

FACOLTÀ DI GIURISPRUDENZA

Corso di Laurea in Diritto delle Amministrazioni e delle Imprese Pubbliche e Private

DISPENSE DELL'INSEGNAMENTO DI INFORMATICA

A.A. 2005-2006
dott.sa Rosa Anna Sasso

NOTA:

- La prima parte del programma relativa al “Linguaggio del calcolatore” non è stata svolta a lezione quindi non è richiesta.
- La parte relativa alla “Architettura di un calcolatore” e alle “Reti di computer” è trattata nel testo: **ECDL modulo 1**. Pezzoni, Vaccaro - Mondadori informatica.
- La parte relativa alla “Gestione elettronica dei flussi documentari” e al relativo “Quadro normativo” è trattata nel testo: **Informatica applicata alla pubblica amministrazione** Pietro Mercatali-Simone (da pag. 1-66, da pag. 171-186, 194-199).

SICUREZZA E RISERVATEZZA SU INTERNET

Proteggere i dati significa garantirne:

1. La **riservatezza** o **confidenzialità**, ovvero la protezione da letture non autorizzate dei dati memorizzati
2. L'**integrità**, ovvero la protezione da modifiche non autorizzate dei dati memorizzati
3. La **disponibilità**, ovvero la capacità di garantire l'accesso ai dati o alle risorse del sistema
4. L'**autenticazione**, ovvero la possibilità di identificare univocamente gli utenti del sistema.

Tipologie di attacco ai Sistemi

- **attacchi passivi**, che hanno l'obiettivo di compromettere la riservatezza e l'autenticazione, entrando in possesso di informazioni private.
- **attacchi attivi**, che hanno l'obiettivo di compromettere l'integrità e la disponibilità, ovvero mirano ad alterare le informazioni e/o danneggiare i sistemi.

LA VULNERABILITÀ

In generale i rischi in termini di sicurezza informatica sono da imputarsi alla vulnerabilità.

La vulnerabilità può essere addebitata:

1. al software (sia il sistema operativo, sia le applicazioni)
2. ai protocolli di rete
3. al comportamento degli utenti

L'AUTENTICAZIONE

- In un sistema informativo distribuito l'autenticazione riguarda la verifica dell'identità di un utente.
- Sulla base di questa verifica il sistema permette o nega l'utilizzazione di risorse e/o l'esecuzione di procedure.

Tecniche di autenticazione

Le tecniche mediante le quali è possibile identificare host o user sfruttano:

- quello che sai (Something You Know - **SYK**)
- quello che possiedi (Something You Have - **SYH**)
- quello che sei (Something You Are - **SYA**)

L'accesso al sistema attraverso riconoscimento di una password (SYK: quello che sai)

- Il metodo più semplice per l'accesso illecito a un sistema è quello di impossessarsi indebitamente della password di un utente autorizzato e, spacciandosi per esso, di compromettere riservatezza, integrità, autenticazione e a volte disponibilità dei dati.

A ogni utente sono tipicamente assegnate una o più password, tra le quali:

- la password di accesso al computer o al dominio locale, che impedisce l'utilizzo improprio delle risorse interne (hardware, software e dati).
- La password di accesso alla posta elettronica e ai servizi Internet, che identifica l'utente nell'uso delle risorse esterne.

Regole di comportamento

- Utilizzare password di almeno 6 caratteri e di tipo non banale
- La password è strettamente personale
- Non trascrivere mai la password su promemoria. (La password deve essere ricordata a memoria)

L'accesso al sistema attraverso il possesso di un token (SYH: quello che possiedi)

- Per potere essere autenticato e quindi accedere al sistema l'utente deve possedere il token (chiave) e, di norma, essere a conoscenza di un segreto, ad esempio un PIN o una password.

Eventuali problemi:

- Il token può essere smarrito, clonato o al momento non disponibile.
- Il token comporta un costo che in alcuni casi può anche essere elevato.
- Il corretto uso del token presuppone l'esistenza di una infrastruttura hardware e software che può essere piuttosto complessa.

L'accesso al sistema attraverso (SYA: quello che sei)

- L'utente viene identificato per mezzo di qualcosa che è.
- Appartengono a questa categoria i meccanismi di identificazione biometria (Impronta digitale, Iride, Voce, Geometria facciale, Geometria della mano).

Eventuali problemi

- Alta percentuale di errore, stimabile nel 10%.
- Costo elevato delle attrezzature.

Tipi di attacchi ai Sistemi Informatici

- abuso dell'identità elettronica
- exploit
- malicious software
- sniffing
- spoofing
- denial of service

ABUSO DELL'IDENTITÀ ELETTRONICA

L'identità elettronica degli utenti può essere sostituita in modo malizioso intercettando la password

- sia al di fuori del sistema (attraverso confidenze o promemoria)
- sia sfruttando vulnerabilità dei sistemi interni (ad esempio con un cavallo di Troia)
- sia mentre queste credenziali transitano sulla rete

EXPLOIT

- Si indica tipicamente con exploit l'esecuzione delle azioni necessarie ad approfittare di una vulnerabilità del sistema per sferrare un attacco (spesso si tratta di bug del sistema operativo).

SOFTWARE DOLOSO (MALICIOUS SOFTWARE O MALWARE)

- Esistono diverse tipologie di software doloso tra cui i più noti e diffusi sono virus, Cavalli di Troia, worm, macro.

Virus

Un virus informatico è un programma, cioè una serie di istruzioni scritte da un programmatore con le caratteristiche di:

- Inglobarsi e confondersi con le istruzioni dei file eseguibili preesistenti sul sistema
- Replicarsi, cioè copiare le istruzioni che lo compongono in altri programmi
- Agire, dopo un tempo prestabilito, necessario per la replicazione, il virus comincia a compiere l'azione per cui è stato scritto (distruggere dati e/o programmi o, semplicemente, far comparire a video un messaggio)

Cavalli di Troia

- Sono programmi apparentemente innocui che una volta eseguiti, effettuano operazioni diverse da quelle che promettono di fare e sono tipicamente dannose.
- Un esempio di cavallo di troia molto semplice è la creazione di una finestra di login identica a quella del sistema ma finta, che invia password e altre informazioni riservate all'autore del software doloso.

Worm

- Sono programmi che utilizzano i servizi di rete per propagarsi da un sistema all'altro.
- Agiscono creando copie di se stessi sugli host ospiti e mettendosi in esecuzione.
- Sono dunque auto-replicanti e autosufficienti poiché in grado di funzionare senza bisogno di un programma ospite.

I Virus di Macro:

tra le funzionalità dei software di trattamento testi (Word) e di gestione tabelle (Excel) c'è quella di poter realizzare dei semplici programmi che lanciano dei comandi automaticamente all'apertura del documento.

Questi programmi sono realizzati con uno pseudo-linguaggio detto linguaggio macro.

Attraverso l'uso delle macro si possono scrivere istruzioni per cancellare e rinominare file, per modificare il loro contenuto e, anche, per scrivere il contenuto del virus in altri file usati dalla medesima applicazione.

Altri programmi maliziosi

- Non hanno un comportamento dannoso rispetto i dati presenti sul calcolatore ma possono essere dannosi in altri termini

Esempio: Programmi per scaricare suonerie per il cellulare

- Si connettono automaticamente ad un numero telefonico internazionale
- Si trovano su internet o vengono ricevuti via email
- Sostituiscono i settaggi utilizzati per la connessione a Internet con altri numeri a pagamento

Posta non sollecitata: spam

- l'equivalente in rete dei volantini pubblicitari infilati nelle cassette postali è l'invio di messaggi e-mail pubblicitari non sollecitati a tanti utenti:
 - costa meno (al mittente)
 - costa di più (all'utente che scarica la posta via modem)
 - gli indirizzi vengono raccolti automaticamente da robot che leggono pagine web e newsgroups estraendo indirizzi e-mail a caso
 - la vendita di indirizzi è un business

Le catene di S.Antonio

- su Internet è ancora più facile, perché non si paga il francobollo
- è comunque una forma di posta non sollecitata
- si presenta in forma:
 - tradizionale (quindi sfortuna o fortuna)
 - falsi virus
 - false notizie da mandare in giro urgentemente

SNIFFING

- Attacco di tipo passivo che mira a compromettere riservatezza e autenticazione effettuando intercettazioni delle comunicazioni.
- Quando i dati viaggiano non criptati su una rete a mezzo condiviso (come sono tipicamente le LAN) è possibile da un qualsiasi punto della rete intercettare i pacchetti in transito destinati ad altri host.

SPOOFING

- Vengono indicati con il termine spoofing diversi tipi di attacchi che hanno come meccanica comune quella della sostituzione.

Tipi di Spoofing

- user account spoofing
- data spoofing
- IP spoofing

NEGAZIONE DI SERVIZIO (DENIAL OF SERVICE)

- Gli attacchi di tipo Denial of service hanno come principale bersaglio la disponibilità delle risorse, in particolare dei sistemi e dei servizi.
- Lo scopo di chi tenta l'attacco non è quindi quello di ottenere informazioni o di modificarle, quanto quello di impedire ad altri l'accesso alle informazioni.

Due forme molto semplici e diffuse di Denial of service sono:

- Il **mail bombing**, che è realizzato inviando a un utente una quantità di posta sufficiente a riempire lo spazio disponibile e dunque bloccare il suo servizio di ricezione
- La **bandwidth consumption**, che consiste nel generare una quantità elevatissima di traffico verso una certa destinazione, occupando tutta la larghezza di banda.

Alcune contromisure

- La crittografia
- I software antivirus
- I firewall

Crittografia

Consente di far transitare sulla rete messaggi codificati in modo da non poter essere compresi.

Antivirus

- E' un software il cui obiettivo è identificare il virus e rimuoverlo prima che entri in azione.
- Esso cerca all'interno della memoria (centrale e di massa) particolari sequenze di byte che costituiscono l'impronta identificativa del virus.
- La continua produzione di nuovi virus rende quindi indispensabile un aggiornamento continuativo del software antivirus per garantirne l'efficacia nel tempo.

Le verifiche del software antivirus vengono tipicamente fatte in via automatica:

- All'avvio del pc, verificando almeno i file di sistema.
- Periodicamente, scandendo la memoria centrale.
- Ogni qualvolta si effettua una operazione rischiosa verificando i file potenzialmente pericolosi (apertura di un attach di posta elettronica, l'inserimento di un dischetto nel drive, il download di un file).

Firewall

Sistema di filtraggio delle informazioni utilizzato per rendere più difficili gli attacchi ai sistemi di una LAN prevenendo gli accessi non autorizzati

controlla tutte le trasmissioni di dati tra la rete LAN e la rete esterna impedendo l'uscita o l'arrivo di dati da utenti sospetti (hacker)

R.U.P.A.

La Rete Unitaria della Pubblica Amministrazione

Gestita dall' **AIPA**
(Autorità Informatica per la Pubblica Amministrazione)

trasformata in seguito in **CNIPA**
(Centro Nazionale per l'Informatica nella Pubblica Amministrazione)

STRUTTURA

La RUPA è costituita:

- dall'insieme delle strutture di rete delle singole Amministrazioni distribuite sul territorio e utilizzate per trasferirsi dati e informazioni;
- da una struttura che a sua volta consente, attraverso i servizi di trasporto e di interoperabilità, l'interscambio delle informazioni tra le varie amministrazioni e tra queste ed il mondo esterno.

La RUPA si avvale delle tecnologie più avanzate, comprese quelle di Internet, offre livelli di sicurezza, di affidabilità e di servizio, garantiti e vigilati dal Centro Tecnico.

AOO (Area Organizzativa Omogenea)

- Le AOO sono intese come una parte di una Amministrazione che rappresenta un aggregato, il più ampio possibile, di uffici caratterizzati da elevati livelli di coesione interna.
- Tutte le AOO utilizzano criteri uniformi di classificazione e archiviazione, nonché di comunicazione interna tra le aree stesse.
- La definizione delle AOO avviene "con apposito atto di documentazione interna" da parte della PA interessata.

OBIETTIVO DELLA RUPA

Garantire a qualunque utente della rete, purché debitamente autorizzato e in condizioni di sicurezza, di poter accedere ai dati e alle procedure residenti nei sistemi informativi automatizzati della propria e delle altre Amministrazioni.

VANTAGGI DERIVANTI DALL'UTILIZZO DELLA RUPA

- razionalizzazione dei costi di comunicazione;
- riduzione delle attività imputabili alla frammentazione dei processi di servizi e ai conseguenti costi di transazione;
- integrazione dei processi;
- diminuzione dei tempi nei servizi;
- migliore qualità dei prodotti intermedi e finali;
- benefici di relazione derivanti dall'aumento di visibilità sui procedimenti amministrativi con la piena attuazione della legislazione sulla trasparenza.

IL MODELLO DELLA RUPA DEVE RISPETTARE I PRINCIPI DI:

- Autonomia
- Cooperazione

LA RUPA È STRUTTURATA IN 3 AREE:

1. Interconnessioni Telematiche
2. Interoperabilità
3. Software

1. Interconnessioni Telematiche

Riguardano i collegamenti geografici interni ai domini delle singole amministrazioni;
Esiste anche una Struttura interdomini: costituita da collegamenti fra le Amministrazioni ed il Centro di gestione dell'interoperabilità;

Alla rete si possono connettere le Amministrazioni regionali e locali.

2. I servizi di interoperabilità

- Posta Elettronica
- Trasferimento di file
- Terminale virtuale
- Il servizio WWW

Sono servizi standard che permettono:

- la comunicazione tra utenti interni di una amministrazione;
- la comunicazione tra utenti di domini di altre amministrazioni;
- l'esecuzione di applicazioni residenti sui computer delle altre amministrazioni.

Il Centro di Gestione del servizio di interoperabilità fornisce servizi:

- di base, per l'interscambio delle informazioni tra le amministrazioni;
- addizionali, per l'interscambio all'interno delle singole amministrazioni.

I flussi informativi delle singole Amministrazioni sono tra di loro separati da barriere di sicurezza.

3. Servizi software

La RUPA è un **sistema distribuito disomogeneo** ad *architettura client/server*

- I **Middleware** sono prodotti software, che realizzano l'integrazione delle parti di un sistema client/server, consentendo l'identificazione, l'autenticazione, l'autorizzazione e la sicurezza;
- Tutti i domini della Rete devono adottare gli stessi middleware realizzando comuni modalità standard di interconnessione applicativa;
- In questo modo la Rete diventa una "**Dorsale Cooperativa**" cioè un sistema informativo unico in cui tutti i domini client hanno la capacità tecnica di accedere a tutti i domini server.

CRITTOGRAFIA

- È la scienza che studia i sistemi per rendere certe informazioni segrete e leggibili solo a chi possiede la chiave per decifrarle
- Oggi è fondata quasi esclusivamente sull'impiego di sistemi informatici e di programmi che svolgono complesse operazioni matematiche.
- Trasforma in numeri tutte le lettere che compongono un testo e poi compie su questi numeri una serie di moltiplicazioni, ottenendo un numero molto grande.
- Chi è a conoscenza delle operazioni compiute e dei valori per i quali sono stati moltiplicati i numeri di partenza (cifrario e chiave) - è in grado di decifrare il contenuto.
- Chi non dispone di queste informazioni, deve cercare di **rompere il cifrario** per decrittare il testo
- la sicurezza della crittografia non è una sicurezza assoluta, ma relativa al tempo necessario per rompere il cifrario.
- In termini tecnici si parla di **robustezza** del sistema di crittografia (lunghezza della chiave di cifratura): più essa è lunga, più il cifrario è robusto.

Un calcolatore di enorme potenza può impiegare anni per trovare la chiave e mettere in chiaro il testo cifrato.

Crittografia a chiavi simmetriche (TRIPLE DES) (RCA)

Utilizza la stessa chiave (192 bit) sia per cifrare che per decifrare il documento

DIFETTO: se la chiave viene a conoscenza di chi è interessato a conoscere abusivamente il contenuto del testo, la segretezza viene meno

Crittografia a chiavi asimmetriche (RSA)

Utilizza una coppia di chiavi diverse (1024 bit) una per cifrare e una per decifrare il documento

(non importa quale delle due chiavi della coppia venga usata per la prima operazione)

chiunque può inviare un messaggio segreto a chi renda pubblica una delle due chiavi.

non si può decifrare il testo con la stessa chiave usata per cifrarlo

le due chiavi sono generate con la stessa procedura e correlate univocamente conoscendo una delle due chiavi, non c'è nessun modo di ricostruire l'altra

Funzionamento

- munirsi di un software crittografico (compatibile con quelli usati dagli altri interessati) e generare la propria coppia di chiavi;
- rendere disponibile a chiunque una delle due chiavi (chiave pubblica), mentre si deve custodire gelosamente l'altra (chiave privata);
- per mandare a qualcuno un messaggio segreto si deve cifrarlo con la chiave pubblica del destinatario;
- solo il destinatario può decifrare il messaggio, perché solo lui dispone della chiave privata correlata alla chiave pubblica usata dal mittente.

Riconoscimento del mittente

- I cifrari a chiave pubblica possono essere usati anche "al contrario", cioè cifrando il testo chiaro con la chiave privata del mittente
- (chiunque può decifrare il testo con la chiave pubblica dello stesso mittente) ma, se l'operazione riesce, significa che il messaggio è stato inviato proprio dal titolare della chiave pubblica usata per la decifratura

Riservatezza e Autenticità

- Per ottenere nello stesso tempo sia la riservatezza del contenuto sia l'autenticità della sottoscrizione si possono combinare le due operazioni:
- il mittente può inviare un messaggio segreto, cifrato con la propria chiave privata e con la chiave pubblica del destinatario.
- Il destinatario decifra il messaggio con la propria chiave privata e con la chiave pubblica del mittente.

FIRMA DIGITALE

- Sul documento cartaceo la firma certifica il supporto;
- Nel documento elettronico la firma certifica il contenuto;
- Accompagna il documento elettronico nei suoi trasferimenti.

La firma digitale viene usata:

- per trasmettere documenti (per via telematica o a mezzo posta elettronica);
- per archiviare documenti.

Ciascuna Amministrazione deve istituire una casella di posta elettronica adibita alla protocollazione dei messaggi ricevuti.

L'indirizzo di tale casella è pubblicato sul Registro delle Amministrazioni Pubbliche.

La Firma Digitale è basata sulla crittografia a **chiavi asimmetriche**:

Il Procedimento:

Il sistema più elementare è:

- inviare un testo chiaro insieme a una versione cifrata con la chiave privata del mittente A
- Decifrare il testo cifrato con la chiave pubblica del mittente A
- se i due testi risultano uguali, si ottengono le due certezze sull'identità del mittente e sull'integrità del contenuto

DIFETTO:

il sistema è lento, perché è necessario cifrare e decifrare tutto il testo, che potrebbe essere molto lungo

SCORCIATOIA:

- cifrare solo un brevissimo riassunto del testo: l'**impronta del testo (message-digest o digest)** ottenuto con una procedura detta **funzione di hash**
- Se, alla fine della procedura, l'impronta che risulta dalla decifrazione è uguale a quella che si ottiene applicando la funzione di hash al testo chiaro, vuol dire che esso non è stato alterato dopo la generazione della firma digitale

Funzione di HASH

- L'**Impronta** del testo è ottenuta con una procedura detta **funzione di Hash**
- L'**Hash** è un algoritmo matematico che riduce un testo di lunghezza arbitraria in una stringa binaria costante e piccola (128 o 160 bit) garantendo:
 - Univocità della stringa binaria prodotta (impossibile ottenere lo stesso digest partendo da due testi diversi)
 - Impossibilità di risalire al testo originale conoscendo solo il suo digest

Vantaggi del Digest

- Consente di ridurre i tempi di cifratura
- Permette l'autenticazione della firma senza rendere noto l'intero testo ad una terza parte
- Evita la cifratura di tutto il testo con la chiave privata che lo rende decifrabile a tutti tramite la chiave pubblica
- Elimina lo spaccettamento del testo e la firma dei singoli blocchi riducendone la vulnerabilità

Il procedimento assicura:

AUTENTICITÀ

Il destinatario della transazione è certo dell'identità del mittente;

INTEGRITÀ

Il destinatario può verificare con certezza che il contenuto della transazione non sia stato alterato;

NON RIPUDIO

Il mittente non può negare di aver eseguito la transazione;

RISERVATEZZA

L'informazione è cifrata e solo chi è in possesso della chiave di decodifica può leggerla.

Il processo di firma digitale richiede una serie di azioni preliminari necessarie alla predisposizione delle chiavi.

In particolare occorre:

- la registrazione dell'utente presso un'autorità di certificazione;
- la generazione di una coppia di chiavi;
- la certificazione della chiave pubblica;
- la registrazione della chiave pubblica.

Inoltre è necessario dotarsi di:

- Smart Card per la generazione delle chiavi;
- Relativo lettore;
- Software.

La chiave privata resta nel dispositivo, è accessibile tramite PIN e non può essere esportata
Della chiave pubblica è richiesta la certificazione

Le Autorità di Certificazione (CA)

L'Autorità di Certificazione:

- assicura la corrispondenza tra ogni chiave di dominio pubblico e il soggetto che usa la corrispondente chiave privata emettendo un apposito **certificato digitale**
- stabilisce il termine di scadenza dei certificati, quindi il periodo di validità delle chiavi, in funzione:
 - degli algoritmi utilizzati
 - della lunghezza delle chiavi
 - del tipo di servizio per il quale sono impiegate
- riceve la segnalazione di eventuali smarrimenti, furti, cancellazioni, divulgazioni improprie, ecc. di chiavi private e pubblica quindi la lista dei certificati revocati o sospesi in conseguenza di tali fatti.

Validità temporale di una coppia di chiavi

Una coppia di chiavi a 1024 bit può avere validità massima di due anni
Il termine di scadenza del certificato e il periodo di validità delle chiavi possono essere anticipati dal certificatore

VALIDAZIONE TEMPORALE (Marca temporale)

Consiste nella generazione da parte di una autorità di certificazione di una firma digitale aggiuntiva a quella del sottoscrittore
Garantisce che un documento non venga, in un secondo momento, sostituito con uno diverso da parte dell'autore stesso

Procedura:

- L'impronta del documento è inviata al servizio di marcatura temporale
- Il servizio aggiunge data e ora ottenendo una "impronta marcata"
- L'impronta marcata è cifrata con la chiave segreta del servizio ottenendo la marca temporale
- La marca temporale è inviata al richiedente che la allega al documento