Bob (Alice) non riveli la chiave

Esempio di algoritmo crittografico (cifrario con shift)

Algoritmo: $X \leftarrow M+K \bmod 26$ $K=\{0,1,\ldots,25\}$

Testo in chiaro:	C	A	S	A
Testo cifrato:	R	P	H	P

Chiave: K = 15

- Ogni lettera è sostituita con la lettera che si trova K posizioni dopo nell'alfabeto inglese
- M è la posizione nell'afabeto della lettera in chiaro
- X è la posizione nell'afabeto della lettera cifrata

Esempio di algoritmo crittografico (cifrario con shift)

- Enigma, lo strumento di cifratura usato dai tedeschi nella seconda guerra mondiale per le comunicazioni tra sommergibili, si basava su una tecnica di cifratura con shift, ma con chiave variabile
  - ogni lettera del messaggio era cifrata con una chiave diversa
  - Impostata la chiave per la prima lettera le chiavi delle lettere successive venivano impostate automaticamente dalla macchina Enigma
- La “rottura” del codice di Enigma ha consentito agli inglesi di infliggere pesanti sconfitte ai tedeschi
- Alan Turing (matematico padre dell’Informatica) è stato il protagonista della rottura di Enigma

Algoritmi crittografici in Informatica

- Data Encryption Standard (DES): utilizza chiavi di 56 bit. Il messaggio da cifrare viene diviso in blocchi di 64 bit, ogniuno dei quali viene "mischiato" alla chiave tramite una funzione matematica complicata.
- Da anni è ritenuto poco sicuro per la ridotta dimensione della chiave. Servono al massimo 2^{56} tentativi (circa 72 milioni di miliardi) per provare tutte le chiavi (attacco brute force). Un supercomputer odierno ci mette poche ore.

Algoritmi crittografici in Informatica

- Triple DES (DES3): consiste nell'applicare l'algoritmo DES per 3 volte di seguito con chiavi diverse. Molto più sicuro di DES.
- Advanced Encryption Standard (AES): evoluzione di DES che può usare chiavi di 128, 192 o 256 bit. Molto più sicuro, si sta affermando come standard.

Crittografia asimmetrica

- Detta anche crittografia a chiave pubblica
- La chiave usata per cifrare è diversa dalla chiave usata per decifrare
- Le chiavi si usano in coppie di cui una è detta privata (segreta) e l'altra è detta pubblica (disponibile a tutti)
  - Ogni chiave privata ha la sua chiave pubblica (unica) e viceversa
  - Dedurre la chiave privata conoscendo quella pubblica è estremamente difficile
- Può richiedere una fase iniziale in cui gli interlocutori si scambiano le rispettive chiavi pubbliche
  - Problema: chi garantisce che chi fornisce la chiave pubblica sia veramente l'interlocutore con cui si vuole comunicare?
  - In situazioni critiche si utilizza una Public Key Infrastructure : autorità di certificazione terza e fidata che raccoglie le chiavi pubbliche certificando l'identità del proprietario

L’algoritmo RSA

- Il più noto algoritmo crittografico a chiave asimmetrica è l’algoritmo RSA (acronimo dei nomi degli inventori)
- Si basa sul fatto che la scomposizione in fattori primi di un numero molto grande è un problema complicato
  - Nel 2005 un gruppo di ricerca riuscì a scomporre un numero di 640 bit (193 cifre decimali) in due numeri primi, impiegando per cinque mesi un supercomputer con 80 processori da 2,2 GHz

L’algoritmo RSA

- Funzionamento (semplificato):
  - A deve mandare un messaggio segreto a B
  - B sceglie due numeri primi molto grandi (>300 cifre) e il moltiplica con il suo computer (impiegando meno di un secondo)
  - B invia il numero che ha ottenuto ad A. Chiunque può vedere questo numero (chiave pubblica)
  - A usa questo numero come chiave per cifrare il messaggio
  - A manda il messaggio cifrato a B. Chiunque può vederlo, ma non decifrarlo
  - B riceve il messaggio e utilizzando i due fattori primi che solo lui conosce (chiave privata) lo decifra

L’algoritmo RSA

- Sebbene siano abbastanza rapide, le operazioni di cifratura e decifratura dell’algoritmo RSA richiedono molto più tempo che le rispettive operazioni in algoritmi di crittografia simmetrica
- Nella pratica RSA viene spesso utilizzato per scambiarsi una chiave segreta da usare per comunicare tramite crittografia simmetrica
  - Così non si deve ricorrere a un canale diverso per lo scambio della chiave

Firma digitale

- Le tecniche di crittografia a chiave asimmetrica trovano applicazioni che vanno oltre la semplice comunicazione segreta
  - Firma digitale: si vuole fornire una prova di provenienza di un messaggio
  - E' un valido mezzo di autenticazione e per garantire il non repudio
- Un esempio di come funziona:
  - Alice invia un messaggio a Bob che lo deve restituire firmandolo con la propria chiave privata.
  - Alice può decifrare il messaggio ricevuto usando la chiave pubblica di Bob
  - Se funziona (riottiene il messaggio originale) ha parlato con Bob, perché solo lui possiede la chiave privata.

Firma digitale

- ***Bob non vuole inviare un messaggio segreto ad Alice, ma vuole fornirle una prova di provenienza***

- Solo chi ha la chiave privata può firmare un documento
- Tutti gli altri possono verificare la firma con la chiave pubblica

Attacchi alle comunicazioni crittografate

- Attacco a forza bruta (brute force):
  - si cerca di decifrare un messaggio usando tutte le chiavi possibili
  - per avere successo richiede in media di provare con la metà delle chiavi possibili
- Analisi crittografica
  - Si basa sulla natura dell'algoritmo e sfrutta qualche conoscenza delle caratteristiche generali del testo in chiaro e/o crittografato
  - Esempio: se si usa cifrario con shift (esempio sostituzione delle lettere dell'afabeto visto in precedenza) e si sa che il messaggio è scritto in italiano, avendo a disposizione un po' di messaggi cifrati si possono fare delle deduzioni sul contenuto dei messaggi originali

Dove la crittografia non aiuta

- Protezione di sistema
  - Accesso fisico (di persona) non autorizzato alle risorse hardware e software di sistema
  - Alterazione dei programmi (virus, ecc...)
- Protezione dei servizi
  - Attacchi mirati a rendere indisponibili i servizi , come gli attacchi Denial of Services (DoS) in cui si sovraccarica un servizio bombardandolo di richieste

Distribuzione delle chiavi nella crittografia asimmetrica

- Ma come si fa a procurarsi la chiave pubblica di una persona in maniera affidabile?
- Una chiave non può essere trasmessa in chiaro sulla rete perché la rete è insicura
- Possibili soluzioni
  - Faccia a faccia
  - Corriere fidato
  - Chiave in tanti pezzetti ed invio di ciascun pezzetto attraverso un diverso canale di comunicazione (telefono, email, piccione,…)
- Non sempre queste soluzioni sono possibili e/o economiche e/o efficienti
- Si vorrebbe utilizzare la rete per distribuire le chiavi

Distribuzione delle chiavi

- Ci vuole una Public Key Infrastructure.
- Di solito ci si affida:
  - ad una Trusted Third Party che ogni volta distribuisce le chiavi (ma può diventare un collo di bottiglia che rallenta la comunicazione)
  - oppure a una Certification authority (es. Verisign) che firma digitalmente le chiavi pubbliche che saranno poi distribuite dai proprietari
- Esempio: Protocollo HTTPs (web sicuro)
  - Usa SSL (Secure Socket Layer), un protocollo che fa uso di crittografia a chiave asimmetrica.
  - Il Web Server si identifica con un certificato (chiave pubblica firmata digitalmente da una certification authority) che si può accettare o meno

Certificati

- Vantaggi
  - Le certification authority non devono necessariamente memorizzare tutte le chiavi pubbliche
  - Le certification authority devono “lavorare” una volta sola per ogni chiave pubblica (al momento della firma)
- Svantaggi
  - Se la chiave privata della certification authority (usata per firma digitale) viene scoperta, tutte le comunicazioni diventano insicure (un attaccante può generare certificati falsi)

Certificati

- Un certificato ($Cert_A$) lega un nome (A) ad una chiave pubblica (K_{pubA})
- Lo firma digitalmente (garantisce) una Certification Authority (CA)
- B controlla l'autenticità di K_{pubA} in $Cert_A$ controllando la firma della CA sul certificato tramite K_{pubCA} della cui autenticità B è certo

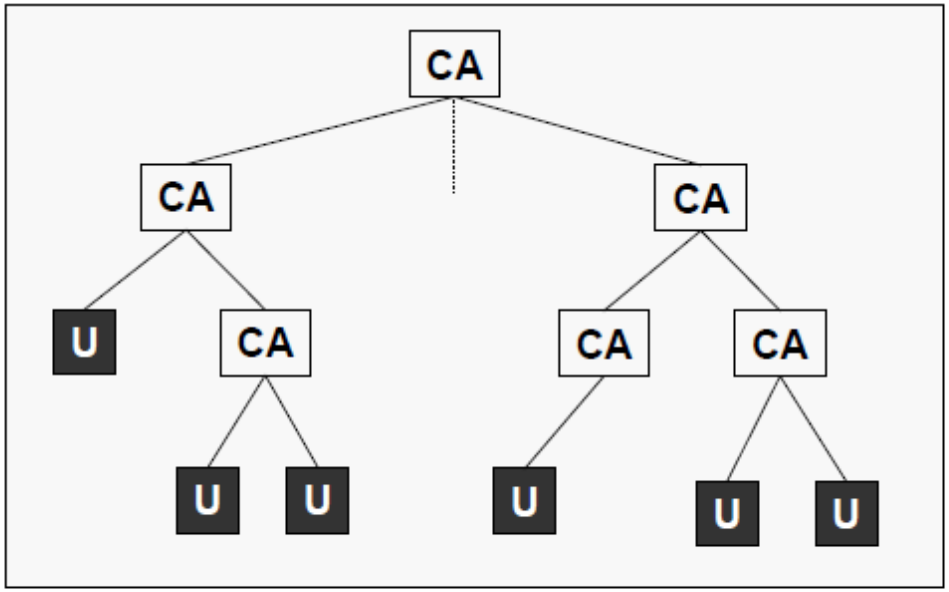
Uso del certificato

- Alice vuole sapere la chiave pubblica e_B di Bob
  - Alice verifica la firma della CA sul certificato e si convince che e_B è la chiave pubblica di Bob, ma..
  - Per verificare la firma sul certificato, Alice si deve procurare e_{CA}, la chiave pubblica di CA…
    - Come fa Alice ad essere sicura che e_{CA} è proprio la chiave pubblica di CA?
    - Chi rilascia un certificato alla CA
    - Dove si trova questo certificato?

Chi certifica la Certification authority?

- La chiave di CA è certificata da un'altra CA
  - un'altra chiave pubblica, un altro certificato e così via…
  - Certification Hierarchy (X.509)

Organizzazione gerarchica



CA = Certification Autority

U = User

SCALABILITÀ

DELEGA dell'AUTORITÀ e della FIDUCIA

In generale tra una CA e l'utente possono esserci una o più CA
I certificati delle CA in cima alla gerarchia (es Verisign) spesso sono già incluse nei sistemi operativi e/o browser

Come viene implementata la sicurezza nei protocolli di rete

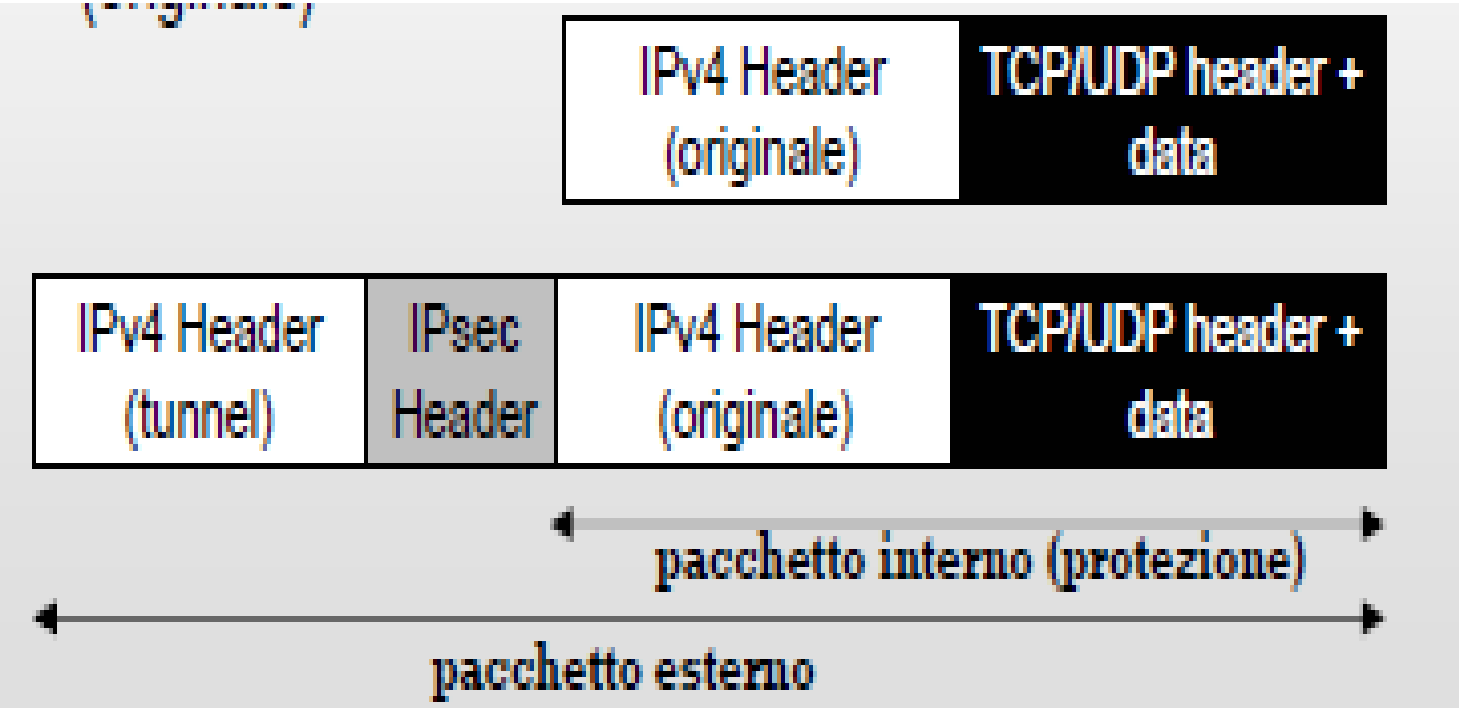
- Protocolli che forniscono servizi di sicurezza ad altri protocolli
  - IPSec (versione sicura di IP)
  - SSL (servizi di crittografia per le reti)
- Molti protocolli che finiscono con “s” funzionano come nel caso senza “s” e in più ricorrono a SSL per crittografare i propri messaggi
  - HTTPs
  - FTPs

IPSec

- IPSec è un meccanismo di sicurezza che opera al livello IP. Fornisce confidenzialità, integrità ed autenticità utilizzando algoritmi crittografici, in maniera trasparente per gli host e le reti che non lo supportano.
- IPSec opera inserendo delle strutture dati nei comuni pacchetti IP da proteggere per fornirgli i requisiti di sicurezza desiderati.
- IPSec opera secondo due modalità di funzionamento:
  - Modo Tunnel. Il pacchetto IP è incapsulato all'interno di un altro pacchetto. Questa modalità viene utilizzata solitamente da una coppia di gateway, situati nei punti di ingresso ed uscita di una rete non sicura
  - Modo Transport. In questo caso il pacchetto IP viene trasportato da un punto all'altro della rete senza subire modifiche. In sostanza quindi è il pacchetto originale che viene modificato, iniettandogli internamente le strutture dati per la sicurezza.

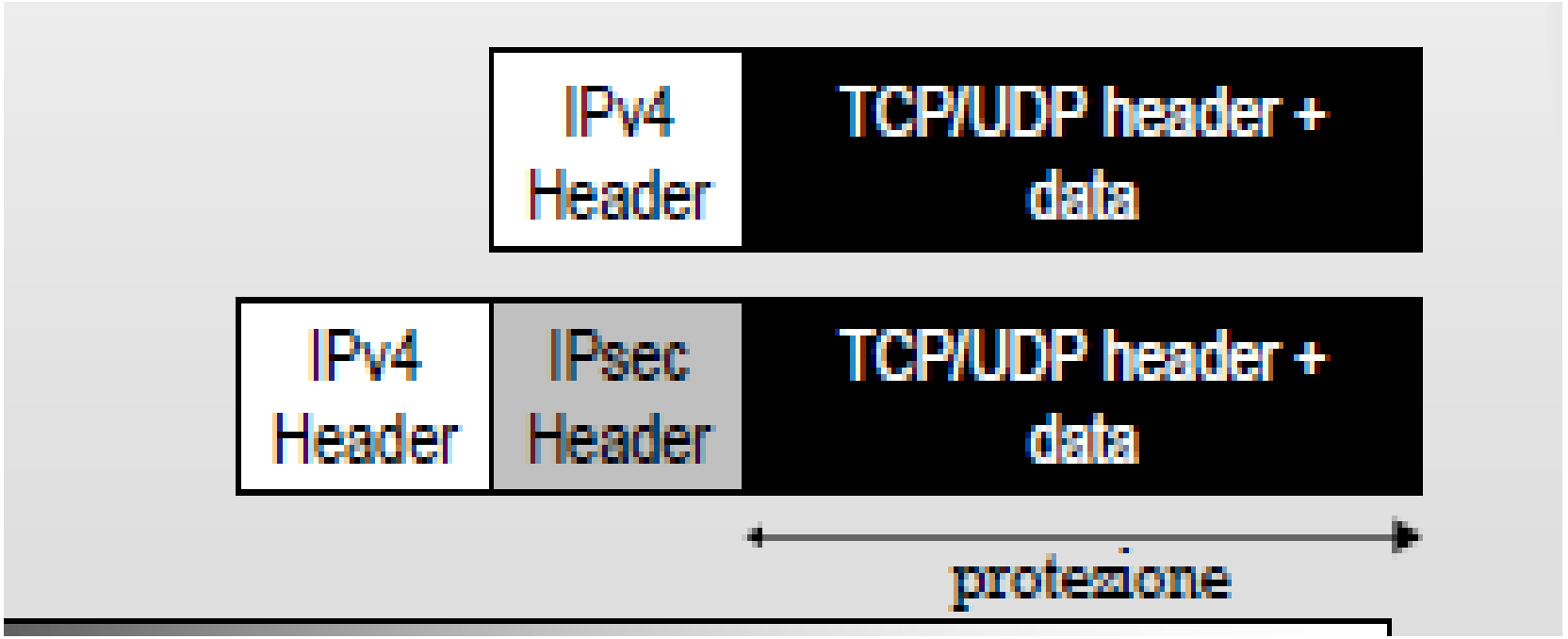
IPsec in modalità Tunnel

- Fornisce protezione (tramite crittografia) all'intero pacchetto IP (originale). Nessun intermediario può modificarlo
- Gli indirizzi IP di mittente e destinatario nell'header del pacchetto esterno possono essere diversi da quelli nell'header IP interno (originale)
  - Di solito sono due gli indirizzi di due router/gateway intermedi tra i quali si vuole costruire un "tunnel" sicuro


IPv4 Header (originale)
TCP/UDP header + data
IPv4 Header (tunnel)
IPsec Header
IPv4 Header (originale)
TCP/UDP header + data
pacchetto interno (protezione)
pacchetto esterno

IPsec in modalità trasporto

- Fornisce protezione ai pacchetti del livello trasporto (TCP, UDP..) contenuti nel pacchetto IP
- non modifica gli indirizzi nell'header IP (mittente e destinatario)
  - Sicurezza end-to-end (chi intercetta il messaggio non può utilizzarlo)
  - Non coinvolge i gateway (di fatto viaggia sulla rete un pacchetto IP indistinguibile dagli altri)


IPv4
Header
TCP/UDP header +
data
IPv4
Header
IPsec
Header
TCP/UDP header +
data
protezione

Secure Socket Layer (SSL)

- Secure Socket Layer (SSL) è un protocollo tra il livello di trasporto e quello applicativo che fornisce alcuni servizi di sicurezza appoggiandosi a TCP/IP in modo indipendente dall'applicazione.
- SSL fornisce: autenticazione dei due soggetti che comunicano (nello standard sono indicati come *peer*) basandosi su algoritmi di crittografia a chiave pubblica, confidenzialità del traffico (che viene automaticamente cifrato dopo lo stabilimento della connessione sicura), autenticità ed integrità del traffico.
- HTTPS è la versione di HTTP che usa SSL per garantire traffico sicuro sul web (siti di e-commerce)