



UNIVERSITÀ DEGLI STUDI
DI GENOVA

UNIVERSITÀ DEGLI STUDI DI GENOVA

Computer Security

Lorenzo Vaccarecci

Indice

1	Introduzione	2
1.1	Information Security	2
1.2	Security Properties	2
1.3	Protection Countermeasures	3
1.4	Managing security: implementing a solution	3
2	Introduzione alla Crittografia	4
2.1	Concetti base	4
2.2	Schema generale della crittografia	4
2.3	Classificazione della sicurezza	5
2.4	Criptanalisi	5
2.4.1	Brute-force attack	5
2.4.2	Tipi di attacco	5
2.5	Matematicamente	5
2.6	Cifrari a blocchi, a flusso e a codici	6
2.7	Cifrari a sostituzione	6
2.7.1	Esempio: Cifrario affine	6
2.7.2	Cifrario a sostituzione omofono	6
2.7.3	Cifrario a sostituzione polialfabetica	6
2.7.4	One-time pads (cifrario di Vernam)	7
2.7.5	Cifrario a trasposizione	7
2.7.6	Cifrario composito	7
3	Crittografia simmetrica	8
4	Message auth & Digital signature	9
5	Public key cryptography	10
6	Security protocols	11
7	Web security	12

Capitolo 1

Introduzione

1.1 Information Security

- La sicurezza concerne la protezione degli **asset** dalle **minacce (threats)**
- I proprietari (**owners**) valorizzano i loro asset e vogliono proteggerli
- I proprietari analizzano le minacce e valutano i rischi. Questo aiuta la selezione di **contromisure** che riducono le **vulnerabilità**

$$Risk_E = P(E) \cdot I_E$$

Dove E è l'evento che rappresenta la minaccia, $P(E)$ è la probabilità che l'evento si verifichi e I_E è l'impatto che l'evento ha.

$$Risk_{Tot} = \sum_{e \in E} (P(e) \cdot I_e)$$

$P(\cdot)$ può essere:

- 0.7 - 1 : Alta
- 0.4 - 0.7 : Media
- ≤ 0.3 : Bassa

1.2 Security Properties

- Confidentiality: l'informazione non è conosciuta da non autorizzati, bisogna permettere solo a chi ne ha diritto attraverso **security policies**. Qualche volta si dice **privacy** per gli individui, **secrecy** per le organizzazioni, **anonymity** invece per nascondere l'identità.
- Integrity: l'informazione non deve essere modificata in modo malizioso.
- Authentication: i dati o i servizi devono essere accessibili solo da chi autorizzato. Solitamente il metodo di autenticazione è qualcosa che si ha, qualcosa che si conosce o qualcosa che sei (impronta digitale, firma, biometrica).
- Availability: i dati o i servizi devono essere accessibili e utilizzabili in qualsiasi momento. Questo significa che bisogna prevenire da attacchi DoS (**Denial of Service**)
- Accountability: le azioni sono registrate e rintracciabili dalle parti responsabili.

1.3 Protection Countermeasures

- Prevention: prevenire gli attacchi attraverso la progettazione di sistemi e impiegando tecnologie di sicurezza.
- Detection: i metodi principali sono il **logging** e il **MACs** (file hash per rilevare alterazioni).
- Response: varia dal ripristinare backup all'informare le autorità competenti o le parti coinvolte.
- Remediation

1.4 Managing security: implementing a solution

- Security Analysis: analizza le minacce che potrebbero compromettere l'asset e propone delle politiche e soluzioni a costi appropriati.
- Threat Model: documenta le possibili minacce al sistema, immaginando tutte le possibili vulnerabilità che possono essere sfruttate.
- Risk Assessment: valutazione quantitativa dei rischi.
- Security Policy: per ogni rischio si descrivono le contromisure da adottare.
- Security Solution: progettazione e implementazione delle tecnologie appropriate a costi appropriati.

Capitolo 2

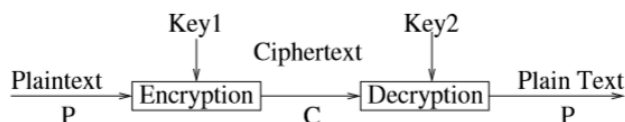
Introduzione alla Crittografia

2.1 Concetti base

CIA: Confidentiality, Integrity, Authentication

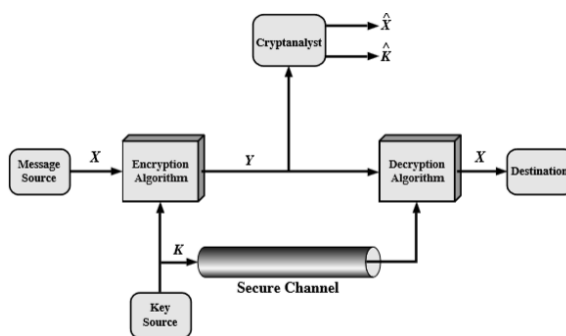
- Confidentiality: l'informazione rimane segreta
- Integrity: l'informazione non è alterata
- Authentication: i principali (Alice e Bob) sanno con chi stanno parlando
- Cryptology: lo studio di scritture segrete
- Steganography: la scienza di nascondere un messaggio in un altro messaggio
- Cryptography: la scienza di scrivere in modo segreto

2.2 Schema generale della crittografia



Dove $E_{key_1}(P) = C$ e $D_{key_2}(C) = P$.

- **La sicurezza dipende dalla segretezza (secrecy) della chiave non dell'algoritmo**
- Algoritmi Simmetrici: le due chiavi sono uguali oppure sono facilmente derivabili l'una dall'altra



Dove nel canale sicuro si invia la chiave e \hat{X} è parte del messaggio decriptato e \hat{K} è parte della chiave decriptata.

- Algoritmi Asimmetrici: le due chiavi sono diverse e non è possibile derivare una dall'altra e una chiave pubblica (**public key**) può essere distribuita senza compromettere le chiavi private (**private key**)
- Quando si costruisce un sistema crittografico bisogna presumere che l'algoritmo sia conosciuto, quindi la sicurezza dipende dalla chiave

2.3 Classificazione della sicurezza

- **Unconditional Security**: il sistema è sicuro anche se l'avversario ha potenza computazionale illimitata. La sicurezza è misurata in termini di teoria dell'informazione (information theory).
- **Conditional Security**: il sistema può essere violato se l'avversario ha abbastanza potenza computazionale. La sicurezza è misurata in termini di teoria della complessità (complexity theory).

2.4 Criptoanalisi

E' la scienza del recuperare il messaggio originale da quello criptato senza la chiave. L'obiettivo non è solo quello di recuperare il messaggio ma anche la chiave.

2.4.1 Brute-force attack

- E' sempre possibile: basta provare tutte le chiavi, solitamente sono $2^{\#bit}$ chiavi possibili se sono caratteri invece è una permutazione di $n!$ chiavi possibili.
- Costa molto, dipende dalla dimensione della chiave
- Presume che il messaggio decifrato sia conosciuto o riconoscibile

2.4.2 Tipi di attacco

- **Ciphertext only**: l'avversario conosce il testo cifrato e prova a dedurne la chiave
- **Known plaintext**: rispetto a ciphertext only, l'avversario conosce anche il testo decifrato
- **Chosen plaintext**: come sopra ma l'avversario può scegliere il testo cifrato
- **Adaptive chosen plaintext**: può, non solo scegliere il testo decifrato, ma può modificare il testo decifrato in base ai risultati della cifratura
- **Chosen ciphertext**: l'avversario può scegliere il testo cifrato e vedere il testo decifrato

2.5 Matematicamente

- \mathcal{A} è l'alfabeto, un insieme finito
- $\mathcal{M} \subseteq \mathcal{A}^*$ è lo spazio dei messaggi. $M \in \mathcal{M}$ è un messaggio in chiaro
- \mathcal{C} è lo spazio dei testi cifrati, il cui alfabeto può essere diverso da quello di \mathcal{M}
- \mathcal{K} denota l'insieme delle chiavi
- $e \in \mathcal{K}$ determina una funzione biettiva $e : \mathcal{M} \rightarrow \mathcal{C}$, la funzione di cifratura è denotata da E_e

- $\forall d \in \mathcal{K}, D_d : \mathcal{C} \rightarrow \mathcal{M}$, la funzione di decifratura è denotata da D_d ed è biettiva
- $D_d(E_e(M)) = E_e^{-1}(M) = M$

2.6 Cifrari a blocchi, a flusso e a codici

- **Block cipher**: è uno schema di cifratura che divide il messaggio in blocchi di lunghezza fissa t e cifra ogni blocco separatamente.
- **Stream cipher**: è uno schema di cifratura dove il blocco è di lunghezza 1 (un bit alla volta)
- **Code**: è uno schema di cifratura dove il messaggio è cifrato in blocchi di lunghezza variabile

2.7 Cifrari a sostituzione

- **Cifrario di Cesare**: ogni carattere del messaggio in chiaro viene sostituito dal carattere n a destra modulo 26 (26! possibili chiavi, molto poco sicuro)
- **ROT13**: è un cifrario di Cesare con $n = 13$
- **Alfanumerico**: si sostituisce ogni carattere con un numero

2.7.1 Esempio: Cifrario affine

- E' una sostituzione monoalfabetica tale che $E(m) = (a \cdot m + b) \bmod |\mathcal{A}|$ dove a, b sono interi positivi e sono chiave del cifrario
- Per essere invertibile a deve essere coprimo con $|\mathcal{A}|$
- La decifratura è $D(c) = a^{-1}(c - b) \bmod |\mathcal{A}|$ dove $1 = a \cdot a^{-1} \bmod |\mathcal{A}|$

2.7.2 Cifrario a sostituzione omofono

Sostituisce ogni lettera a con una stringa scelta a caso da $H(a)$. Per decifrare una stringa c di t simboli, bisogna determinare a tale che $H(a) = c$. La chiave del cifrario è la funzione H .

Esempio

- $H(A) = \{1, 2\}$
- $H(B) = \{3, 4\}$
- $H(C) = \{5, 6\}$

ABC \rightarrow 135 oppure 246 oppure 145 ecc.

2.7.3 Cifrario a sostituzione polialfabetica

E' un cifrario a blocchi con lunghezza t sull'alfabeto A

2.7.4 One-time pads (cifrario di Vernam)

E' un cifrario a flusso definito sull'alfabeto $\mathcal{A} = \{0, 1\}$ il messaggio è cifrato scegliendo casualmente una chiave k binaria di lunghezza uguale al messaggio m e facendo $c = m \oplus k$ dove \oplus è l'operazione di XOR, $d = c \oplus k$ è la decifratura.

Le chiavi non vanno mai riutilizzate.

La funzione di cifratura $E(K, M)$ è **malleabile** se e solo se

$$F(E(K, M)) = E(K, G(M)) \quad \forall K, M$$

Esempio

La funzione $E(K, M) = K \oplus M$ è chiaramente malleabile. Se $F(X) = G(X) = N \oplus X$

$$F(E(K, M)) = N \oplus (K \oplus M) = K \oplus (N \oplus M) = E(K, N \oplus M) = E(K, G(M))$$

2.7.5 Cifrario a trasposizione

E' un cifrario che "mischia" (permutazione) le lettere del messaggio senza cambiarne il significato (delle lettere) (es. CIAO \rightarrow OICA) per decifrare bisogna eseguire l'operazione inversa della permutazione.

2.7.6 Cifrario composito

I cifrari basati su sostituzione e trasposizione non sono sicuri però possono essere combinati, è difficile farlo "a mano" infatti sono state inventate le macchine cifranti.

Capitolo 3

Crittografia simmetrica

Capitolo 4

Message auth & Digital signature

Capitolo 5

Public key cryptography

Capitolo 6

Security protocols

Capitolo 7

Web security