REGIONE DEL VENETO

Direzione Sistema Informatico

Sun microsystems

Crittografia: una sfida e un'opportunità

Giuseppe Russo

Chief Technologist

Principal Engineer & Security Ambassador

Sun Microsystems, Inc.

Agenda

- Le sfide a cui è soggetta l'**Informazione** nell'*Era della Partecipazione*
- La **protezione** del bene Informazione
- La **crittografia** come opportunità
- Cosa è la crittografia e come si usa: *schemi, modelli, chiavi*

Le tecnologie e le onde del cambiamento

Il bagaglio minimo del viaggiatore

- **1995**

  Cash & Travel Cheques

  Biglietti Aereo

  Cabine ed uffici Telefonici

  Posta Ordinaria

- **2005**

  ATMs & carte di credito

  Biglietti Elettronici

  Telefoni cellulari & Voice over IP (es. Skype)

  E-mail & internet cafè

Evoluzione del Web

- **Web 1.0**

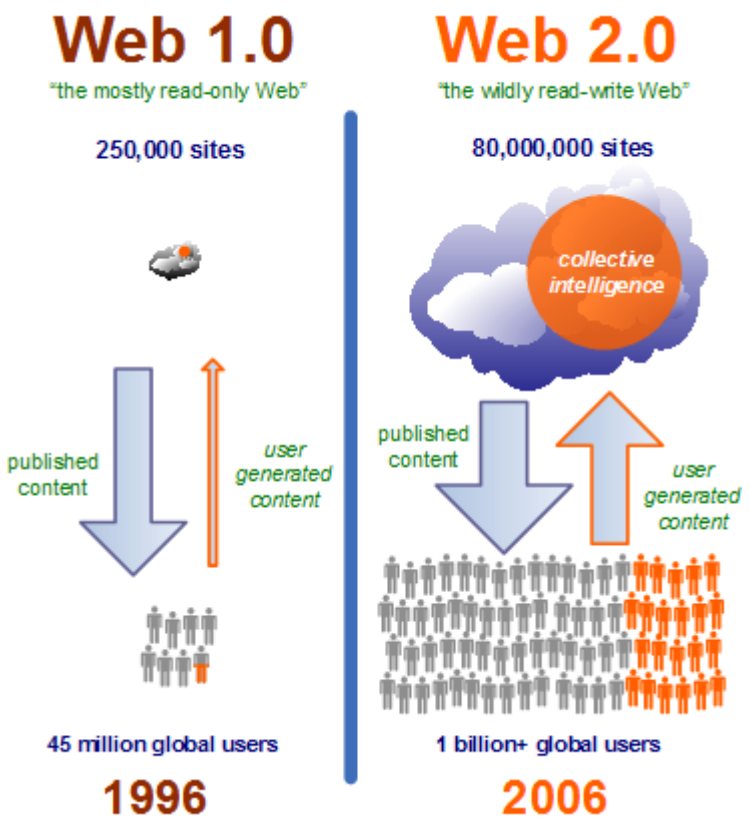
  Era una navigazione di tipo *read only*

  Pochi addetti ai lavori generavano i contenuti

- **Web 2.0**

  È un'approccio attivo di tipo *read-write*

  Grande partecipazione



L'epoca della Connettività Massima

- Una rapida evoluzione

  In poco più di dieci anni il mondo è diventato massivamente connesso

- Le attuali tecnologie promuovono sempre maggiore connettività

  proliferazione dei device, la crescita di banda trasmissiva, architetture informatiche orientate ai servizi ⇨ relazioni multi dimensionali

- Architetture Frattali

  Connessione di reti dinamiche da reti con sempre maggiore intelligenza

La nuova realtà: L'era della Partecipazione

Ognuno e Ogni Cosa capace di Partecipare alla Rete

Partecipazione = Opportunità e Rischi

Più di 5 Milioni Utenti / Settimana

Proliferazione di Device

Transazioni in continuo Aumento

Enorme traffico di Informazioni in Rete

Quale Sicurezza nell'Era della Partecipazione?

La Sicurezza coinvolge i diversi aspetti degli individui: *privacy, integrity, reliability, availability, etc*.

La Sicurezza è un aspetto chiave della Qualità

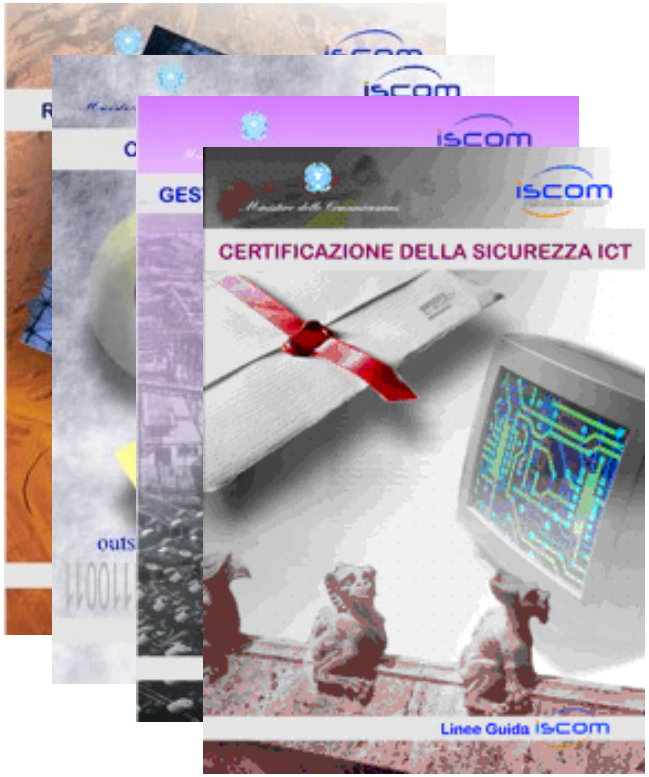
La Sicurezza abilita a relazioni sociali e commerciali fidate

In molti casi una omissione alla Sicurezza implica problemi legali:

DL196/2003, Misure Minime, Basilea 2, SOX, GLB, PATRIOT, HIPAA, SB1386, etc

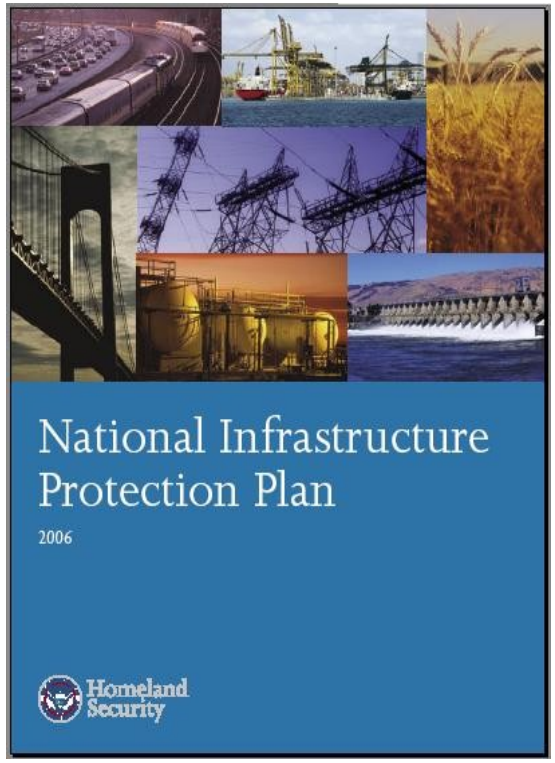
Quali Rischi nell'Era della Partecipazione?

Non ci sono più confini tra le reti, tutto è interconnesso



Le PA richiedono Architetture e Soluzioni di Sicurezza Certificate (CNIPA, OCSI, ISCOM)

Le minacce alla sicurezza si sono spostate dai Sistemi alle Applicazioni e ai Dati



Massima Attenzione ai programmi di Protezione delle Infrastrutture Critiche Nazionali ed Europee

L'informazione come bene primario

L'Informazione va protetta dovunque

Alla Creazione

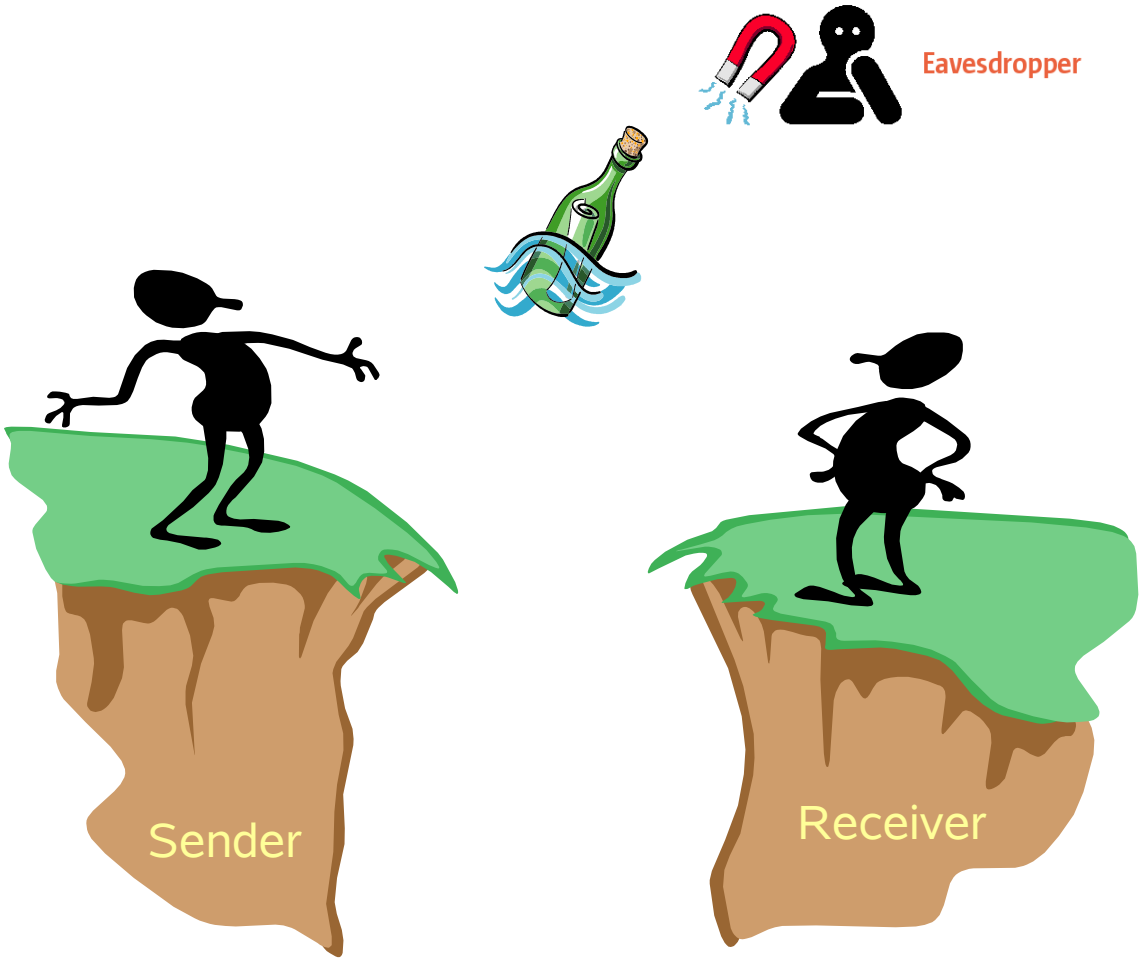
In Transito in Rete

Negli Archivi

Diversi scenari di Sicurezza delle Informazioni

Crittografia come Opportunità

Crittografia: *Il Modello delle Minacce*



Avversari e Attacchi

Attacco Passivo

- l'avversario si limita ad osservare il flusso di dati in transito:
  - si puó prevenire, ma non si puó rilevare

Attacco Attivo

- l'avversario modifica il flusso di dati in transito:
  - si puó rilevare, ma non si puó prevenire

Crittografia: definizioni

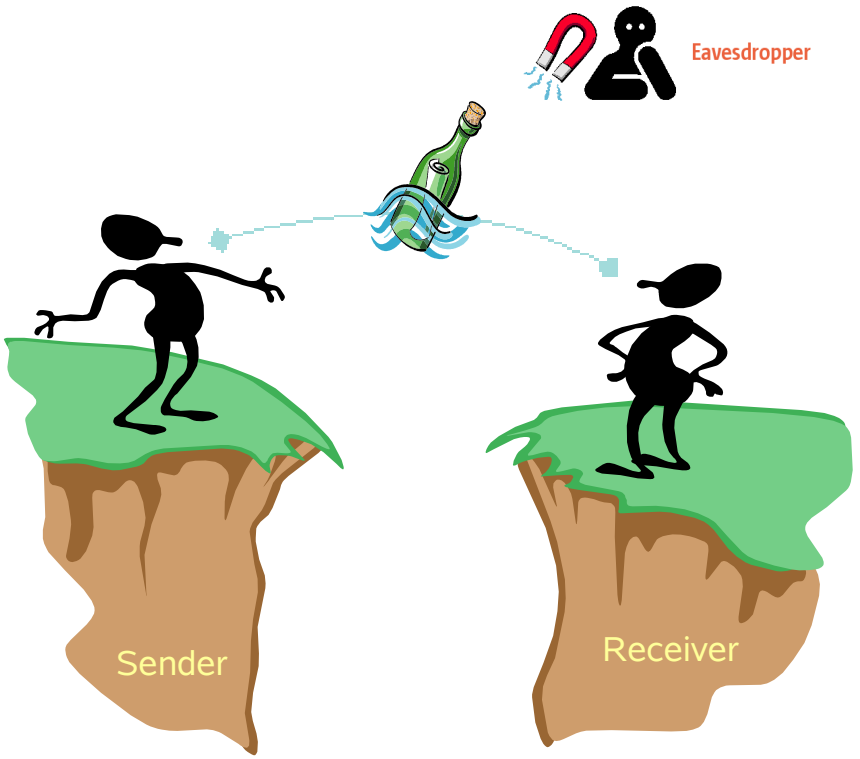
"**la comunicazione in presenza di un avversario**"

(Prof. R. Rivest – Coinventore di RSA)

la scienza che si occupa di rendere incomprensibili le informazioni a chi non possiede un'opportuna chiave di lettura

Crittografia: *Riservatezza delle Comunicazioni*

- lo schema prevede:
  - *sender*
  - *receiver*
  - *Eavesdropper*
- sender e receiver devono scambiarsi informazioni in presenza di un avversario

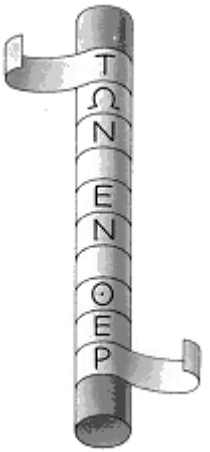


Crittografia: *una contromisura per...*

- La confidenzialitá e riservatezza delle informazioni in transito o depositate
- L'integritá delle informazioni in transito
- Il non ripudio delle transazioni effettuate
- La prevenzione dell'analisi del traffico
- La prevenzione dei canali subliminali
- molte altre cose.....

Alcuni usi della crittografia nella storia

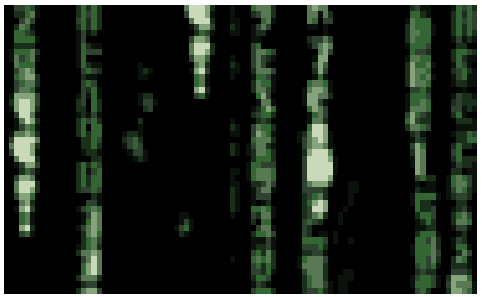
- **Gli schiavi nella antica Persia**
  (Erodoto)
- **La Scytala di Sparta**
  (Plutarco - "*Vite Parallele*")
- **Il cifrario di Cesare**
  (Cicerone)
- **Il rotore Enigma**
  (II guerra mondiale)



La forza di questa crittografia stava nella segretezza dell'algoritmo

La Crittografia Moderna

- si fonda su algoritmi di dominio pubblico
- *basa la sua forza unicamente sulla segretezza della chiave di cifratura (Principio di Kerckhoff)*
- risulta **computazionalmente impossibile** recuperare il messaggio senza conoscere la chiave con cui è stato cifrato



Una divisione fondamentale

- **Crittografia Simmetrica**

  sender e receiver condividono una stessa chiave per cifrare e decifrare

- **Crittografia Asimmetrica o Public Key Cryptography**

  sender e receiver possiedono ognuno una coppia di chiavi (pubblica, segreta)

Crittografia Simmetrica

- ***Sender*** e ***Receiver*** si devono accordare per una chiave crittografica condivisa da usare nella comunicazione
- la chiave comune di cifratura deve essere tenuta segreta, pena la *compromissione* di tutto il cifrario
- l'***Avversario*** che scopre la chiave è in grado di inviare falsi messaggi e comprendere i messaggi riservati di ***S*** e ***R***
- l'utente **A** deve avere una chiave segreta per parlare con l'utente **B**, una diversa per l'utente **C**, un'altra ancora per **D** .... e così via

il numero delle chiavi cresce come n^2 dove n è il numero di utenti del sistema

Crittografia Simmetrica (2)

- utile per cifrare:

  file generici, backup dei dischi, nastri, e-mail, data link, trasmissione fax, digital voice conversation, digital video transmission, etc.

- i cifrari simmetrici si dividono in:

  Block Cipher

  Stream Cipher

Cifrari a blocchi

M = "*Nel mezzo del cammin di nostra vita mi ritrovai in una selva oscura che la diritta via era smarrita* "

M = M_1 M_2 M_3 M_4 M_5

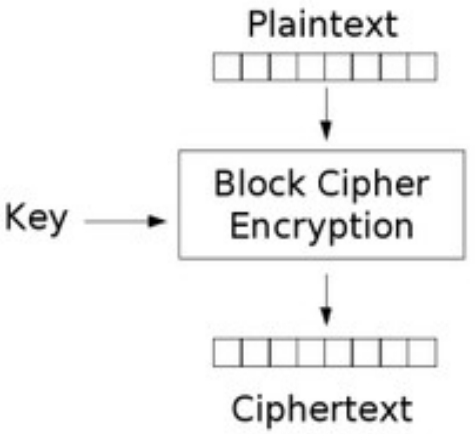
Cifrari a blocchi

- Sia *M* il messaggio in formato chiaro

$$M = M_1 M_2 \ldots\ldots M_n$$

- Sia *K* la chiave di cifratura del messaggio
- il messaggio cifrato *C* si ottiene:

$$C = E_k(M) = E_k(M_1)\, E_k(M_2) \ldots. E_k(M_n)$$



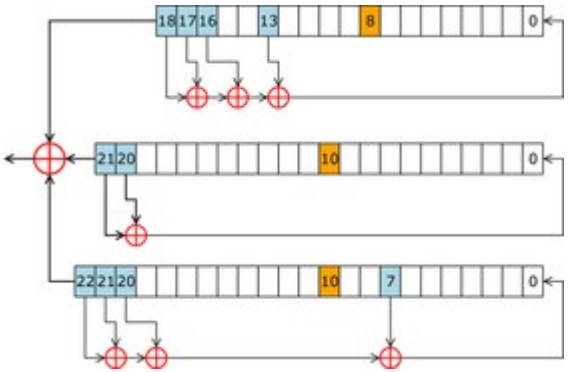
Cifrari a stream

- Sia M il messaggio in chiaro

  $\mathbf{M = m_1\ m_2\ ....\ m_i\ ....\ m_n.....}$ dove m_i è un carattere

- Sia $\mathbf{K = k_1\ k_2\ ....\ k_i\ ....\ k_n.....}$ la chiave di cifratura
- il messaggio cifrato **C** allora è

  $\boldsymbol{C = E_K(M) = E_{k_1}(m_1)\ E_{k_2}(m_2)\ E_{k_3}(m_3)\ .....}$



Autore: *Matt Crypto*

Alcuni cifrari simmetrici

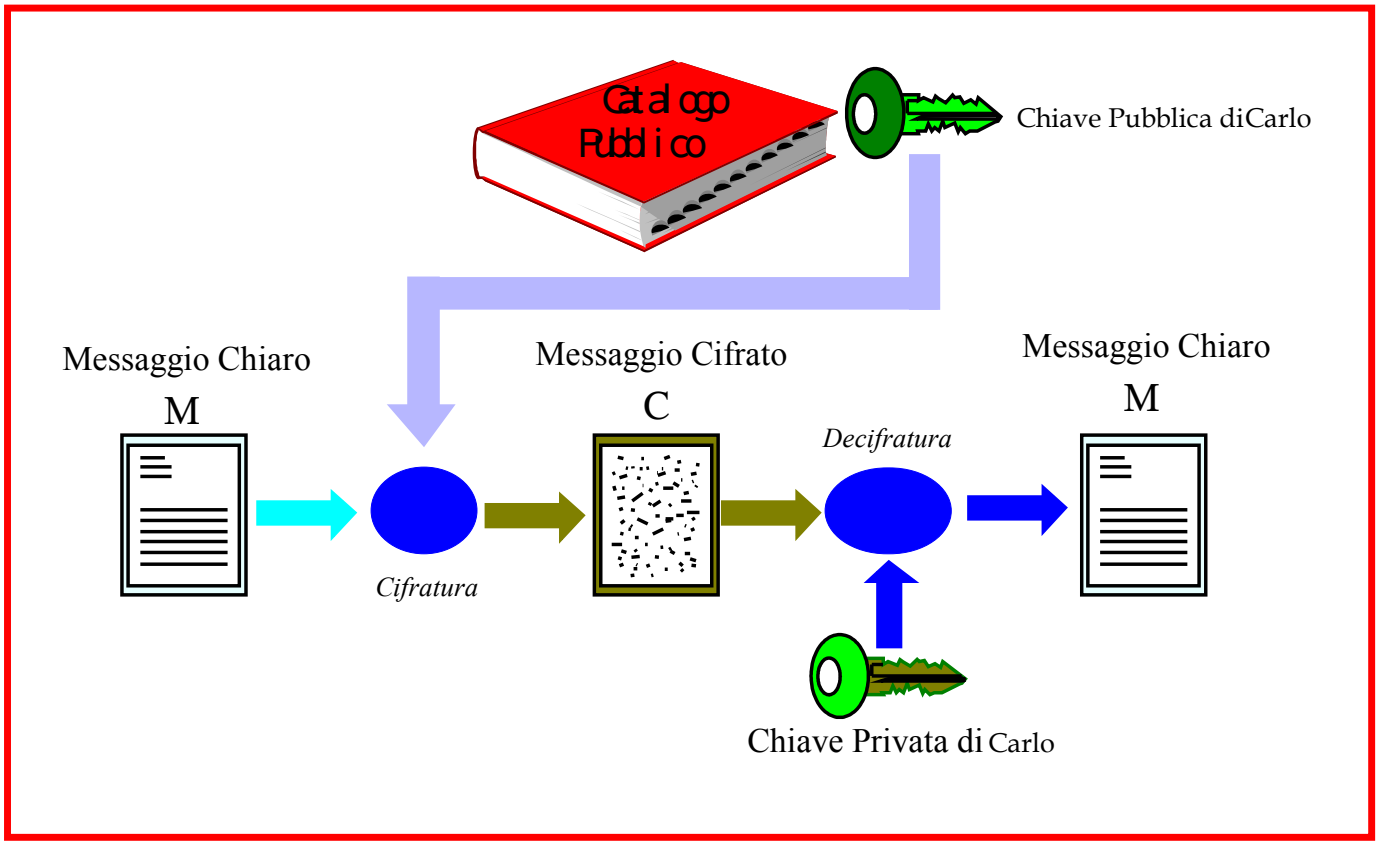
- **DES** (56 bit)
- **Triple DES** (112 o 168 bit)
- **IDEA** (128 bit)
- **Serpent** (128 bit)
- **AES** (128, 192 o 256 bit)
- **Blowfish** (33-448 bit - default 128)
- **CAST** (128 o 256 bit)
- **RC4** chiave a lunghezza variabile
- **RC5** chiave a lunghezza variabile

La crittografia Asimmetrica

- ogni utente possiede una coppia di chiavi (*privata, pubblica*) matematicamente legate
- la *chiave privata* è conservata dal legittimo utente
- la *chiave pubblica* è resa nota a tutti
- non c'è modo di recuperare la chiave privata pur conoscendo quella pubblica

il numero delle chiavi cresce come $2n$ *dove* n *è il numero di utenti del sistema*

Crittografia Asimmetrica (2)



Consente di implementare il meccanismo di NON-RIPUDIO

Alcuni cifrari asimmetrici

- algoritmo per lo scambio di chiavi:

  Diffie-Helmann

- algoritmi per la cifratura

  RSA, ElGamal, Cifrari su Curve Ellittiche

- algoritmi per la firma

  RSA, ElGamal, DSA, Cifrari su Curve Ellittiche

La Crittanalisi

- *L'insieme dei metodi per recuperare il messaggio originale, contenuto in messaggio cifrato, senza conoscerne la chiave di cifratura*
- È lo strumento di lavoro che usa l'attaccante (eavesdropper)
- Esistono vari metodi di crittanalisi

Eavesdropper

Alcuni tipi di critto attacchi classici

- **Ciphertext-only**: l'attaccante ha accesso solo a un insieme di *ciphertext* e *plaintex*
- **Known-plaintext**: l'attaccante possiede un insieme *ciphertext* dei quali conosce il corrispondente *plaintex*
- **Chosen-plaintext** (**chosen-ciphertext**): l'attaccante può ottenere il corrispondente *ciphertext* (*plaintext*) di un arbitrario insieme di *plaintext* (*ciphertext*) che può scegliere

Tutti questi attacchi si possono mitigare con una opportuna scelta della lunghezza delle chiavi crittografiche

Crittanalisi oggi

- Cerca di guadagnare il massimo delle informazioni dalle modalità di *implementazione* dei crittosistemi sotto analisi
- L'attacco si sposta dalla teoria alla pratica
- Tali attacchi sono denominati **Side Channel Attack**

Principali Side Channel Attack

- **Timing attack**: attacchi basati sulla misurazione del tempo necessario affinche una computazione abbia luogo
- **Power monitoring attack**: attacchi che misurano i consumi elettrici/energetici dell'hardware durante la computazione
- **TEMPEST**: attacchi che recuperano dalle radiazioni elettromagnetiche direttamente il plaintext o altre informazioni
- **Acoustic cryptanalysis**: attacchi che recuperano informazioni sulla chiave conservata in un dispositivo sulla base del rumore emesso durante la computazione

Importanza della lunghezza delle chiavi

- poiché i cifrari sono pubblici, uno dei modi per recuperare il messaggio in chiaro consiste nel tentare tutte le possibili 2^n chiavi (*attacco a forza bruta*)
- al crescere della lunghezza della chiave, cresce esponenzialmente il numero di combinazioni da esplorare
- mediamente occorre esplorare il **50%** delle possibili chiavi di lunghezza n cioè 2^{n-1} chiavi

La lunghezza delle chiavi (2)

- tempo medio per rompere un cifrario con una data lunghezza della chiave su una macchina ad hoc ($1 milione) dimostrazione del '95:

40 bit	.2 sec
56 bit	3.6 ore
64 bit	38 giorni
80 bit	7000 anni
112 bit	10^{13} anni
128 bit	10^{18} anni

- in confronto l'*età del sistema solare* è circa **10^{10} anni**
- inoltre si assume che ogni 5 anni gli attacchi saranno 10 volte più veloci e 10 volte più economici

La lunghezza delle chiavi (3)

Livello di Protezione	Crittografia Simmetrica	Crittografia Asimmetrica	Crittografia su Curve Ellittiche	Utile a
Attacchi in "real-time" di singoli invividui	32			*Accettabile solo per i tag di autenticazione*
Protezione a brevissimo termine contro piccole organizzazioni	64	816	128	Non dovrebbe essere usato per garantire la confidenzialità dei dati archiviati
Protezione a breve-termine contro organizzazioni medie e protezione a medio-termine contro piccole organizzazioni	72	1008	144	
Protezioni a brevissimo tempo contro grandi organizzazioni e protezione a lungo-termine contro piccole organizzazioni	80	1248	160	Il più piccolo livello general-purpose, fornisce una protezione dal 2007 al 2010
Protezione Medio-Termine	112	2432	224	*Fornisce una protezione dal 2007 al 2025*
Protezione Lungo-Termine	128	3248	256	Raccomandazione generica e indipendente dall'applicazione, fornisce una protezione dal 2007 al 2035

Fonte: *ECRYPT Report del 2006*

REGIONE DEL VENETO

Direzione Sistema Informatico

Sun microsystems

Grazie

Giuseppe Russo
Chief Technologist
Principal Engineer & Security Ambassador

Sun Microsystems, Inc.