

**Operatore Informatico Giuridico**  
**Informatica Giuridica di Base**  
**A.A 2003/2004**  
**I Semestre**

**Appendice::**  
Spunti sulla sicurezza e Internet  
Materiale fuori programma  
dedicato rigorosamente solo ai curiosi

---

prof. Monica Palmirani

## Sicurezza del WEB

---

- Con l'introduzione del commercio elettronico il grado di sicurezza della rete Internet e delle connessioni HTTP si sono evolute al fine di assicurare la la correttezza, l'integrità e la riservatezza delle transazioni in rete
- SSL - secure socket layer - Netscape - garantisce la cifratura e l'autenticazione della comunicazione fra client e server Web. Abbinato a questo troviamo l'TLS - Transport Layer Security del livello di trasporto
- SSL garantisce:
  - autenticazione del server
  - autenticazione del client
  - una sessione cifrata per la trasmissione dati

# SSL

---

- Si accede ad un sito protetto da SSL via browser e la sicurezza è garantita da una chiave simmetrica cifrata condivisa fra client e server
- l'url che compare è **https** invece che http
- inizia la fase di **handshake** (stretta di mano) fra server e client
- il server invia il certificato
- il client genera una **chiave pubblica** sulla base del **certificato** ricevuto e una **simmetrica** che cifra con la chiave pubblica appena costruita - RSA a chiave pubblica
- il client invia la **chiave simmetrica** cifrata al server
- ora il client e il server condividono una chiave simmetrica di connessione attraverso la quale possono cifrare e decifrare i dati che si trasmetteranno

© Palmirani

## Limiti dell'SSL

---

- Tutto il procedimento non garantisce che chi sta comunicando sia **autorizzato** a compiere operazioni, transizioni, pagamenti con carta di credito
- Il client potrebbe inserire una carta di credito falsa o rubata che il meccanismo SSL non è in grado di tutelare l'effettiva bontà della transazione
- SSL garantisce solo la sicurezza, l'integrità e l'autenticazione e non garantisce da operazione fraudolente

© Palmirani

## SET (i)

---

- SET - Secure Electronic Transaction
- Visa e MasterCard nel 1996
- SET cifra i dati **tipici di un pagamento** con carta di credito, **non può cifrare dati** di diverso tipo (immagini, testo, messaggi generici, etc.)
- SET coinvolge i **tre attori principali**: acquirente, venditore, banca del venditore
- SET richiede l'autenticazione di tutte e tre le parti tramite certificati rilasciati dalle rispettive banche

## SET (ii)

---

- Il **certificato dell'acquirente** risulta essere una **rappresentazione elettronica della carta di credito** a tutela del venditore
- Il certificato del venditore rassicura l'acquirente sul buon esito della transazione e dell'accettazione della carta di credito
- Il **SET garantisce che il numero di carta di credito** passi direttamente alla banca del venditore senza che questi lo veda (segretezza e riservatezza)

## SET (iii)

---

- **Portafogli del browser** - browser wallet - tiene traccia delle transazioni eseguite dall'acquirente
- **Server del venditore** - merchant server- è il server che comunica con il cliente e con la banca del venditore
- **Gateway degli acquisti** - acquirer gateway- modulo software della banca del venditore

## I Firewall

---

- dispositivo **hardware** dotato di software programmabile che costituisce una barriera di protezione fra la rete interna e la rete esterna. La barriera viene implementata con diverse tecniche:
  - monitoraggio di tutti i pacchetti in entrata e in uscita
  - controllo dei servizi Internet ammessi in entrata e in uscita
  - effettua un filtraggio degli IP secondo una stop-list e regole di security policy
  - implementa una barriera protettiva nei confronti degli utenti interni alla rete
  - effettua filtri sui comportamenti (blocca spamming, virus, inibisce accessi a siti nella stop-list, etc.)

# I Proxy

---

- Dispositivo **software e/o hardware** che viene installato fra la rete interna e la rete esterna
- Tutte le richieste via HTTP passano attraverso il proxy il quale consente di gestire una sorta di "memoria storica" delle richieste più recenti e quindi di evitare l'accesso continuo verso l'esterno
- Il proxy consente anche un grado di programmabilità **come filtro** di alcuni siti e l'implementazione di alcune regole elementari di sicurezza

© Palmirani

# Virus - (i)

---

- Tutti i virus attraversano quattro fasi:
  - fase latente
  - fase di propagazione
  - fase di innesco
  - fase di esecuzione

© Palmirani

## Virus - (ii)

---

- **Bomba logica** - istruzioni inserite all'interno del sistema che scattano al verificarsi di un determinato evento. Esempio: una data, un determinato comportamento dell'utente, l'esecuzione di un certo programma, etc. A questo punto le istruzioni lesive vengono innescate e parte il danneggiamento di tutto o di parte del sistema
- **cavalli di troia** - meccanismi veicolati attraverso i normali programmi di gestione o le normali attività quotidiane di generica utilità. Una determinata istruzione scatena l'attacco inserito in un normale contesto.

## Virus - (iii)

---

- **Virus** - sono programmi che sono in grado di infettare parti del sistema. I virus informatici, analogamente ai virus biologici, contengono istruzioni in grado di replicare copie di se stesso diffondersi in modo subdolo fino a creare danni visibili. I metodi di replicazione sono molteplici: prelevare la lista delle e-mail spedite ed inviare in modo casuale il virus a questi destinatari, infettare i documenti che si trasmettono via dischetto o via e-mail, infettare file particolari di sistema, etc.

## Virus - (iv)

---

- **Worm** - programmi che utilizzano la rete per diffondersi. I worm possono usare la posta elettronica, la connessione in remoto, replicarsi in remoto su un altro sistema.
- **Batteri** - i batteri hanno lo scopo di auto-replicarsi senza in genere danneggiare direttamente il sistema. Il sistema collassa per "infezione" ovvero per esempio perché un file si è replicato n volte occupando tutto l'hard disk o perché ha occupato tutta la RAM. A questo punto l'accesso al sistema è impedito

© Palmirani

## Rimedi

---

- Rilevazione
- Identificazione
- Rimozione
  
- Pacchetti di uso comune, Norton, McAfee, etc.
- Pacchetti sofisticati, IBM, ditte specializzate che eseguono monitoraggio costante dei sistemi

© Palmirani

# Anonymizer

- Esistono programmi o siti che consentono di utilizzare i servizi di Internet in modo anonimo: web, e-mail, ftp
- Ci sono siti che fungono da filtro e da intermediario per cui reindirizzano la richiesta dell'utente dal loro host senza rivelare la provenienza della richiesta
- Vi sono programmi che "mascherano" l'IP reale rendendo difficile o illeggibile l'indirizzo IP

© Palmirani

The screenshot shows the Anonymizer.com website in a Microsoft Internet Explorer browser window. The address bar displays "http://www.anonymiser.com/". The browser's menu bar includes "File", "Modifica", "Visualizza", "Preferiti", and "Strumenti". The toolbar contains icons for "Indietro", "Avanti", "Termina", "Aggiorna", "Pagina iniziale", "Cerca", "Preferiti", "Cronologia", "Posta", "Stampa", and "Modifica". The address bar shows "http://www.anonymiser.com/#".

The website content includes the "Anonymizer.com" logo, a "STAY INFORMED" newsletter sign-up form, and a navigation menu with "SIGN UP", "PRODUCTS & SERVICES", "BECOME AN AFFILIATE", "PROFESSIONAL", and "HELP/FAQ". Below the navigation menu, there are search boxes for "LEARN:" (containing "About Privacy") and "SHOP:" (containing "Services/Products").

The main content area features several promotional banners:

- FREE ANONYMOUS WEBSURFING**: A section with a text input field for a URL and a "Go" button. It lists benefits: "Prevent tracking by Web sites, hackers and others.", "Shields your IP address", and "Removes privacy threats from the pages you view." Below this is a "NOW -- AN EASIER WAY!" section promoting the "NEW Privacy Button" for privacy protection.
- Wash away your web tracks!**: A banner for "WindowWasher 4.5" with a "Free Trial - Click Here" button.
- MAXIMUM SECURITY SECURE TUNNELLING SSH**: A banner for "Secure Tunneling SSH" with a "Click Here" button.

At the bottom, there is a "New! ANONYMIZER PRIVACYBUTTON" banner with the tagline "The easiest way to take control of your privacy."

# Uso di dati falsi

---

- Un altro modo per mascherare la propria identità in rete è fornire una serie di dati falsi nelle transazioni on-line come:
- Codice fiscale
- Carta di credito
- Partita iva
- Dati personali
- E-mail
- Esistono infatti programmi che consentono la creazione di questi dati in linea con le regole generative e che quindi simulano la loro autenticità

© Palmirani

# Esempio di creazione di dati falsi

---

- Carta di credito –  
[www.elfgrin.com/discard.html](http://www.elfgrin.com/discard.html)



The screenshot shows a web interface for generating fake credit card numbers. At the top, there is a dropdown menu labeled "Choose Pattern" with "MasterCard - Eurocard France" selected. Below it is a text input field containing the pattern "5130 xxxx xxxx xxxx". Underneath that is a "Separator:" label with a dropdown menu showing "(space)". A "Generate" button is positioned below the separator. At the bottom, a text area displays the output: "Valid MasterCard - Eurocard France # found: 5130 6803 3744 4245".

© Palmirani

# Esempio di creazione di dati falsi

---

- Codice fiscale –  
<http://www.telextra.com/home/codfis/>

**Creazione Codice Fiscale**

Inserire il **cognome** per intero:

  

REPUBLICA ITALIANA  
MINISTERO DELLE FINANZE  
Powered by [www.telextra.com](http://www.telextra.com)  
Powered by [www.telextra.com](http://www.telextra.com)

CODICE FISCALE	PLMMNC66B69A944S	
COGNOME	PALMIRANI	
NOME	MONICA	SESSO F
LUOGO DI NASCITA	BOLOGNA	
PROVINCIA	BO	DATA DI NASCITA 29/02/66
2002	Il Ministro delle Finanze	