Sicurezza in Rete

Gregorio D'Agostino

25 Maggio 2021

Livello Name

DNS

Esercizi

Http

Internet Sicura

Autorità e certificati

Il livello Name

- I campi si analizzano partendo da quello finale gordion.casaccia.enea.it

Il livello Name

- I campi si analizzano partendo da quello finale gordion.casaccia.enea.it
  - Il campo it definisce il dominio (quello italiano): tutti i nomi assegnati ai sotto-domini devono essere accettati e definiti nel dominio. Dovrà esistere una autorità di dominio che gestisce i nomi al suo interno.

Il livello Name

- I campi si analizzano partendo da quello finale gordion.casaccia.enea.it
  - Il campo it definisce il dominio (quello italiano): tutti i nomi assegnati ai sotto-domini devono essere accettati e definiti nel dominio. Dovrà esistere una autorità di dominio che gestisce i nomi al suo interno.
  - Il campo enea definisce il sotto-dominio dell'ENEA: questo significa che l'autorità di dominio italiana, conferisce all'ENEA la possibilità di definire i nomi (e di solito anche gli IP) dei nodi il cui nome finisce con "enea.it"

Il livello Name

- I campi si analizzano partendo da quello finale gordion.casaccia.enea.it
  - Il campo it definisce il dominio (quello italiano): tutti i nomi assegnati ai sotto-domini devono essere accettati e definiti nel dominio. Dovrà esistere una autorità di dominio che gestisce i nomi al suo interno.
  - Il campo enea definisce il sotto-dominio dell'ENEA: questo significa che l'autorità di dominio italiana, conferisce all'ENEA la possibilità di definire i nomi (e di solito anche gli IP) dei nodi il cui nome finisce con "enea.it"
  - L'autorità di dominio in ENEA ha definito un sotto-dominio denominato casaccia (un centro di ricerca)

Il livello Name

- I campi si analizzano partendo da quello finale gordion.casaccia.enea.it
  - Il campo it definisce il dominio (quello italiano): tutti i nomi assegnati ai sotto-domini devono essere accettati e definiti nel dominio. Dovrà esistere una autorità di dominio che gestisce i nomi al suo interno.
  - Il campo enea definisce il sotto-dominio dell'ENEA: questo significa che l'autorità di dominio italiana, conferisce all'ENEA la possibilità di definire i nomi (e di solito anche gli IP) dei nodi il cui nome finisce con "enea.it"
  - L'autorità di dominio in ENEA ha definito un sotto-dominio denominato casaccia (un centro di ricerca)
  - Infine l'autorità del centro Casaccia attribuisce al nome gordion il numero IP.

Legami tra IP e name

- Con il comando ping (o nslookup) verifichiamo l'ip corrispondente al nome: ping gordion.casaccia.enea.it (192.107.77.13). In questo caso si tratta di un indirizzo pubblico lo stesso in tutto il mondo. In altri casi gli indirizzi valgono solo in un Authonomus System (tipicamente una LAN) e si dicono privati.

Legami tra IP e name

- Con il comando ping (o nslookup) verifichiamo l'ip corrispondente al nome: ping gordion.casaccia.enea.it (192.107.77.13). In questo caso si tratta di un indirizzo pubblico lo stesso in tutto il mondo. In altri casi gli indirizzi valgono solo in un Authonomus System (tipicamente una LAN) e si dicono privati.
- Il processo con cui si risolve il nome è anch'esso gerarchizzato:

Legami tra IP e name

- Con il comando ping (o nslookup) verifichiamo l'ip corrispondente al nome: ping gordion.casaccia.enea.it (192.107.77.13). In questo caso si tratta di un indirizzo pubblico lo stesso in tutto il mondo. In altri casi gli indirizzi valgono solo in un Authonomus System (tipicamente una LAN) e si dicono privati.
- Il processo con cui si risolve il nome è anch'esso gerarchizzato:
  - Su ogni piattaforma esiste un file (hosts) che contiene una prima tabella di conversione. Questa conversione è prioritaria.

Legami tra IP e name

- Con il comando ping (o nslookup) verifichiamo l'ip corrispondente al nome: ping gordion.casaccia.enea.it (192.107.77.13). In questo caso si tratta di un indirizzo pubblico lo stesso in tutto il mondo. In altri casi gli indirizzi valgono solo in un Authonomus System (tipicamente una LAN) e si dicono privati.
- Il processo con cui si risolve il nome è anch'esso gerarchizzato:
  - Su ogni piattaforma esiste un file (hosts) che contiene una prima tabella di conversione. Questa conversione è prioritaria.
  - Se il nome non è risolvibile localmente si cerca in rete un DNS Domain Name Server o DNS server (attenzione l'acronimo si usa sia per il domain name service che per i server). Nella configurazione della rete deve quindi essere indicato l'IP del DNS. Non si può indicare un nome!

Legami tra IP e name

- Con il comando ping (o nslookup) verifichiamo l'ip corrispondente al nome: ping gordion.casaccia.enea.it (192.107.77.13). In questo caso si tratta di un indirizzo pubblico lo stesso in tutto il mondo. In altri casi gli indirizzi valgono solo in un Authonomus System (tipicamente una LAN) e si dicono privati.
- Il processo con cui si risolve il nome è anch'esso gerarchizzato:
  - Su ogni piattaforma esiste un file (hosts) che contiene una prima tabella di conversione. Questa conversione è prioritaria.
  - Se il nome non è risolvibile localmente si cerca in rete un DNS Domain Name Server o DNS server (attenzione l'acronimo si usa sia per il domain name service che per i server). Nella configurazione della rete deve quindi essere indicato l'IP del DNS. Non si può indicare un nome!
  - A volte sono memorizzati più DNS per ridondanza. Se nessuno dei nostri DNS è in grado di risolvere il name chiede l'informazione ad un DNS di livello gerarchico più elevato.

Legami tra IP e name

- Il file che contiene le definizioni autonome (e quindi gerarchicamente prioritarie) si trova nella locazione:
  /etc/hosts per le macchine linux
  in C:/WINDOWS/system32/drivers/etc per le macchine windows.

Legami tra IP e name

- Il file che contiene le definizioni autonome (e quindi gerarchicamente prioritarie) si trova nella locazione:
  /etc/hosts per le macchine linux
  in C:/WINDOWS/system32/drivers/etc per le macchine windows.
- Con il comando nslookup 192.107.77.13 si può ricavare il nome dall'IP rispettando la gerarchia dei DNS.

Legami tra IP e name

- Il file che contiene le definizioni autonome (e quindi gerarchicamente prioritarie) si trova nella locazione:
  /etc/hosts per le macchine linux
  in C:/WINDOWS/system32/drivers/etc per le macchine windows.
- Con il comando nslookup 192.107.77.13 si può ricavare il nome dall'IP rispettando la gerarchia dei DNS.
- Ognuno faccia una prova nel proprio portatile.

Relazioni plurime

- Vediamo un altro esempio il sito www.motia.eu. Il ping ci fornisce 192.107.77.41.

Relazioni plurime

- Vediamo un altro esempio il sito www.motia.eu. Il ping ci fornisce 192.107.77.41.
- Se chiediamo nslookup 192.107.77.41 troviamo una sfilza di name (tra cui manca motia):
  41.77.107.192.in-addr.arpa name = www.climantartide.it.
  41.77.107.192.in-addr.arpa name = www.medcordex.eu.
  41.77.107.192.in-addr.arpa name = www.climrun.eu.
  41.77.107.192.in-addr.arpa name = utmea.enea.it.
  41.77.107.192.in-addr.arpa name = leonardo.casaccia.enea.it.
  41.77.107.192.in-addr.arpa name = www.utmea.enea.it.
  41.77.107.192.in-addr.arpa name = climantartide.utmea.enea.it.
  41.77.107.192.in-addr.arpa name = www.thuleatmos-it.it.

Relazioni plurime

- Vediamo un altro esempio il sito www.motia.eu. Il ping ci fornisce 192.107.77.41.
- Se chiediamo nslookup 192.107.77.41 troviamo una sfilza di name (tra cui manca motia):
  41.77.107.192.in-addr.arpa name = www.climantartide.it.
  41.77.107.192.in-addr.arpa name = www.medcordex.eu.
  41.77.107.192.in-addr.arpa name = www.climrun.eu.
  41.77.107.192.in-addr.arpa name = utmea.enea.it.
  41.77.107.192.in-addr.arpa name = leonardo.casaccia.enea.it.
  41.77.107.192.in-addr.arpa name = www.utmea.enea.it.
  41.77.107.192.in-addr.arpa name = climantartide.utmea.enea.it.
  41.77.107.192.in-addr.arpa name = www.thuleatmos-it.it.
- Ciò è dovuto alla configurazione del DNS che è asimmetrico. Il server ha due tabelle distinte. La prima (name to IP) è univoca, la seconda (IP to name) può non esserlo.

DNS privati

- Il punto fondamentale da osservare è che si possono costituire gerarchie di DNS server DIVERSE da quelle ufficiali e quindi navigare accedendo a degli IP con nomi diversi da quelli ufficiali.

DNS privati

- Il punto fondamentale da osservare è che si possono costituire gerarchie di DNS server DIVERSE da quelle ufficiali e quindi navigare accedendo a degli IP con nomi diversi da quelli ufficiali.
- Molti IP possono non essere censiti nei DNS ufficiali ma fornire dei servi di rete tramite degli applicativi.

DNS privati

- Il punto fondamentale da osservare è che si possono costituire gerarchie di DNS server DIVERSE da quelle ufficiali e quindi navigare accedendo a degli IP con nomi diversi da quelli ufficiali.
- Molti IP possono non essere censiti nei DNS ufficiali ma fornire dei servi di rete tramite degli applicativi.
- Quindi possono esistere (ed esistono) delle reti gerarchiche di DNS server assolutamente riservate.

Esercizi

- Usare ping e nslookup su indirizzi noti

Esercizi

- Usare ping e nslookup su indirizzi noti
- Verificare la locazione del prorio file hosts. Fare una prova di ping ad un nome inventato (messo in hosts) e vedere che il sistema lo risolve.

Esercizi

- Usare ping e nslookup su indirizzi noti
- Verificare la locazione del prorio file hosts. Fare una prova di ping ad un nome inventato (messo in hosts) e vedere che il sistema lo risolve.
- Usare traceroute per vedere i percorsi dei pacchetti

Esercizi

- Usare ping e nslookup su indirizzi noti
- Verificare la locazione del prorio file hosts. Fare una prova di ping ad un nome inventato (messo in hosts) e vedere che il sistema lo risolve.
- Usare traceroute per vedere i percorsi dei pacchetti
- Verificare propria configurazione internet con il comando ipconfig (o ifconfig in linux).

Protocollo HTTP

- l'HTTP (Hypertext Transfer Protocol) è un protocollo al livello applicazione (sopra TCP/IP) che consente di dialogare con siti ipertestuali.

Protocollo HTTP

- l'HTTP (Hypertext Transfer Protocol) è un protocollo al livello applicazione (sopra TCP/IP) che consente di dialogare con siti ipertestuali.
- I siti ipertestuali sono dei siti su cui è attivo un server http che comunica rispettando le regole del linguaggio ipertestuale HTML. I siti ipertestuali si chiamano anche iper-media.

Protocollo HTTP

- l'HTTP (Hypertext Transfer Protocol) è un protocollo al livello applicazione (sopra TCP/IP) che consente di dialogare con siti ipertestuali.
- I siti ipertestuali sono dei siti su cui è attivo un server http che comunica rispettando le regole del linguaggio ipertestuale HTML. I siti ipertestuali si chiamano anche iper-media.
- L'insieme dei siti ipertestuali forma il www (world wide web: la ragnatela che copre il mondo)

Protocollo HTTP

- l'HTTP (Hypertext Transfer Protocol) è un protocollo al livello applicazione (sopra TCP/IP) che consente di dialogare con siti ipertestuali.
- I siti ipertestuali sono dei siti su cui è attivo un server http che comunica rispettando le regole del linguaggio ipertestuale HTML. I siti ipertestuali si chiamano anche iper-media.
- L'insieme dei siti ipertestuali forma il www (world wide web: la ragnatela che copre il mondo)
- L'Internet Engineering Task Force (IETF) è una struttura federale US, al momento, responsabile di definire gli standard per la comunicazione a livello IP.

Protocollo HTTP

- l'HTTP (Hypertext Transfer Protocol) è un protocollo al livello applicazione (sopra TCP/IP) che consente di dialogare con siti ipertestuali.
- I siti ipertestuali sono dei siti su cui è attivo un server http che comunica rispettando le regole del linguaggio ipertestuale HTML. I siti ipertestuali si chiamano anche iper-media.
- L'insieme dei siti ipertestuali forma il www (world wide web: la ragnatela che copre il mondo)
- L'Internet Engineering Task Force (IETF) è una struttura federale US, al momento, responsabile di definire gli standard per la comunicazione a livello IP.
- Esiste un consorzio internazionale denominato W3C (Worl Wide Web Consortium) a cui aderiscono la maggior parte degli stati che definisce ed aggiorna gli standard HTTP.

Protocollo HTTP

- l'HTTP (Hypertext Transfer Protocol) è un protocollo al livello applicazione (sopra TCP/IP) che consente di dialogare con siti ipertestuali.
- I siti ipertestuali sono dei siti su cui è attivo un server http che comunica rispettando le regole del linguaggio ipertestuale HTML. I siti ipertestuali si chiamano anche iper-media.
- L'insieme dei siti ipertestuali forma il www (world wide web: la ragnatela che copre il mondo)
- L'Internet Engineering Task Force (IETF) è una struttura federale US, al momento, responsabile di definire gli standard per la comunicazione a livello IP.
- Esiste un consorzio internazionale denominato W3C (Worl Wide Web Consortium) a cui aderiscono la maggior parte degli stati che definisce ed aggiorna gli standard HTTP.
- Una sessione HTTP su un computer è una sequenza di istruzione inviate da un client html ad un html gestite da applicativi in genere in modo trasparente per l'utente.

Server HTTP

- Esistono molti Server http, il più famoso è anche open source ed è denominato apache. Chiunque può trasformare il proprio computer (in pratica solo se dotato di IP pubblico o di un name stabile) in un server http.

Server HTTP

- Esistono molti Server http, il più famoso è anche open source ed è denominato apache. Chiunque può trasformare il proprio computer (in pratica solo se dotato di IP pubblico o di un name stabile) in un server http.
- Le funzionalità base definite dal protocollo HTTP sono anche arricchite dal PHP un preprocessore che interpreta le richieste al server, prima di fornire il servizio http.

Server HTTP

- Esistono molti Server http, il più famoso è anche open source ed è denominato apache. Chiunque può trasformare il proprio computer (in pratica solo se dotato di IP pubblico o di un name stabile) in un server http.
- Le funzionalità base definite dal protocollo HTTP sono anche arricchite dal PHP un preprocessore che interpreta le richieste al server, prima di fornire il servizio http.
- Il PHP è un insieme di istruzioni (linguaggio) che di solito esegue il server (tipicamente per creare dinamicamente accesso alle risorse della macchina ospite), ma che possono essere eseguite anche dalla macchina client. Il PHP consente di far apparire un sito in modo dinamico: crea in maniera variabile nel tempo le pagine html che ricevono gli utenti.

Server HTTP

- L'abilitazione dei comandi PHP deve essere strettamente controllata. L'inserzione di comandi da passare al PHP può consentire l'accesso a risorse che sarebbero interdette ai processi provenienti dalla rete. Quando si realizza un attacco di questo genere si parla di Command injection.

Server HTTP

- L'abilitazione dei comandi PHP deve essere strettamente controllata. L'inserzione di comandi da passare al PHP può consentire l'accesso a risorse che sarebbero interdette ai processi provenienti dalla rete. Quando si realizza un attacco di questo genere si parla di Command injection.
- Moltissime vulnerabilità dei sistemi sono legate all'uso dei PHP. Anche il protocollo HTTP (che risponde alla porta 80 normalmente) può presentare delle vunerabilità, ma l'insieme PHP arricchisce notevolmente le possibilità dell'attaccante.

Server HTTP

- L'abilitazione dei comandi PHP deve essere strettamente controllata. L'inserzione di comandi da passare al PHP può consentire l'accesso a risorse che sarebbero interdette ai processi provenienti dalla rete. Quando si realizza un attacco di questo genere si parla di Command injection.
- Moltissime vulnerabilità dei sistemi sono legate all'uso dei PHP. Anche il protocollo HTTP (che risponde alla porta 80 normalmente) può presentare delle vunerabilità, ma l'insieme PHP arricchisce notevolmente le possibilità dell'attaccante.
- Buona pratica: limitare i servizi di rete (in particolare http) al necessario.

Server HTTP

- L'abilitazione dei comandi PHP deve essere strettamente controllata. L'inserzione di comandi da passare al PHP può consentire l'accesso a risorse che sarebbero interdette ai processi provenienti dalla rete. Quando si realizza un attacco di questo genere si parla di Command injection.
- Moltissime vulnerabilità dei sistemi sono legate all'uso dei PHP. Anche il protocollo HTTP (che risponde alla porta 80 normalmente) può presentare delle vunerabilità, ma l'insieme PHP arricchisce notevolmente le possibilità dell'attaccante.
- Buona pratica: limitare i servizi di rete (in particolare http) al necessario.
- Usando il firewall (filtri di rete) possiamo impedire (blacklist) l'uso del protocollo ad alcuni IP oppure limitare (whitelist) l'accesso agli IP di una lista. Questo si può realizzare anche in forma selettiva limitando il filtro ad un protocollo ed ad una o più porte.

Client HTTP

- E' un programma che dialoga con il server HTTP usando il protocollo TCP/IP.

Client HTTP

- E' un programma che dialoga con il server HTTP usando il protocollo TCP/IP.
- La gestione è trasparente per l'utente che utilizza dei browser di rete che trasformano tramite una GUI (Graphic User Interface) le richieste in metodi HTTP.

Client HTTP

- E' un programma che dialoga con il server HTTP usando il protocollo TCP/IP.
- La gestione è trasparente per l'utente che utilizza dei browser di rete che trasformano tramite una GUI (Graphic User Interface) le richieste in metodi HTTP.
- I sistemi operativi sono dotati di Browser nativi, ma spesso se ne usano altri più popolari.

Client HTTP

- E' un programma che dialoga con il server HTTP usando il protocollo TCP/IP.
- La gestione è trasparente per l'utente che utilizza dei browser di rete che trasformano tramite una GUI (Graphic User Interface) le richieste in metodi HTTP.
- I sistemi operativi sono dotati di Browser nativi, ma spesso se ne usano altri più popolari.
- I due browser più famosi sono Firefox e Chrome.

Client HTTP

- E' un programma che dialoga con il server HTTP usando il protocollo TCP/IP.
- La gestione è trasparente per l'utente che utilizza dei browser di rete che trasformano tramite una GUI (Graphic User Interface) le richieste in metodi HTTP.
- I sistemi operativi sono dotati di Browser nativi, ma spesso se ne usano altri più popolari.
- I due browser più famosi sono Firefox e Chrome.
- Quando i PHP vengono gestiti in modalità client le stesse raccomandazioni valgono per il sistema client dell'utente.

Client HTTP

- E' un programma che dialoga con il server HTTP usando il protocollo TCP/IP.
- La gestione è trasparente per l'utente che utilizza dei browser di rete che trasformano tramite una GUI (Graphic User Interface) le richieste in metodi HTTP.
- I sistemi operativi sono dotati di Browser nativi, ma spesso se ne usano altri più popolari.
- I due browser più famosi sono Firefox e Chrome.
- Quando i PHP vengono gestiti in modalità client le stesse raccomandazioni valgono per il sistema client dell'utente.
- I cookies sono dei file dati che vengono istallati sulla macchina client per accelerare il browsing dei siti (in particolare l'autenticazione), sono una potenziale vulnerabilità.

HTML - HyperText Markup Language

- Lo HTML HyperText Markup Language (che significa linguaggio a marcatori per iper-testi) è un linguaggio (a marcatori) che consente un accesso ordinato alle risorse dati contenute in un server in modalità ipretestuale.

HTML - HyperText Markup Language

- Lo HTML HyperText Markup Language (che significa linguaggio a marcatori per iper-testi) è un linguaggio (a marcatori) che consente un accesso ordinato alle risorse dati contenute in un server in modalità ipretestuale.
- Consente di definire la posizione (layout) dei campi da visualizzare (istruzioni da interpretare da parte del server).

HTML - HyperText Markup Language

- Lo HTML HyperText Markup Language (che significa linguaggio a marcatori per iper-testi) è un linguaggio (a marcatori) che consente un accesso ordinato alle risorse dati contenute in un server in modalità ipretestuale.
- Consente di definire la posizione (layout) dei campi da visualizzare (istruzioni da interpretare da parte del server).
- Contengono dei link interni ipertestuali alle differenti parti della pagina o ad altre pagine.

Identificazione universale delle risorse sulla rete

- Esiste un metodo generale per identificare una risorsa sulla rete. L'indicazione classica è detto URL (Uniform Resource Locator):
  <protocollo>://<dominio>/<percorso>?<query>
  in cui il protocollo di solito è http (https) o ftp (sftp)
  il dominio è a livello name (risolubile dal DNS) e il percorso usa la convenzione che il simbolo / indica una sottodirectory
  il simbolo ? indica una richiesta da porre ad un server che risponde al dominio indicato col protocollo indicato ed il percorso indicato.

Identificazione universale delle risorse sulla rete

- Esiste un metodo generale per identificare una risorsa sulla rete. L'indicazione classica è detto URL (Uniform Resource Locator):
  <protocollo>://<dominio>/<percorso>?<query>
  in cui il protocollo di solito è http (https) o ftp (sftp)
  il dominio è a livello name (risolubile dal DNS) e il percorso usa la convenzione che il simbolo / indica una sottodirectory
  il simbolo ? indica una richiesta da porre ad un server che risponde al dominio indicato col protocollo indicato ed il percorso indicato.
- Si tratta di un caso articolare degli URI (Uniform Resource Identifiers):
  <scheme>://<authority><path>?<query>
  lo schema oltre che un protocollo può indicare organizzazione editoriale (isbn), telefonica (tel) per i quali si usano URN (Uniform Resource Name) in cui la locazione non è assegnata, l'autority può essere omessa, ma l'identificativo è unico.

Java e Javascript

- Java è un linguaggio standard universale (ma di scarse prestazioni) del tipo interpretato (o compilato in tempo reale) che viene utilizzato principalmente per la sua Interoperabilità (la capacità di operare su tutte le macchine).

Java e Javascript

- Java è un linguaggio standard universale (ma di scarse prestazioni) del tipo interpretato (o compilato in tempo reale) che viene utilizzato principalmente per la sua Interoperabilità (la capacità di operare su tutte le macchine).
- Molti siti sono scritti in java: eseguono delle istruzioni in java alla ricezione di input dagli utenti di rete. Questo causa un impegno di risorse di calcolo da parte del server. L'attacco denominato line injection consiste nel far eseguire line di codice diverso alle macchine server.

Java e Javascript

- Java è un linguaggio standard universale (ma di scarse prestazioni) del tipo interpretato (o compilato in tempo reale) che viene utilizzato principalmente per la sua Interoperabilità (la capacità di operare su tutte le macchine).
- Molti siti sono scritti in java: eseguono delle istruzioni in java alla ricezione di input dagli utenti di rete. Questo causa un impegno di risorse di calcolo da parte del server. L'attacco denominato line injection consiste nel far eseguire line di codice diverso alle macchine server.
- Per alleggerire i server del lavoro è stato introdotto Javascript che esegue molte delle sequenze di codice sulla macchina client (quella dell'utente). L'approccio tramite javascript riduce, ma non risolve le possibilità di line injection.

Java e Javascript

- Java è un linguaggio standard universale (ma di scarse prestazioni) del tipo interpretato (o compilato in tempo reale) che viene utilizzato principalmente per la sua Interoperabilità (la capacità di operare su tutte le macchine).
- Molti siti sono scritti in java: eseguono delle istruzioni in java alla ricezione di input dagli utenti di rete. Questo causa un impegno di risorse di calcolo da parte del server. L'attacco denominato line injection consiste nel far eseguire line di codice diverso alle macchine server.
- Per alleggerire i server del lavoro è stato introdotto Javascript che esegue molte delle sequenze di codice sulla macchina client (quella dell'utente). L'approccio tramite javascript riduce, ma non risolve le possibilità di line injection.
- Javascript è meno standardizzato di Java e richiede installazione di software specifici (anche open source) come Node.js.

Java e Javascript

- Java è un linguaggio standard universale (ma di scarse prestazioni) del tipo interpretato (o compilato in tempo reale) che viene utilizzato principalmente per la sua Interoperabilità (la capacità di operare su tutte le macchine).
- Molti siti sono scritti in java: eseguono delle istruzioni in java alla ricezione di input dagli utenti di rete. Questo causa un impegno di risorse di calcolo da parte del server. L'attacco denominato line injection consiste nel far eseguire line di codice diverso alle macchine server.
- Per alleggerire i server del lavoro è stato introdotto Javascript che esegue molte delle sequenze di codice sulla macchina client (quella dell'utente). L'approccio tramite javascript riduce, ma non risolve le possibilità di line injection.
- Javascript è meno standardizzato di Java e richiede installazione di software specifici (anche open source) come Node.js.
- Controllando il server Javascript diviene un mezzo perfetto per fare line injection nel client!

Rete sommersa e Rete Oscura: Deep Web - Dark web

- I motori di ricerca sono dei servizi di rete gestiti da soggetti privati che forniscono indicazioni sui siti che contengono informazioni correlate con un testo.

Rete sommersa e Rete Oscura: Deep Web - Dark web

- I motori di ricerca sono dei servizi di rete gestiti da soggetti privati che forniscono indicazioni sui siti che contengono informazioni correlate con un testo.
- Si basano su delle grandi banche date (aggiornate costantemente dagli ispezionatori della rete web crawling) che forniscono all'interrogante una serie di indirizzi http e pagine in essi contenute relative alle richieste.

Rete sommersa e Rete Oscura: Deep Web - Dark web

- I motori di ricerca sono dei servizi di rete gestiti da soggetti privati che forniscono indicazioni sui siti che contengono informazioni correlate con un testo.
- Si basano su delle grandi banche date (aggiornate costantemente dagli ispezionatori della rete web crawling) che forniscono all'interrogante una serie di indirizzi http e pagine in essi contenute relative alle richieste.
- Il web (www) viene suddiviso in surface web e deep (o hidden o dark etc) web, in base alla capacità dei motori di ricerca di indicizzarne i contenuti. Il deep web NON è indicizzato.

La rete sommersa: Deep Web

- A questi siti si trovano motori di ricerca per il deep web, ma di solito chi lo usa sa dove andare non ne ha bisogno:

La rete sommersa: Deep Web

- A questi siti si trovano motori di ricerca per il deep web, ma di solito chi lo usa sa dove andare non ne ha bisogno:
- Esistono altri motori di ricerca (non limitati come sopra al protocollo http) che aiutano a cercare anche sul deepweb, ma si calcola che sia molto più grande di www:
  http://deeperweb.com DeeperWeb è il motore esteso di Google.
  http://vlib.org La libreria virtuale www (WWW Virtual Library) in realtà è una lista di siti dove si trova materiale.
  Altri siti prendono informazioni dai blog e i social come Twitter. I messaggi dei social non sono indicizzati http.

La rete sommersa: Deep Web

- A questi siti si trovano motori di ricerca per il deep web, ma di solito chi lo usa sa dove andare non ne ha bisogno:
- Esistono altri motori di ricerca (non limitati come sopra al protocollo http) che aiutano a cercare anche sul deepweb, ma si calcola che sia molto più grande di www:
  http://deeperweb.com DeeperWeb è il motore esteso di Google.
  http://vlib.org La libreria virtuale www (WWW Virtual Library) in realtà è una lista di siti dove si trova materiale.
  Altri siti prendono informazioni dai blog e i social come Twitter. I messaggi dei social non sono indicizzati http.
- Il deep web non è illegale: usa forme non http per il flusso di dati. Il web crawling consente di osservarlo.

La rete sommersa: Deep Web

- A questi siti si trovano motori di ricerca per il deep web, ma di solito chi lo usa sa dove andare non ne ha bisogno:
- Esistono altri motori di ricerca (non limitati come sopra al protocollo http) che aiutano a cercare anche sul deepweb, ma si calcola che sia molto più grande di www:
  http://deeperweb.com DeeperWeb è il motore esteso di Google.
  http://vlib.org La libreria virtuale www (WWW Virtual Library) in realtà è una lista di siti dove si trova materiale.
  Altri siti prendono informazioni dai blog e i social come Twitter. I messaggi dei social non sono indicizzati http.
- Il deep web non è illegale: usa forme non http per il flusso di dati. Il web crawling consente di osservarlo.
- Il deep web, la rete sommersa consente moltissime azioni segrete e potenzialmente quindi anche illegali. Per contrapposizione la rete di superficie (surface web) viene anche chiamata "rete in chiaro" o Clearnet

Il lato oscuro della rete: Dark web

- La maggior parte del deep web non è visitata dai motori di ricerca solo perché non si ha necessità di farlo, ma non vi è intento di segretezza: chiunque con gli appositi mezzi può accedervi.

Il lato oscuro della rete: Dark web

- La maggior parte del deep web non è visitata dai motori di ricerca solo perché non si ha necessità di farlo, ma non vi è intento di segretezza: chiunque con gli appositi mezzi può accedervi.
- Alcune parti del deep web vengono mantenute segrete ai motori di ricerca deliberatamente. Queste parti vengono genericamente denominate Dark Web (rete oscura).

Il lato oscuro della rete: Dark web

- La maggior parte del deep web non è visitata dai motori di ricerca solo perché non si ha necessità di farlo, ma non vi è intento di segretezza: chiunque con gli appositi mezzi può accedervi.
- Alcune parti del deep web vengono mantenute segrete ai motori di ricerca deliberatamente. Queste parti vengono genericamente denominate Dark Web (rete oscura).
- Le attività che si svolgono nel dark web sono confidenziali, ma non necessariamente illegali.

Il lato oscuro della rete: Dark web

- La maggior parte del deep web non è visitata dai motori di ricerca solo perché non si ha necessità di farlo, ma non vi è intento di segretezza: chiunque con gli appositi mezzi può accedervi.
- Alcune parti del deep web vengono mantenute segrete ai motori di ricerca deliberatamente. Queste parti vengono genericamente denominate Dark Web (rete oscura).
- Le attività che si svolgono nel dark web sono confidenziali, ma non necessariamente illegali.
- I termini rete sommersa e rete oscura sono libere traduzioni che rendono pienamente i concetti, ma in genere si preferiscono i termini originali in inglese.

Il lato oscuro della rete: Dark web

- Per garantire la confidenzialità i gestori forniscono strumenti informatici specifici che non usano il protocollo standard HTTP, ma sono a base TCP/IP.

Il lato oscuro della rete: Dark web

- Per garantire la confidenzialità i gestori forniscono strumenti informatici specifici che non usano il protocollo standard HTTP, ma sono a base TCP/IP.
- Si naviga a livello name, ma si usano pseudo-router oppure IP dinamici (cioè ad un name corrisponde nel tempo un IP diverso) e non allocati dai gestori di dominio ufficialmente riconosciuti da ICANN.

Il lato oscuro della rete: Dark web

- Per garantire la confidenzialità i gestori forniscono strumenti informatici specifici che non usano il protocollo standard HTTP, ma sono a base TCP/IP.
- Si naviga a livello name, ma si usano pseudo-router oppure IP dinamici (cioè ad un name corrisponde nel tempo un IP diverso) e non allocati dai gestori di dominio ufficialmente riconosciuti da ICANN.
- Uno pseudo-router è un computer qualsiasi che riceve pacchetti in cui nella parte informativa, che viene cifrata, ci sono le informazioni su mittente destinatario etc. Lo pseudo-router ha le sue tabelle di routing. Il prefisso pseudo ricorda che l'istradamento avviene ad un livello più altro di internet.

Il lato oscuro della rete: Dark web

- Per garantire la confidenzialità i gestori forniscono strumenti informatici specifici che non usano il protocollo standard HTTP, ma sono a base TCP/IP.
- Si naviga a livello name, ma si usano pseudo-router oppure IP dinamici (cioè ad un name corrisponde nel tempo un IP diverso) e non allocati dai gestori di dominio ufficialmente riconosciuti da ICANN.
- Uno pseudo-router è un computer qualsiasi che riceve pacchetti in cui nella parte informativa, che viene cifrata, ci sono le informazioni su mittente destinatario etc. Lo pseudo-router ha le sue tabelle di routing. Il prefisso pseudo ricorda che l'istradamento avviene ad un livello più altro di internet.
- Nella rete oscura operano social network in cui le persone parlano in libertà senza paura di censura o repressione. Ma si svolgono anche attività illegali come i traffici delle armi, degli organi, dei bambini, delle donne; contrabbando di merci e farmaci; traffico di stupefacenti e perfino attività terroristiche.

Navigare nella rete oscura: Dark web

- Il più noto gestore è TOR (acronimo di "The Onion Router" il router a cipolla). Gli indirizzi del dark web spesso finiscono con .onion (pseudo-dominio) da cui deriva il nome. La rete di gestori di tor è di volontari (come wikipedia). Il suffisso .onion dall'ottobre del 2015 è stato approvato (registrato) dallo IETF (Internet Engineering Task Force) e disciplinato con il Request for comment: RFC 7686 https://tools.ietf.org/html/rfc7686

Navigare nella rete oscura: Dark web

- Il più noto gestore è TOR (acronimo di "The Onion Router" il router a cipolla). Gli indirizzi del dark web spesso finiscono con .onion (pseudo-dominio) da cui deriva il nome. La rete di gestori di tor è di volontari (come wikipedia). Il suffisso .onion dall'ottobre del 2015 è stato approvato (registrato) dallo IETF (Internet Engineering Task Force) e disciplinato con il Request for comment: RFC 7686 https://tools.ietf.org/html/rfc7686
- Andando su https://www.torproject.org/projects/torbrowser.html.en si può scaricare il tor browser che utilizza la rete DNS di TOR e i suoi protocolli.

Navigare nella rete oscura: Dark web

- Il più noto gestore è TOR (acronimo di "The Onion Router" il router a cipolla). Gli indirizzi del dark web spesso finiscono con .onion (pseudo-dominio) da cui deriva il nome. La rete di gestori di tor è di volontari (come wikipedia). Il suffisso .onion dall'ottobre del 2015 è stato approvato (registrato) dallo IETF (Internet Engineering Task Force) e disciplinato con il Request for comment: RFC 7686 https://tools.ietf.org/html/rfc7686
- Andando su https://www.torproject.org/projects/torbrowser.html.en si può scaricare il tor browser che utilizza la rete DNS di TOR e i suoi protocolli.
- Come si è detto i siti .onion posseggono tutti le loro chiavi pubbliche che corrispondono al soggetto che fornisce il servizio, non esiste un vero dns. Un servizio può reindirizzare ad altri servizi.

Anarchia del Dark web

- Chiunque può organizzare la sua fibra (boundle) della rete dark net (cioè un ramo della rete) aggiungendosi ai gestori volontari del sistema (tor o altri).

Anarchia del Dark web

- Chiunque può organizzare la sua fibra (boundle) della rete dark net (cioè un ramo della rete) aggiungendosi ai gestori volontari del sistema (tor o altri).
- Una piattaforma contro la censura (sempre gestita da volontari) è Freenet: https://freenetproject.org/author/freenet-project-inc.html

Anarchia del Dark web

- Chiunque può organizzare la sua fibra (boundle) della rete dark net (cioè un ramo della rete) aggiungendosi ai gestori volontari del sistema (tor o altri).
- Una piattaforma contro la censura (sempre gestita da volontari) è Freenet: https://freenetproject.org/author/freenet-project-inc.html
- Un altro gruppo autonomo di darknet è I2P: https://geti2p.net/en/

Problemi da risolvere per Internet

- Autenticità della provenienza dei pacchetti (proteggerci dallo spoofing e dalla ripudiazione dei messaggi). Ci sono due metodi: ricorrere ad una autorità fidata (si dice "terza" rispetto a chi comunica sulla rete) oppure identificarsi direttamente con canali diversi e diretti.

Problemi da risolvere per Internet

- Autenticità della provenienza dei pacchetti (proteggerci dallo spoofing e dalla ripudiazione dei messaggi). Ci sono due metodi: ricorrere ad una autorità fidata (si dice "terza" rispetto a chi comunica sulla rete) oppure identificarsi direttamente con canali diversi e diretti.
- Integrità dei pacchetti (assenza di alterazioni deliberate).

Problemi da risolvere per Internet

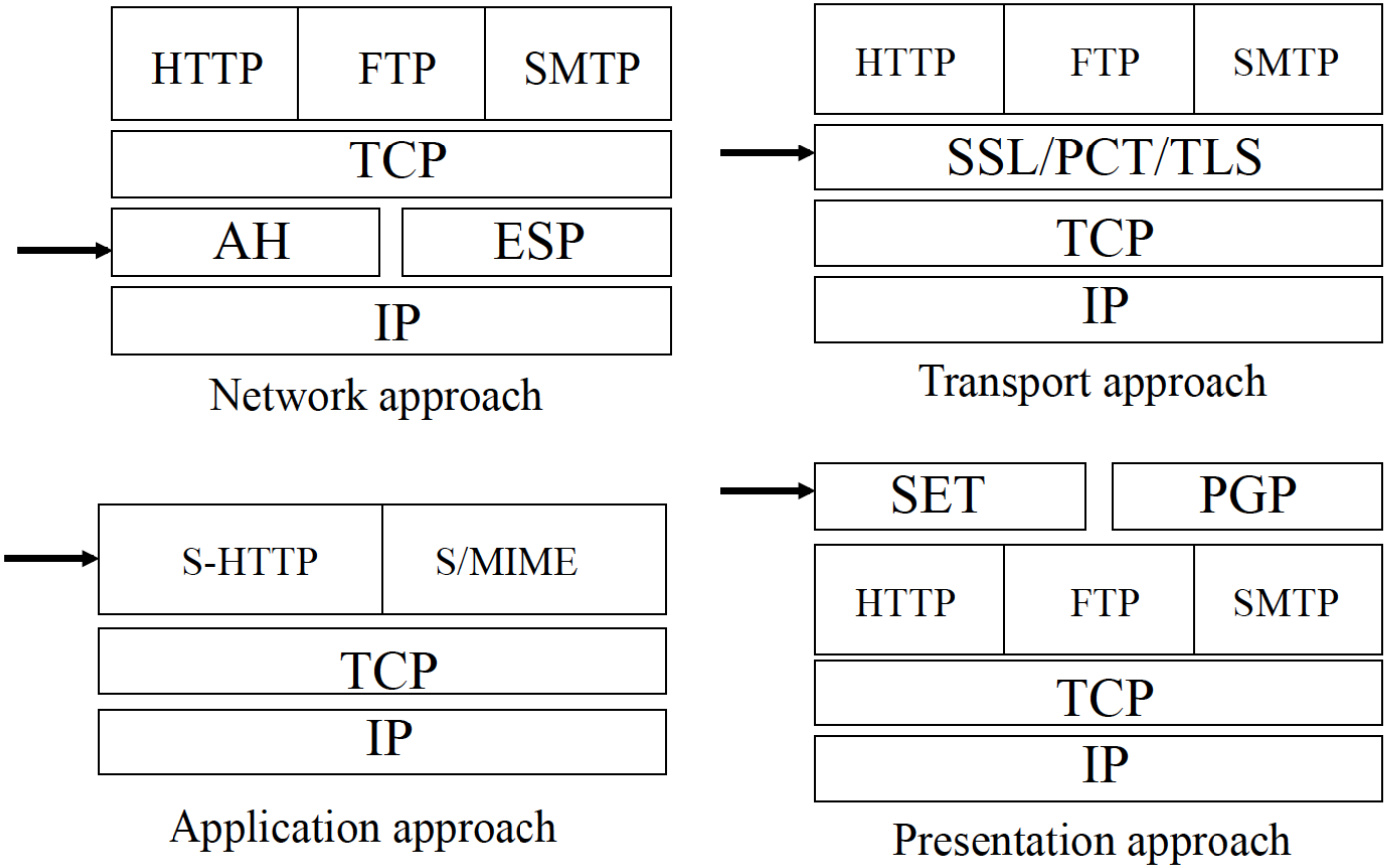
- Autenticità della provenienza dei pacchetti (proteggerci dallo spoofing e dalla ripudiazione dei messaggi). Ci sono due metodi: ricorrere ad una autorità fidata (si dice "terza" rispetto a chi comunica sulla rete) oppure identificarsi direttamente con canali diversi e diretti.
- Integrità dei pacchetti (assenza di alterazioni deliberate).
- Mancanza di riservatezza (vulnerabilità all'eavesdropping)

Problemi da risolvere per Internet

- Autenticità della provenienza dei pacchetti (proteggerci dallo spoofing e dalla ripudiazione dei messaggi). Ci sono due metodi: ricorrere ad una autorità fidata (si dice "terza" rispetto a chi comunica sulla rete) oppure identificarsi direttamente con canali diversi e diretti.
- Integrità dei pacchetti (assenza di alterazioni deliberate).
- Mancanza di riservatezza (vulnerabilità all'eavesdropping)
- Ci sono moltissime soluzioni (dispositivi di sicurezza) per i vari problemi.

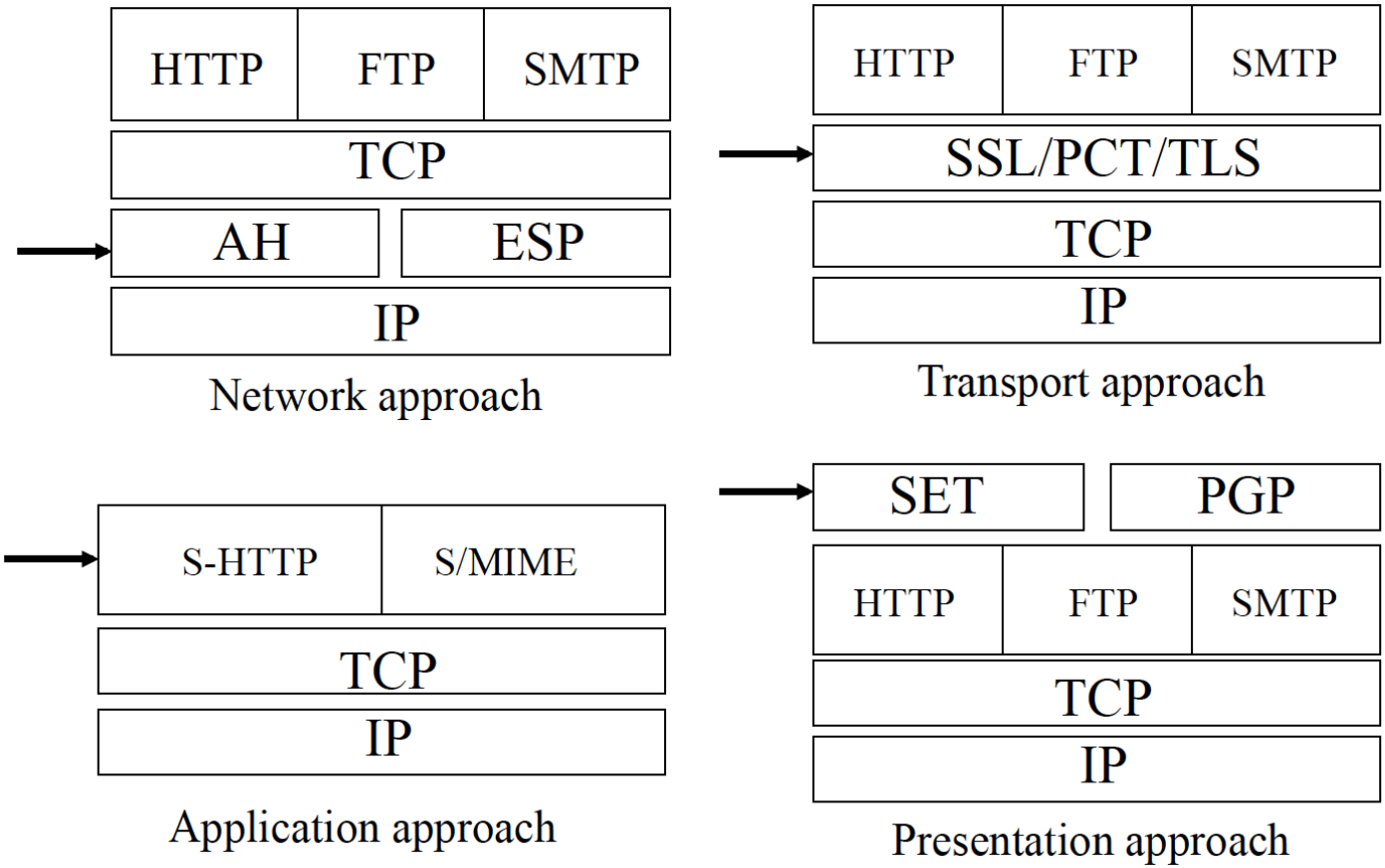
Schemi di locazione dei dispositivi di cifratura di rete

- Questo schema illustra le collocazioni tipiche dei dispositivi di sicurezza (cifratura) utilizzabili in rete. I diversi metodi coesistono e li utilizziamo per le diverse necessità:



Schemi di locazione dei dispositivi di cifratura di rete

- Questo schema illustra le collocazioni tipiche dei dispositivi di sicurezza (cifratura) utilizzabili in rete. I diversi metodi coesistono e li utilizziamo per le diverse necessità:



- Il nome dell'approccio dipende dallo strato in cui si applicano i dispositivi di sicurezza.

Significati degli acronimi

- SMTP (Simple Mail Transfer Protocol) è lo standard più usato in Internet per la trasmissione della posta elettronica (e-mail).

Significati degli acronimi

- SMTP (Simple Mail Transfer Protocol) è lo standard più usato in Internet per la trasmissione della posta elettronica (e-mail).
- TLS (Transport Layer Security) (SSL Secure Socket Layer è il precursore).

Significati degli acronimi

- SMTP (Simple Mail Transfer Protocol) è lo standard più usato in Internet per la trasmissione della posta elettronica (e-mail).
- TLS (Transport Layer Security) (SSL Secure Socket Layer è il precursore).
- SET (Secure Electronic Transaction)

Significati degli acronimi

- SMTP (Simple Mail Transfer Protocol) è lo standard più usato in Internet per la trasmissione della posta elettronica (e-mail).
- TLS (Transport Layer Security) (SSL Secure Socket Layer è il precursore).
- SET (Secure Electronic Transaction)
- HTTPS (HyperText Transfer Protocol over Secure Socket Layer)

Significati degli acronimi

- SMTP (Simple Mail Transfer Protocol) è lo standard più usato in Internet per la trasmissione della posta elettronica (e-mail).
- TLS (Transport Layer Security) (SSL Secure Socket Layer è il precursore).
- SET (Secure Electronic Transaction)
- HTTPS (HyperText Transfer Protocol over Secure Socket Layer)
- PGP (Pretty Good Privacy) è il metodo più usato per le comunicazioni cifrate (esiste OpenPGP open source della GNU).

Significati degli acronimi

- SMTP (Simple Mail Transfer Protocol) è lo standard più usato in Internet per la trasmissione della posta elettronica (e-mail).
- TLS (Transport Layer Security) (SSL Secure Socket Layer è il precursore).
- SET (Secure Electronic Transaction)
- HTTPS (HyperText Transfer Protocol over Secure Socket Layer)
- PGP (Pretty Good Privacy) è il metodo più usato per le comunicazioni cifrate (esiste OpenPGP open source della GNU).
- S/MIME significa Secure MIME (Multipurpose Internet Mail Extensions) è uno standard per la cifratura a chiave pubblica e firma digitale di messaggi di posta elettronica (in formato MIME RFC 1341 - Standard di IEFT), consente di aggiungere contenuti multimediali (suono, video) alla posta elettronica.

Significati degli acronimi

- SMTP (Simple Mail Transfer Protocol) è lo standard più usato in Internet per la trasmissione della posta elettronica (e-mail).
- TLS (Transport Layer Security) (SSL Secure Socket Layer è il precursore).
- SET (Secure Electronic Transaction)
- HTTPS (HyperText Transfer Protocol over Secure Socket Layer)
- PGP (Pretty Good Privacy) è il metodo più usato per le comunicazioni cifrate (esiste OpenPGP open source della GNU).
- S/MIME significa Secure MIME (Multipurpose Internet Mail Extensions) è uno standard per la cifratura a chiave pubblica e firma digitale di messaggi di posta elettronica (in formato MIME RFC 1341 - Standard di IEFT), consente di aggiungere contenuti multimediali (suono, video) alla posta elettronica.
- AH (Authentication Header): l'intestazione di autenticazione,

Significati degli acronimi

- SMTP (Simple Mail Transfer Protocol) è lo standard più usato in Internet per la trasmissione della posta elettronica (e-mail).
- TLS (Transport Layer Security) (SSL Secure Socket Layer è il precursore).
- SET (Secure Electronic Transaction)
- HTTPS (HyperText Transfer Protocol over Secure Socket Layer)
- PGP (Pretty Good Privacy) è il metodo più usato per le comunicazioni cifrate (esiste OpenPGP open source della GNU).
- S/MIME significa Secure MIME (Multipurpose Internet Mail Extensions) è uno standard per la cifratura a chiave pubblica e firma digitale di messaggi di posta elettronica (in formato MIME RFC 1341 - Standard di IEFT), consente di aggiungere contenuti multimediali (suono, video) alla posta elettronica.
- AH (Authentication Header): l'intestazione di autenticazione,
- ESP (Encapsulating Security Payload) la sicurezza dell'incapsulamento del payload, .

Internet Sicura

- La sigla IPsec indica la sicurezza del protocollo Internet (IP Security). Corrisponde all'approccio Internet (Network approach figura precedente). La sicurezza si mette al livello IP. Lo standard è definito in RFC 4301 (dello Internet Engineering Task Force - IETF).

Internet Sicura

- La sigla IPsec indica la sicurezza del protocollo Internet (IP Security). Corrisponde all'approccio Internet (Network approach figura precedente). La sicurezza si mette al livello IP. Lo standard è definito in RFC 4301 (dello Internet Engineering Task Force - IETF).
- IPsec è uno standard che definisce le modalità con cui utilizzare e combinare i dispositivi di sicurezza che abbiamo studiato (autenticazione, cifratura, hash function, meccanismi scambio chiavi etc) per ottenere dei livelli di sicurezza predefiniti.

Internet Sicura

- La sigla IPsec indica la sicurezza del protocollo Internet (IP Security). Corrisponde all'approccio Internet (Network approach figura precedente). La sicurezza si mette al livello IP. Lo standard è definito in RFC 4301 (dello Internet Engineering Task Force - IETF).
- IPsec è uno standard che definisce le modalità con cui utilizzare e combinare i dispositivi di sicurezza che abbiamo studiato (autenticazione, cifratura, hash function, meccanismi scambio chiavi etc) per ottenere dei livelli di sicurezza predefiniti.
- Altre metodologie invece utilizzano i dispositivi di sicurezza al livello applicativo (https, TSL).

Internet Sicura

- La sigla IPsec indica la sicurezza del protocollo Internet (IP Security). Corrisponde all'approccio Internet (Network approach figura precedente). La sicurezza si mette al livello IP. Lo standard è definito in RFC 4301 (dello Internet Engineering Task Force - IETF).
- IPsec è uno standard che definisce le modalità con cui utilizzare e combinare i dispositivi di sicurezza che abbiamo studiato (autenticazione, cifratura, hash function, meccanismi scambio chiavi etc) per ottenere dei livelli di sicurezza predefiniti.
- Altre metodologie invece utilizzano i dispositivi di sicurezza al livello applicativo (https, TSL).
- Utilizzando IPsec la sicurezza si applica ad ogni pacchetto (datagramma) e gli applicativi non necessitano ulteriori dispositivi.

Internet Sicura

- La sigla IPsec indica la sicurezza del protocollo Internet (IP Security). Corrisponde all'approccio Internet (Network approach figura precedente). La sicurezza si mette al livello IP. Lo standard è definito in RFC 4301 (dello Internet Engineering Task Force - IETF).
- IPsec è uno standard che definisce le modalità con cui utilizzare e combinare i dispositivi di sicurezza che abbiamo studiato (autenticazione, cifratura, hash function, meccanismi scambio chiavi etc) per ottenere dei livelli di sicurezza predefiniti.
- Altre metodologie invece utilizzano i dispositivi di sicurezza al livello applicativo (https, TSL).
- Utilizzando IPsec la sicurezza si applica ad ogni pacchetto (datagramma) e gli applicativi non necessitano ulteriori dispositivi.
- IPsec è integrato automaticamente in IPv6 (nuovo standard di indirizzamento IP), ma non in IPv4.

Componenti base di IPsec

- Il protocollo si basa su due diversi sotto-protocolli che consentono lo scambio delle chiavi iniziale per l'instaurazione della trasmissione cifrata e i protocolli che effettuano la cifratura.

Componenti base di IPsec

- Il protocollo si basa su due diversi sotto-protocolli che consentono lo scambio delle chiavi iniziale per l'instaurazione della trasmissione cifrata e i protocolli che effettuano la cifratura.
- La cifratura può seguire due schemi (e protocolli corrispondenti): l'intestazione di autenticazione, Authentication Header (AH) RFC 2402 e la sicurezza dell'incapsulamento del payload, Encapsulating Security Payload (ESP) RFC 2406.

Componenti base di IPsec

- Il protocollo si basa su due diversi sotto-protocolli che consentono lo scambio delle chiavi iniziale per l'instaurazione della trasmissione cifrata e i protocolli che effettuano la cifratura.
- La cifratura può seguire due schemi (e protocolli corrispondenti): l'intestazione di autenticazione, Authentication Header (AH) RFC 2402 e la sicurezza dell'incapsulamento del payload, Encapsulating Security Payload (ESP) RFC 2406.
- AH è un protocollo più semplice che fornisce autenticazione del mittente e verifica di integrità del messaggio, ma non garantisce la confidenzialità ed è il protocollo IP 51. Si spedisce il messaggio in chiaro e la hash function del payload seguito dalla chiave condivisa. Protegge contro attacchi reply (perché l'header è diverso anche se la cifratura della password è corretta).

Componenti base di IPsec

- Il protocollo si basa su due diversi sotto-protocolli che consentono lo scambio delle chiavi iniziale per l'instaurazione della trasmissione cifrata e i protocolli che effettuano la cifratura.
- La cifratura può seguire due schemi (e protocolli corrispondenti): l'intestazione di autenticazione, Authentication Header (AH) RFC 2402 e la sicurezza dell'incapsulamento del payload, Encapsulating Security Payload (ESP) RFC 2406.
- AH è un protocollo più semplice che fornisce autenticazione del mittente e verifica di integrità del messaggio, ma non garantisce la confidenzialità ed è il protocollo IP 51. Si spedisce il messaggio in chiaro e la hash function del payload seguito dalla chiave condivisa. Protegge contro attacchi reply (perché l'header è diverso anche se la cifratura della password è corretta).
- ESP fornisce invece autenticazione, confidenzialità e controllo di integrità del messaggio ed è il protocollo IP 50. Per questi

Protocollo IKE

- Entrambi AH e ESP richiedono la condivisione di una chiave. Lo scambio delle chiavi si realizza tramite il protocollo IKE RFC 2409.

Protocollo IKE

- Entrambi AH e ESP richiedono la condivisione di una chiave. Lo scambio delle chiavi si realizza tramite il protocollo IKE RFC 2409.
- IKE (Internet key exchange) è l'insieme dei protocolli più diffusi (in IPsec) per lo scambio delle chiavi. Lo scopo è quello di scambiarsi informazioni segrete condivise utilizzando un canale non protetto.

Protocollo IKE

- Entrambi AH e ESP richiedono la condivisione di una chiave. Lo scambio delle chiavi si realizza tramite il protocollo IKE RFC 2409.
- IKE (Internet key exchange) è l'insieme dei protocolli più diffusi (in IPsec) per lo scambio delle chiavi. Lo scopo è quello di scambiarsi informazioni segrete condivise utilizzando un canale non protetto.
- IKE è un protocollo versatile che può anche usare informazioni condivise pregresse, ma spesso è basato sul meccanismo di Diffie-Hellman.

Certificati digitali

- Un certificato digitale è un documento reperibile per via elettronica che attesta l'associazione univoca tra una chiave pubblica e l'identità di un soggetto.

Certificati digitali

- Un certificato digitale è un documento reperibile per via elettronica che attesta l'associazione univoca tra una chiave pubblica e l'identità di un soggetto.
- Come qualsiasi certificato il valore (l'affidabilità), la veridicità del suo contenuto dipende dal soggetto certificante detta Autorità di certificazione (Certification Authority).

Certificati digitali

- Un certificato digitale è un documento reperibile per via elettronica che attesta l'associazione univoca tra una chiave pubblica e l'identità di un soggetto.
- Come qualsiasi certificato il valore (l'affidabilità), la veridicità del suo contenuto dipende dal soggetto certificante detta Autorità di certificazione (Certification Authority).
- Ad esempio: l'anagrafe garantisce che alla vostra fotografia sulla carta d'identià corrispondano i vostri dati anagrafici (nome, cognome data di nascita). L'erario fa lo stesso con il codice fiscale. Analogamente un'autorità certifica che le chiavi pubbliche disponibili presso i loro repository siano di proprietà di soggetti fisici.

Certificati digitali

- Un certificato digitale è un documento reperibile per via elettronica che attesta l'associazione univoca tra una chiave pubblica e l'identità di un soggetto.
- Come qualsiasi certificato il valore (l'affidabilità), la veridicità del suo contenuto dipende dal soggetto certificante detta Autorità di certificazione (Certification Authority).
- Ad esempio: l'anagrafe garantisce che alla vostra fotografia sulla carta d'identià corrispondano i vostri dati anagrafici (nome, cognome data di nascita). L'erario fa lo stesso con il codice fiscale. Analogamente un'autorità certifica che le chiavi pubbliche disponibili presso i loro repository siano di proprietà di soggetti fisici.
- Per essere certi della origine della certificazione l'Autorità di certificazione cifra i certificati con la propria chiave privata e rende disponibile la propria chiave pubblica.

Messaggio

- I protocolli TCP/IP ed UDP sono universali e coprono attività di ogni genere dal telefono (voice on IP) ad HTTP ed altri applicativi di alto livello.

Messaggio

- I protocolli TCP/IP ed UDP sono universali e coprono attività di ogni genere dal telefono (voice on IP) ad HTTP ed altri applicativi di alto livello.
- Il mondo delle informazioni ufficiali forma una gigantesca rete con dati accessibili in formato html tramite protocollo HTTP.

Messaggio

- I protocolli TCP/IP ed UDP sono universali e coprono attività di ogni genere dal telefono (voice on IP) ad HTTP ed altri applicativi di alto livello.
- Il mondo delle informazioni ufficiali forma una gigantesca rete con dati accessibili in formato html tramite protocollo HTTP.
- L'indicizzazione delle risorse viene svolta prevalentemente al livello name e gestita dai sever di dominio DNS. I motori di ricerca classificano tutte queste informazioni.

Messaggio

- I protocolli TCP/IP ed UDP sono universali e coprono attività di ogni genere dal telefono (voice on IP) ad HTTP ed altri applicativi di alto livello.
- Il mondo delle informazioni ufficiali forma una gigantesca rete con dati accessibili in formato html tramite protocollo HTTP.
- L'indicizzazione delle risorse viene svolta prevalentemente al livello name e gestita dai sever di dominio DNS. I motori di ricerca classificano tutte queste informazioni.
- La struttura della rete rimane anarchica anche a livello name e una enorme quantità di dati fluisce in forma non indicizzata dai motori di ricerca: rete sommersa: (deep web). Una parte di questa viene gestita volutamente in forma riservata: rete oscura (dark web).

Messaggio

- I protocolli TCP/IP ed UDP sono universali e coprono attività di ogni genere dal telefono (voice on IP) ad HTTP ed altri applicativi di alto livello.
- Il mondo delle informazioni ufficiali forma una gigantesca rete con dati accessibili in formato html tramite protocollo HTTP.
- L'indicizzazione delle risorse viene svolta prevalentemente al livello name e gestita dai sever di dominio DNS. I motori di ricerca classificano tutte queste informazioni.
- La struttura della rete rimane anarchica anche a livello name e una enorme quantità di dati fluisce in forma non indicizzata dai motori di ricerca: rete sommersa: (deep web). Una parte di questa viene gestita volutamente in forma riservata: rete oscura (dark web).
- Ad ogni livello della rete (dal datalink, all'applicazioni si possono instaurare diversi dispositivi di sicurezza: abbiamo visto IPSsec al livello IP.