

Laboratorio di Informatica I livello Corso di laurea in Lingue e Studi interculturali

a.a. 2011-2012

Paola Zamperlin

Sicurezza

Perché sicurezza

Uso massiccio delle reti

Attacchi a sistemi di elaborazione di banche
aziende enti

Fenomeno dei virus in rete worms

Furto dei dati personali (e-commerce)

Sicurezza

Significato:

«comunicare in modo sicuro e riservato tra due utenti della rete, senza che soggetti terzi possano accedere, manipolare, distruggere le informazioni che i due soggetti – i 2 computer – si scambiano»

Proprietà:

Autenticazione	Destinatario / mittente sono sicuri dell'identità reciproca
Segretezza	Destinatario / mittente sono gli unici a comprendere il contenuto dell'informazione trasmessa
Integrità	L'informazione trasmessa non è alterata nell'invio da mittente a destinatario
Non ripudio	L'autore di un messaggio non può disconoscerne la paternità
Disponibilità	Resistenza ad attacchi che rendono inutilizzabile a soggetti autorizzati l'informazione (computer / siti web), ad esempio DoS – denial of service, virus o hackeraggi

Malware (malicious software)

Programmi che possono penetrare computer, danneggiare file, impossessarsi di informazioni, compromettere il funzionamento di hardware e software

Virus, worm, spyware, crimeware, trojan, ...

Sniffing	<p>Si definisce sniffing l'attività di intercettazione passiva dei dati che transitano in una rete telematica. Tale attività può essere svolta sia per scopi legittimi sia per scopi illeciti (intercettazione fraudolenta di password o altre informazioni sensibili).</p> <p>http://it.wikipedia.org/wiki/Sniffing</p>
Spoofing (IP spoofing)	<p>Attacco informatico che ricorre alla falsificazione dell'identità (spoof).</p> <p>http://it.wikipedia.org/wiki/Spoofing</p>
Hijacking (data spoofing)	<p>Tecnica, nota come Browser Hijacking (dirottamento del browser), che consiste nel modificare opportunamente dei pacchetti dei protocolli TCP/IP al fine di dirottare i collegamenti ai propri siti e prenderne il controllo. Permette ai dirottatori di eseguire sul malcapitato computer una serie di modifiche tali da garantirsi la visita alle loro pagine con l'unico scopo di incrementare in modo artificioso il numero di accessi e di click diretti al loro sito e conseguentemente incrementare i guadagni dovuti alle inserzioni pubblicitarie (ad es. banner pubblicitari)</p> <p>http://it.wikipedia.org/wiki/Hijacking</p>
Denial of Service	<p>“Negazione del servizio”. Si tratta di un attacco informatico in cui si cerca di portare al limite delle prestazioni il funzionamento di un sistema informatico che fornisce un servizio, ad esempio un sito web, lavorando su uno dei parametri d'ingresso, fino a renderlo non più in grado di erogare il servizio.</p> <p>http://it.wikipedia.org/wiki/Denial_of_service</p>

Clonazione di siti	Creazione di siti fantasma somiglianti a quelli originali. Web stripper
Penetrazione in un computer	Mediante: - Password -Carta magnetica, microprocessore, ecc. -Caratteristica fisiche (biometria)
Phishing	Phishing is a way of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication. http://en.wikipedia.org/wiki/Phishing
Spyware	Uno spyware è un tipo di software che raccoglie informazioni riguardanti l'attività online di un utente (siti visitati, acquisti eseguiti in rete etc) senza il suo consenso, trasmettendole tramite Internet ad un'organizzazione che le utilizzerà per trarne profitto, solitamente attraverso l'invio di pubblicità mirata. I programmi per la raccolta di dati che vengono installati con il consenso dell'utente (anche se spesso negando il consenso non viene installato il programma) non sono propriamente spyware, sempre che sia ben chiaro all'utente quali dati siano oggetto della raccolta ed a quali condizioni questa avvenga. http://it.wikipedia.org/wiki/Spyware

Il Web degli inganni

Una semplificata tassonomia degli inganni:

- [Piper P.S., “Web Hoaxes, Counterfeit Scams, and Other Spurious Information on the Internet”, in Mintz A.P., Web of Deception: Misinformation on the Internet, CyberAge Book from Information Today 2002]



Il Web degli inganni

Esempi

Confrontare:

www.whitehouse.org

www.whitehouse.com

www.whitehouse.net

www.whitehouse.gov

Oppure

www.gatt.org con www.wto.org

Crittografia

La parola crittografia deriva dall'unione di due parole greche: κρυπτός (kryptós) che significa "nascosto", e γραφία (graphía) che significa "scrittura". La crittografia tratta delle "scritture nascoste", ovvero dei metodi per rendere un messaggio "offuscato" in modo da non essere comprensibile a persone non autorizzate a leggerlo. Un tale messaggio si chiama comunemente crittogramma.

<http://it.wikipedia.org/wiki/Crittografia>

Crittografia simmetrica

Con crittografia simmetrica, o crittografia a chiave privata, si intende una tecnica di cifratura.

Uno schema di crittografia simmetrica è caratterizzato dalla proprietà che, data la chiave di cifratura "e", sia facilmente calcolabile la chiave di decifratura "d". Un caso particolare, che è quello quasi sempre utilizzato nella pratica, è l'utilizzo della stessa chiave sia per l'operazione di cifratura che quella di decifratura.

La forza della crittografia simmetrica è dunque riposta nella segretezza dell'unica chiave utilizzata dai due interlocutori che la usano

http://it.wikipedia.org/wiki/Crittografia_simmetrica

- Cifrario di Cesare
- Algoritmo di DES
- Standard AES

Crittografia asimmetrica

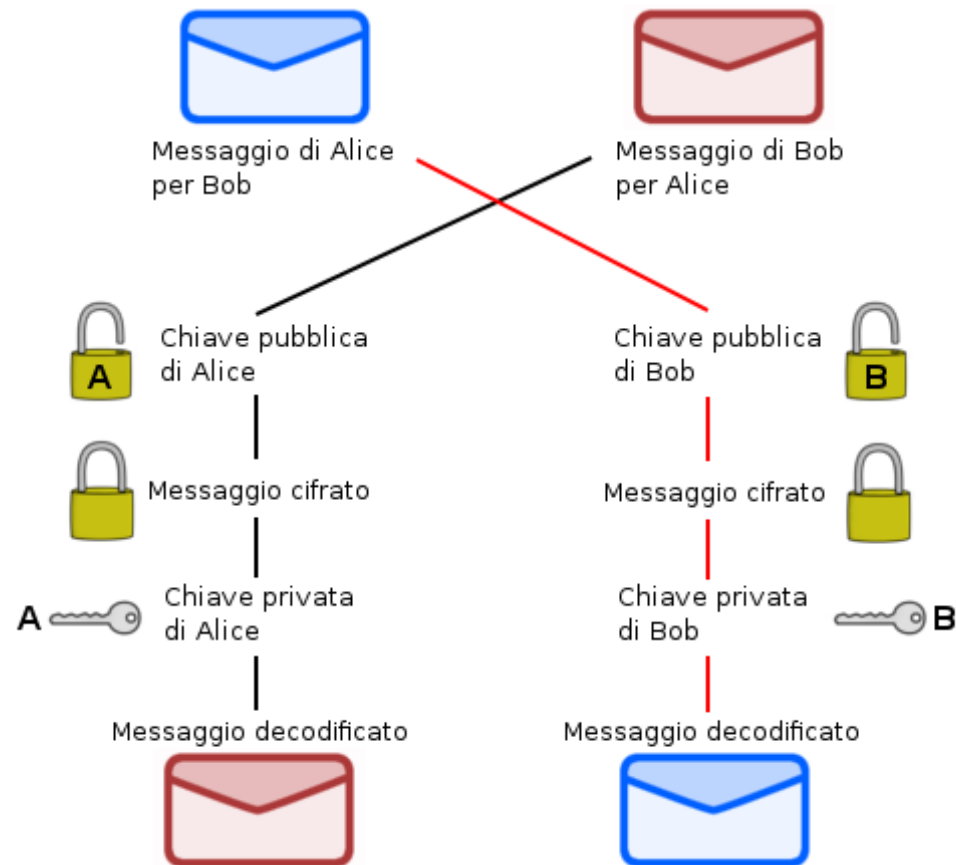
La crittografia asimmetrica (crittografia a coppia di chiavi, crittografia a chiave pubblica/privata o anche crittografia a chiave pubblica) è un tipo di crittografia in cui a ogni attore coinvolto è associata una coppia di chiavi:

1) **chiave pubblica**, che deve essere distribuita, serve a cifrare un documento destinato alla persona che possiede la relativa chiave privata.

2) **chiave privata**, personale e segreta, utilizzata per decodificare un documento cifrato con la chiave pubblica;

evitando così problemi connessi allo scambio dell'unica chiave utile alla cifratura/decifratura presente invece nella crittografia simmetrica.

http://it.wikipedia.org/wiki/Crittografia_asimmetrica



Chiave asimmetrica

Riservatezza

solo il destinatario del messaggio può leggerlo

Autenticazione

Il soggetto che riceve il messaggio ha prova che il mittente (firmatario) è colui che dichiara di essere

Firma digitale

- Chiave pubblica
- Chiave privata
- Certificato

Rappresenta un sistema di autenticazione di documenti digitali tale da garantire il cosiddetto non ripudio. E' basata sulla tecnologia della crittografia a chiave pubblica (o PKI).

La nozione di firma digitale ha in Italia anche un'accezione giuridica, in quanto individua una specie di firma elettronica avanzata che può essere apposta ai documenti informatici alla stessa stregua di come la firma autografa viene apposta ai documenti tradizionali.

[http://it.wikipedia.org/wiki/Firma digitale](http://it.wikipedia.org/wiki/Firma_digitale)

PEC

<http://www.digitpa.gov.it/pec>

CNIPA ora DigitPA

<https://www.postacertificata.gov.it/home/index.dot>