Protocolli per la Sicurezza delle Reti

Pila protocollare ISO/OSI e sicurezza

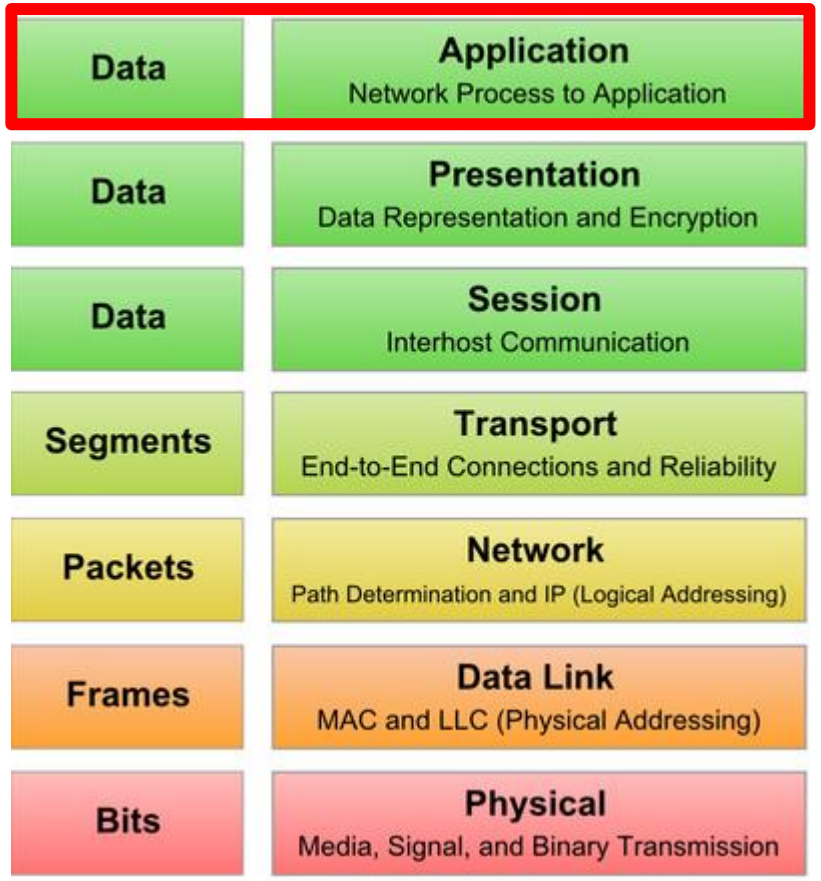
È solo un modello,
non un architettura

Data	**Application** Network Process to Application
Data	**Presentation** Data Representation and Encryption
Data	**Session** Interhost Communication
Segments	**Transport** End-to-End Connections and Reliability
Packets	**Network** Path Determination and IP (Logical Addressing)
Frames	**Data Link** MAC and LLC (Physical Addressing)
Bits	**Physical** Media, Signal, and Binary Transmission

Man mano che scendiamo, aumenta la quantità di informazioni necessarie per la comunicazione

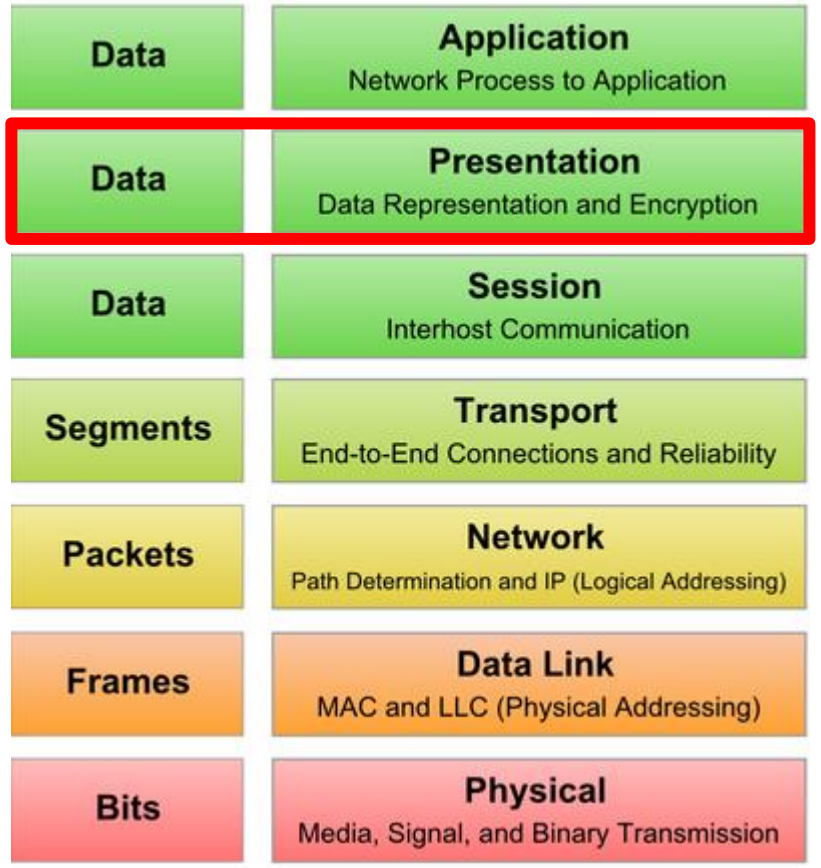
Pila protocollare ISO/OSI e sicurezza

- **Applicazioni** che permettono agli utenti di fruire direttamente dei servizi – Es. Utente che apre Google Chrome e vuole accedere ad un sito, e-mail, trasferimento file



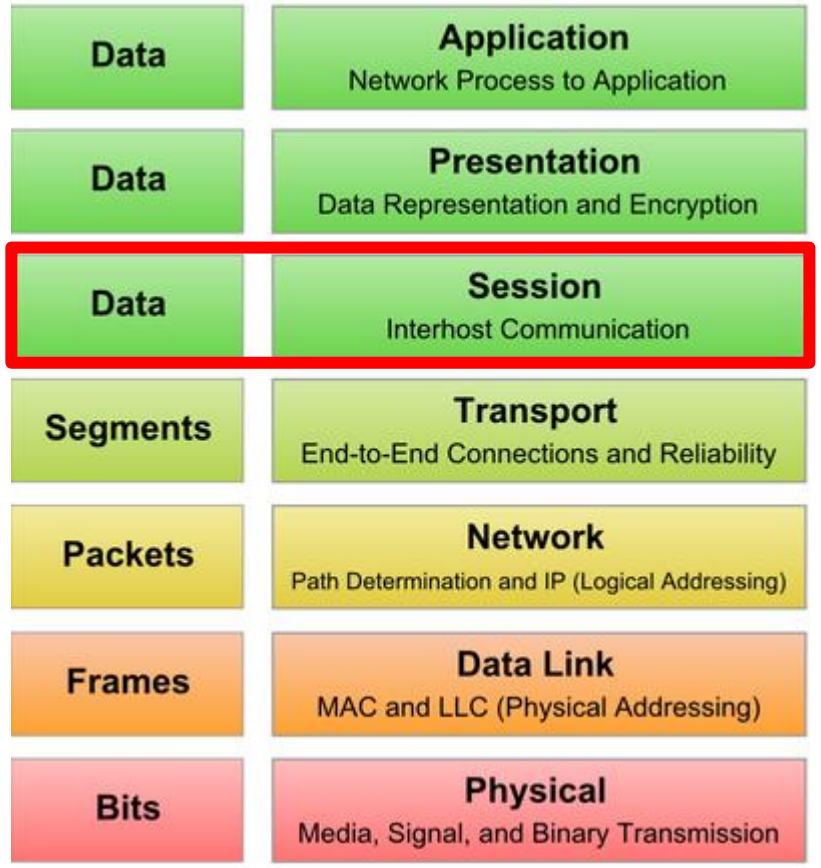
Pila protocollare ISO/OSI e sicurezza

- **Applicazioni** che permettono agli utenti di fruire direttamente dei servizi – Es. Utente che apre Google Chrome e vuole accedere ad un sito, e-mail, trasferimento file
- Si occupa di **rappresentare** i dati in un **formato standard** (sintassi e semantica) – definisce codifica, algoritmo di cifratura, etc.



Pila protocollare ISO/OSI e sicurezza

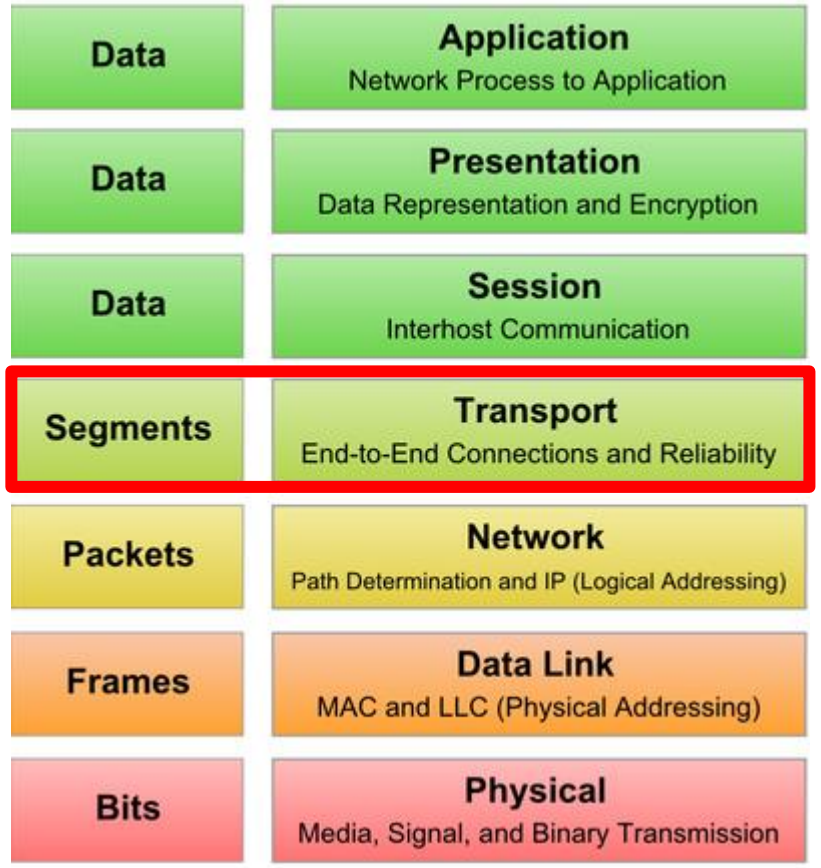
- **Applicazioni** che permettono agli utenti di fruire direttamente dei servizi – Es. Utente che apre Google Chrome e vuole accedere ad un sito, e-mail, trasferimento file
- Si occupa di **rappresentare** i dati in un **formato standard** (sintassi e semantica) – definisce codifica, algoritmo di cifratura, etc.
- Stabilisce una **comunicazione** (logica) tra sistemi diversi – si definiscono regole per aprire, utilizzare, chiudere **connessione** (**sessione**), e **trasferire dati**



Pila protocollare ISO/OSI e sicurezza

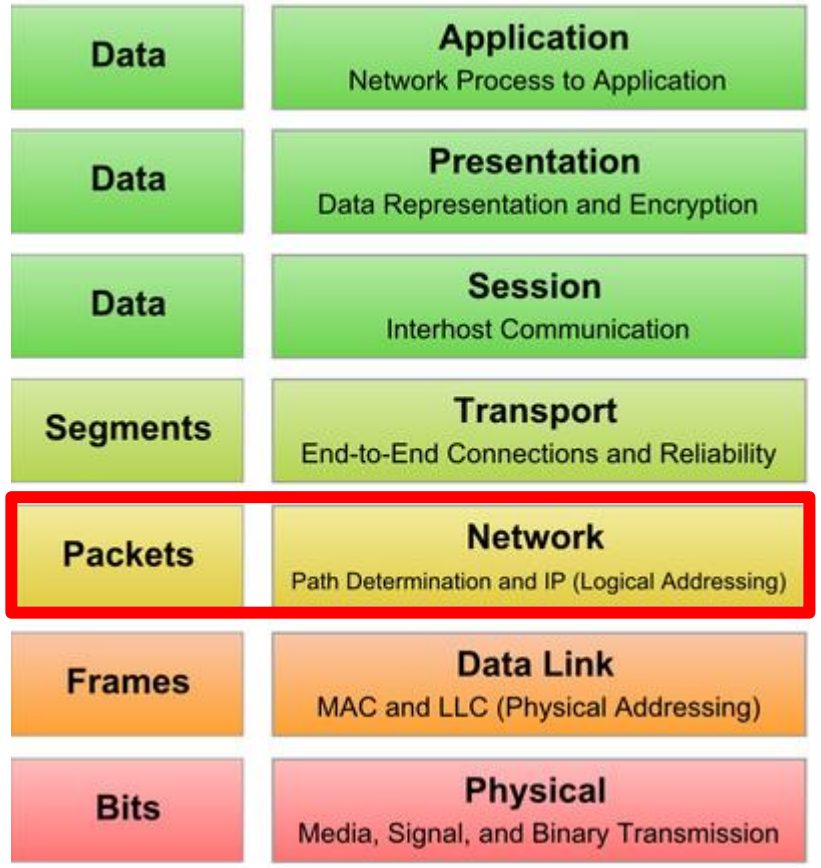
- **Applicazioni** che permettono agli utenti di fruire direttamente dei servizi – Es. Utente che apre Google Chrome e vuole accedere ad un sito, e-mail, trasferimento file
- Si occupa di **rappresentare** i dati in un **formato standard** (sintassi e semantica) – definisce codifica, algoritmo di cifratura, etc.
- Stabilisce una **comunicazione** (logica) tra sistemi diversi – si definiscono regole per aprire, utilizzare, chiudere **connessione** (**sessione**), e **trasferire dati**

- Gestisce la **connessione end-to-end** (tramite la definzione di un canale logico) tra due host remoti, gestisce le **congestioni**, **disassembla e riassembla i dati**



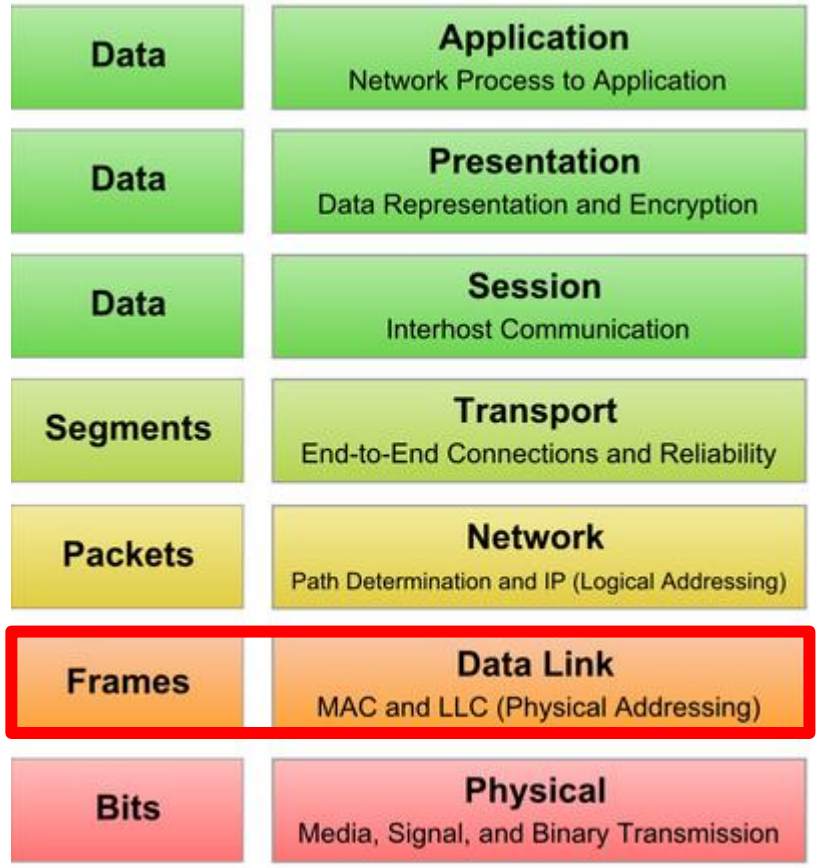
Pila protocollare ISO/OSI e sicurezza

- **Applicazioni** che permettono agli utenti di fruire direttamente dei servizi – Es. Utente che apre Google Chrome e vuole accedere ad un sito, e-mail, trasferimento file
- Si occupa di **rappresentare** i dati in un **formato standard** (sintassi e semantica) – definisce codifica, algoritmo di cifratura, etc.
- Stabilisce una **comunicazione** (logica) tra sistemi diversi – si definiscono regole per aprire, utilizzare, chiudere **connessione** (**sessione**), e **trasferire dati**
- Gestisce la **connessione end-to-end** (tramite la definzione di un canale logico) tra due host remoti, gestisce le **congestioni**, **disassembla e riassembla i dati**
- I **pacchetti** vengono **indirizzati logicamente** su reti geografiche interconnesse e viene scelto il cammino migliore (**routing**)



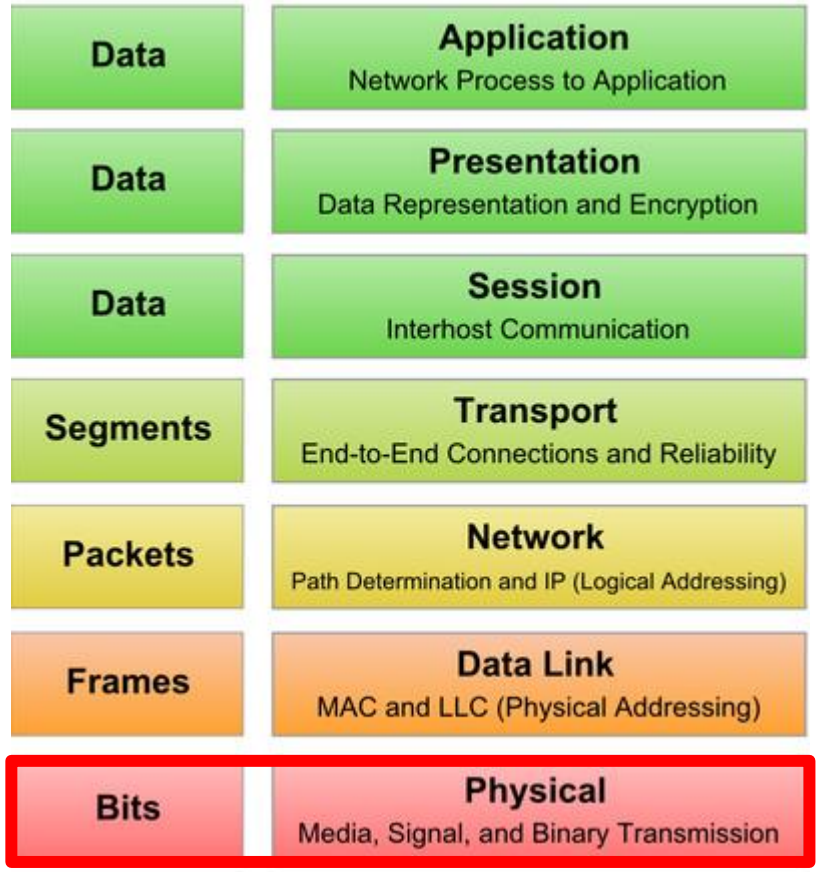
Pila protocollare ISO/OSI e sicurezza

- **Applicazioni** che permettono agli utenti di fruire direttamente dei servizi – Es. Utente che apre Google Chrome e vuole accedere ad un sito, e-mail, trasferimento file
- Si occupa di **rappresentare** i dati in un **formato standard** (sintassi e semantica) – definisce codifica, algoritmo di cifratura, etc.
- Stabilisce una **comunicazione** (logica) tra sistemi diversi – si definiscono regole per aprire, utilizzare, chiudere **connessione** (**sessione**), e **trasferire dati**
- Gestisce la **connessione end-to-end** (tramite la definzione di un canale logico) tra due host remoti, gestisce le **congestioni**, **disassembla e riassembla i dati**
- I **pacchetti** vengono **indirizzati logicamente** su retigeografiche interconnesse e viene scelto il cammino migliore (**routing**)
- Gestisce la **comunicazione** punto punto tra PC della stessa rete (**LAN**) tramiti **indirizzi fisici** (MAC); in ricezione **controlla gli errori** e eventualmente chiede ritrasmissione



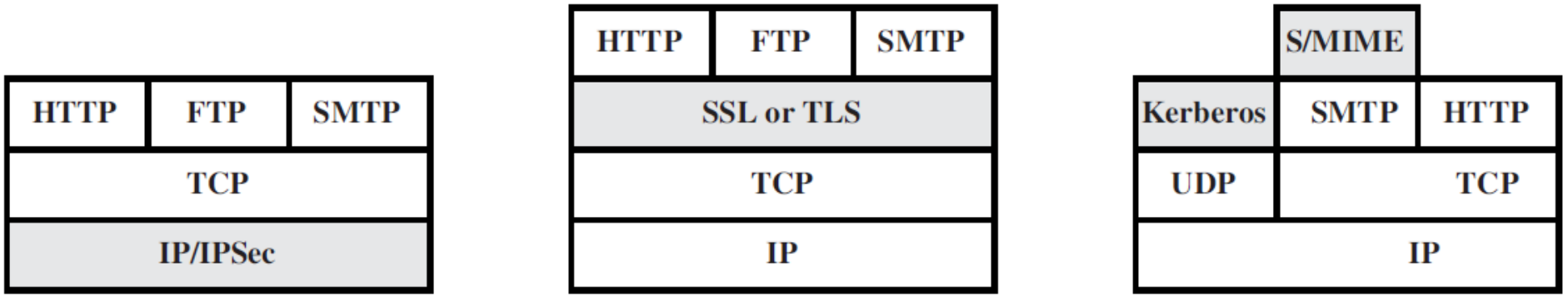
Pila protocollare ISO/OSI e sicurezza

- **Applicazioni** che permettono agli utenti di fruire direttamente dei servizi – Es. Utente che apre Google Chrome e vuole accedere ad un sito, e-mail, trasferimento file
- Si occupa di **rappresentare** i dati in un **formato standard** (sintassi e semantica) – definisce codifica, algoritmo di cifratura, etc.
- Stabilisce una **comunicazione** (logica) tra sistemi diversi – si definiscono regole per aprire, utilizzare, chiudere **connessione** (**sessione**), e **trasferire dati**
- Gestisce la **connessione end-to-end** (tramite la definzione di un canale logico) tra due host remoti, gestisce le **congestioni**, **disassembla e riassembla i dati**
- I **pacchetti** vengono **indirizzati logicamente** su reti interconnesse e viene scelto il cammino migliore (**routing**)
- Gestisce la **comunicazione** punto punto tra PC della stessa rete (**LAN**) tramiti **indirizzi fisici** (MAC); in ricezione **controlla gli errori** e eventualmente chiede ritrasmissione
- **Trasmettere** i dati non strutturati (**bit**) sul **collegamento fisico** (tipologia segnale, caratteristiche cavi, etc.)



Un esempio nella vita reale

Approcci alla sicurezza delle reti



(a) Network level (b) Transport level (c) Application level

Qualche volta i protocolli di sicurezza lavorano **“on top of”** determinati livelli della pila ISO/OSI, qualche volta lavorano proprio su determinati livelli

Sicurezza a livello Applicazione

- La comunicazione tra applicazioni può includere funzioni di **sicurezza custom**, nel senso che ogni applicazione applica la sua sicurezza, o standard

- Es: standard **S/MIME** (Secure / Multipurpose Internet Mail Extensions) per la **sicurezza della posta elettronica** (non è la PEC!)
  - Supporta **crittografia a chiave pubblica** e **firma digitale**
  - È incluso nella maggior parte dei moderni software di posta elettronica

End-to-end encryption (E2EE)

- Denota comunicazioni che **non vengono mai decifrate** durante il trasferimento da mittente a destinatario

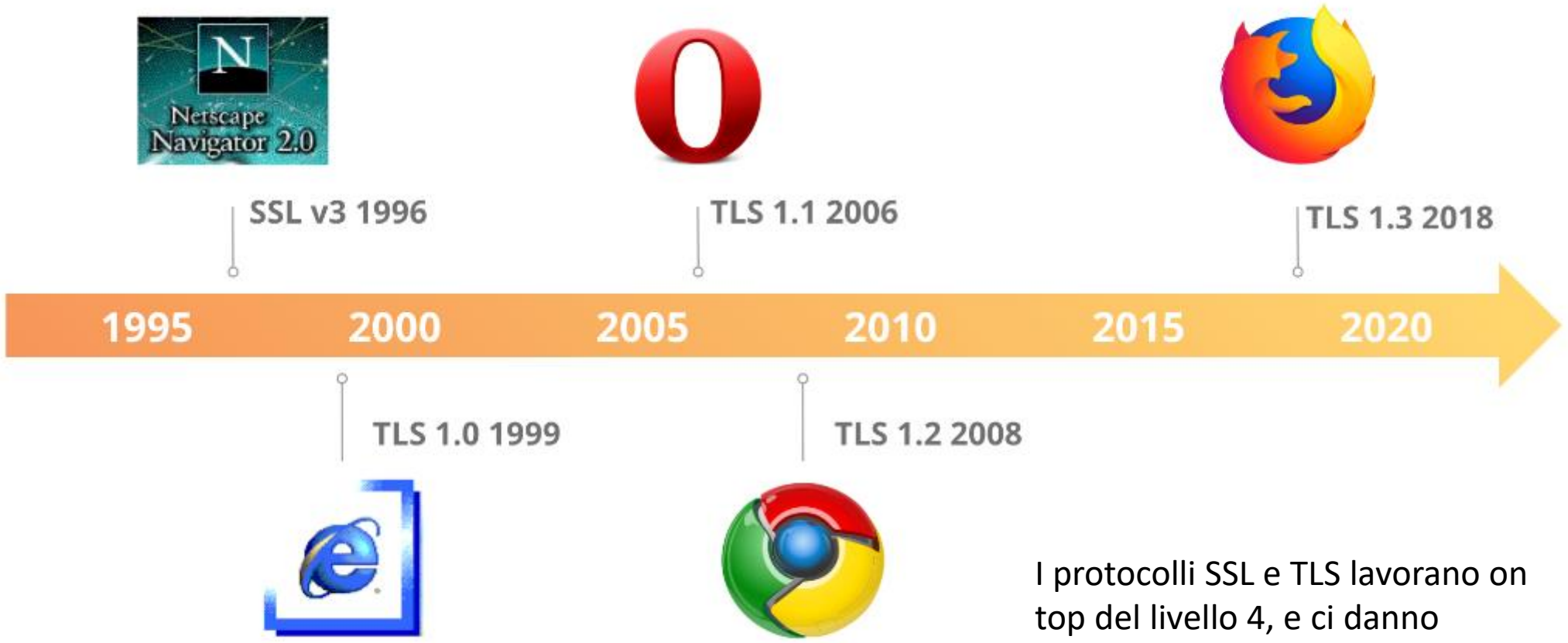
- Proposto nel 2003
- Solo gli utenti che comunicano possono leggere i messaggi

- Mira ad impedire le **intercettazioni**, **incluse** quelle effettuate dallo stesso **fornitore del servizio** o dell'infrastruttura di rete

- Spesso implementato a livello di applicazione

- Eticamente, è corretto indebolire la crittografia per agevolare le intercettazioni per scopi giudiziari?

Sicurezza "on top of" il livello Trasporto



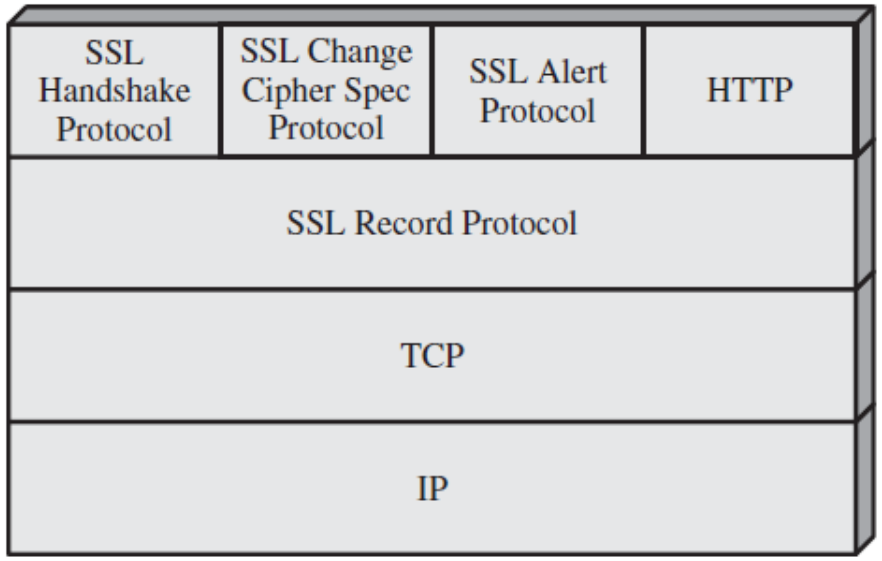
I protocolli SSL e TLS lavorano on top del livello 4, e ci danno connessioni sicure standard

Secure Socket Layer: storia

- **1994**: SSL introdotto da Netscape per servizi web sicuri (1.0 mai rilasciato per problemi di sicurezza)
- **1995**: SSL 2.0 rilasciato
- **1996**: SSL 3.0 rilasciato (versione «stabile»)
- **1999**: **TLS** (**Transport Layer Security**) 1.0 rilasciato come standard IETF (RFC 2246): è un upgrade di SSL 3.0 ma non è interoperabile con SSL 3.0, sebbene le differenze tra i due siano limitate
- **2006**: TLS 1.1 (RFC 4346) migliora TLS 1.0 (protezione contro attacchi a Cipher Block Chaining…)
- **2008**: TLS 1.2 (RFC 5246) rilasciato con diverse modifiche (aggiunte funzioni pseudo-random specifiche, aggiunte modalità AES, rimossi IDEA e DES ed altro)
- **2011**: IETF annuncia che SSL 2.0 è deprecato (RFC 6176) per problemi di sicurezza
- **2015**: IETF annuncia che **SSL** 3.0 è **deprecato** (RFC 7568) e qualsiasi versione di TLS garantisce maggiore sicurezza di SSL
- **2018**: TLS 1.3 (RFC 8446) rilasciato con modifiche rilevanti per semplificare il protocollo (rimosse SHA-1, MD5, RC4, DES e 3DES, handshake abbreviato, cifratura delle informazioni sul server, aggiunta della firma RSA-PSS…)

Protocolli SSL/TLS

- Due livelli protocollari:
  - **Record Protocol**: fornisce la base per servizi sicuri (**compressione, cifratura simmetrica**)
  - **Handshake Protocol**, **Change Cipher Spec Protocol** e **Alert Protocol** svolgono funzioni di gestione di SSL/TLS appoggiandosi sul record protocol



- Protocolli di livello 7 (ad es. HTTP, FTP…) poggiano su SSL/TLS per ottenere sicurezza (ad es. HTTP + SSL/TLS = HTTPS per navigazione web sicura)

Protocolli SSL

- **SSL Handshake Protocol**: ha lo scopo di far partire la sessione tra client e server, di creare la connessione sicura da zero:
  - Negoziazione dei parametri di sicurezza
  - Uso dei certificati
  - Scambio delle chiavi
  - Attivazione funzioni di sicurezza
  - …

Protocolli SSL

- **SSL Record Protocol** ha lo scopo di fornire due servizi:
  - **Confidenzialità**: cifratura dei dati sfruttando una chiave segreta definita dall'Handshake Protocol
  - **Integrità**: controllo di integrità e autenticità dei dati tramite un message authentication code (MAC) che sfrutta una chiave segreta definita dall'Handshake Protocol

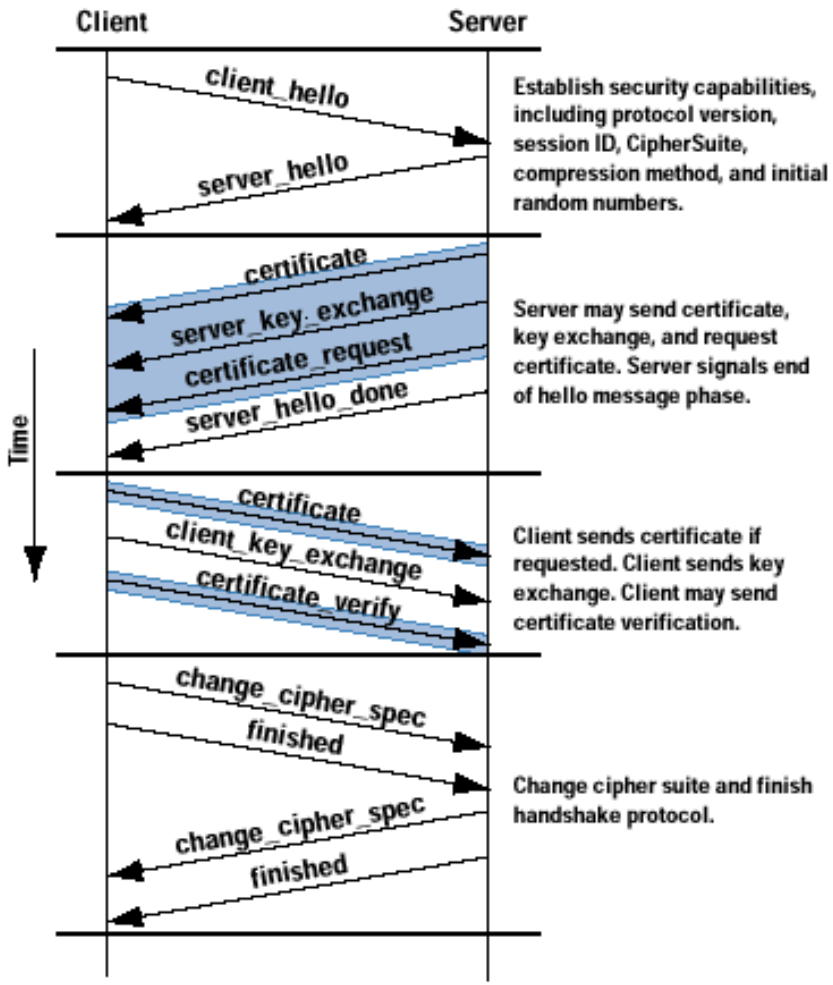
Protocolli SSL

- **SSL Change Cipher Spec Protocol** ha un solo messaggo di 1 byte, che vale 1
- Comunica il cambio di stato della connessione SSL
- Permette di **aggiornare** la "**cipher suite**", ovvero il set di parametri di sicurezza

Protocolli SSL

- **SSL Alert Protocol** serve a trasmettere allarmi relativi alla connessione SSL (controllo integrità fallito, certificato non valido, messaggio inatteso, …)
- Due tipi di allarmi: "warning" (1) oppure "fatal" (2)
- Se l'allarme è fatale, SSL termina immediatamente la connessione

Protocolli SSL – Focus sull'SSL Handshake Protocol

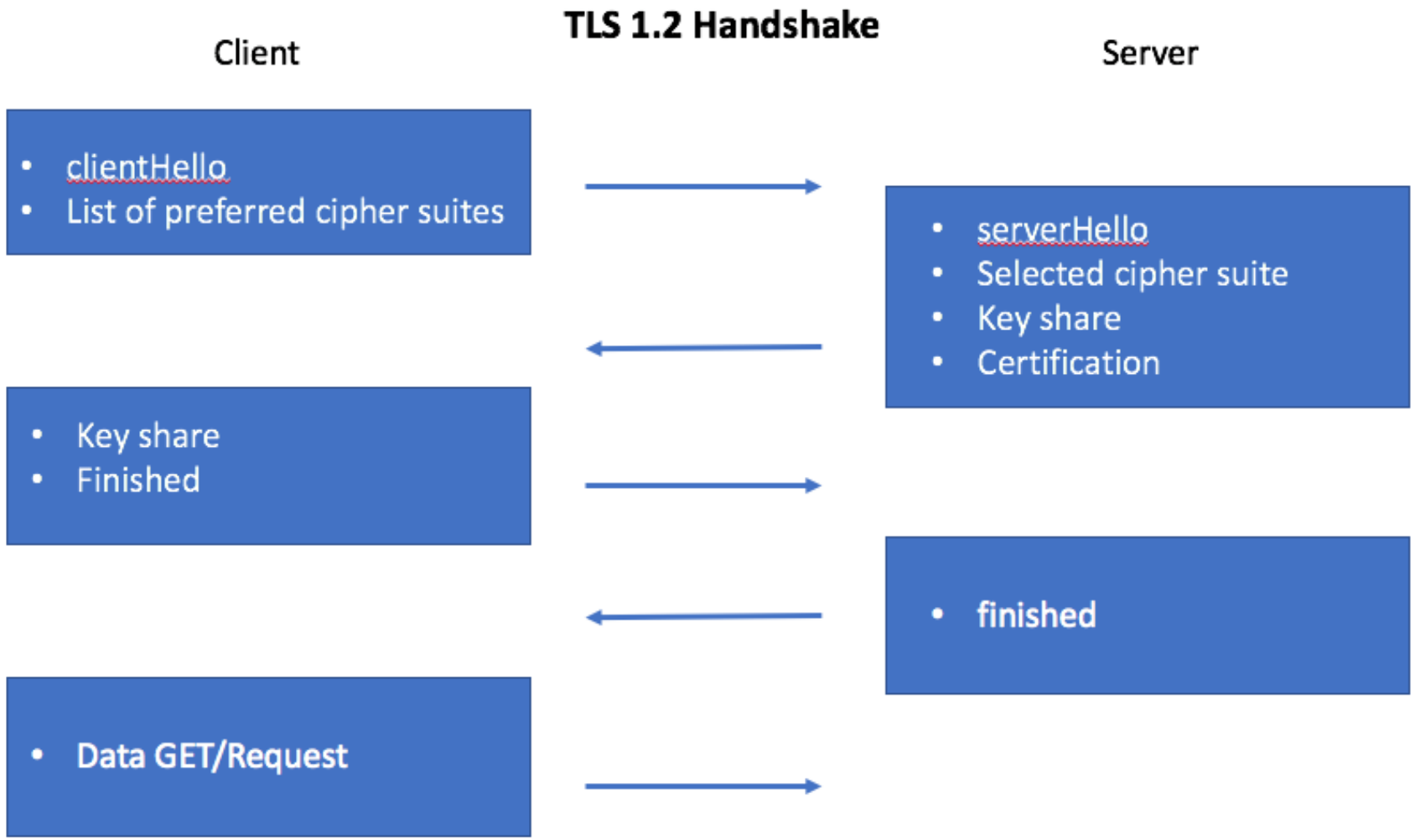


Transport Layer Security

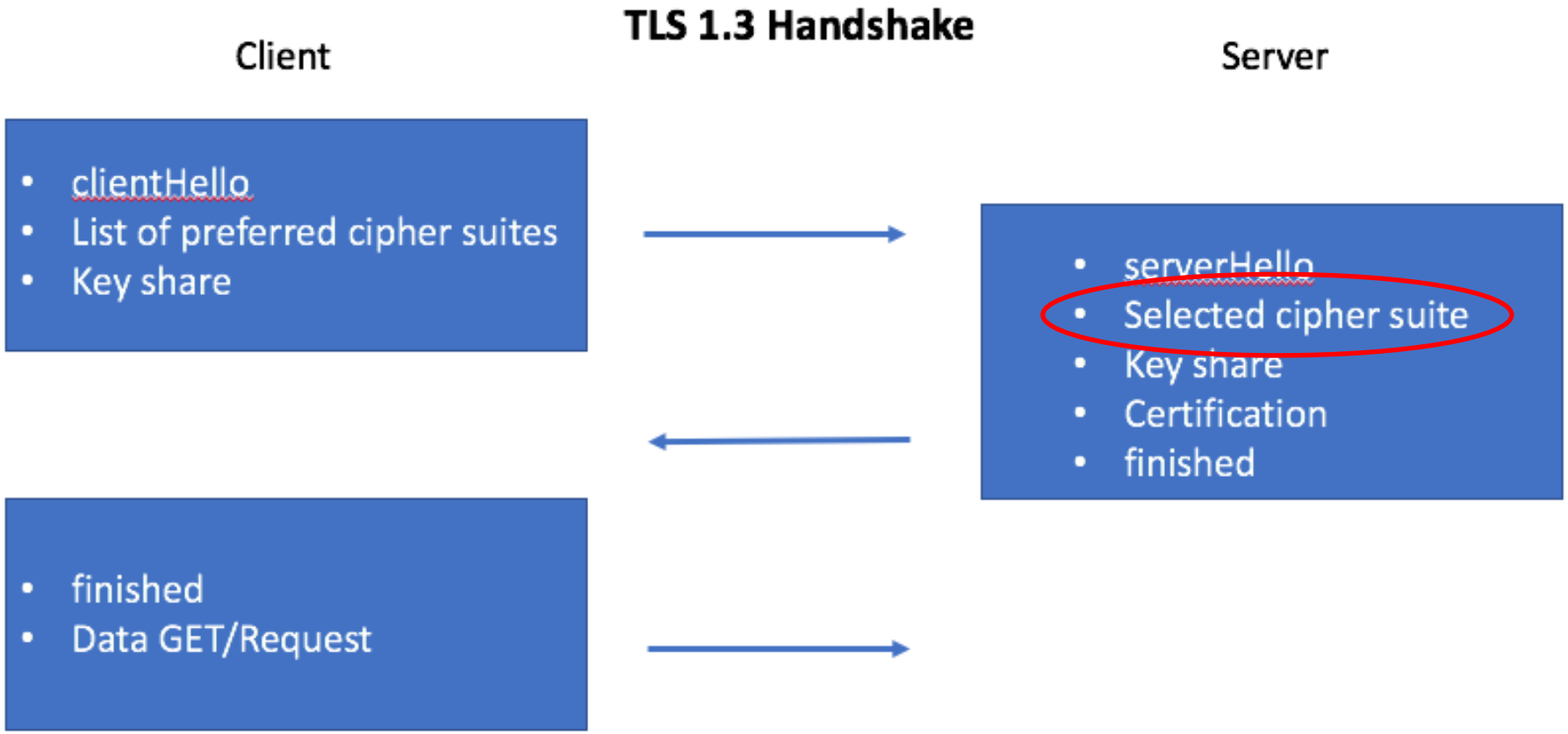
- TLS è un'iniziativa di standardizzazione IETF avente lo scopo di produrre una versione standard di SSL

- TLS include diverse migliorie rispetto ad SSL (ad esempio fa uso dell'algoritmo HMAC definito in RFC 2104 e di funzioni pseudorandom per espandere le chiavi segrete)

Handshake TLS 1.2



Handshake TLS 1.3



HTTPS (HTTP over SSL)

- Combinazione di HTTP e SSL per implementare comunicazioni sicure tra un web browser ed un web server
- Protocollo incluso in tutti i browser moderni (ma l'effettivo uso dipende dal supporto da parte del server)
- Quando è usato, l'url cambia da http://... a https://...

HTTPS (HTTP over SSL)

- Quando HTTPS è usato, i seguenti elementi della comunicazione sono cifrati:
  - URL delle pagine richieste dal client
  - contenuti delle pagine
  - contenuti dei moduli compilati dall'utente
  - cookies scambiati tra client e server
  - contenuti delle intestazioni HTTP

- Non ci sono differenze fondamentali tra HTTP over SSL e HTTP over TLS (entrambi sono denominati HTTPS)

Sicurezza a livello rete: IP security

- Nel 1994, la Internet Architecture Board (IAB) emise un rapporto intitolato “Security in the Internet Architecture” (RFC 1636)
- Esso evidenziava la necessità di **rendere sicure le infrastrutture di rete** rispetto all'uso ed al controllo non autorizzato del traffico di rete
- Si esprimeva la necessità di rendere sicuro il **traffico tra due end-user** (un PC in Italia e uno negli USA) utilizzando tecniche di autenticazione e cifratura
- Tali tecniche sono state incluse nella versione più recente del protocollo IP (IPv6)
- Esse sono state progettate per essere usate anche con la versione precedente del protocollo IP (IPv4)

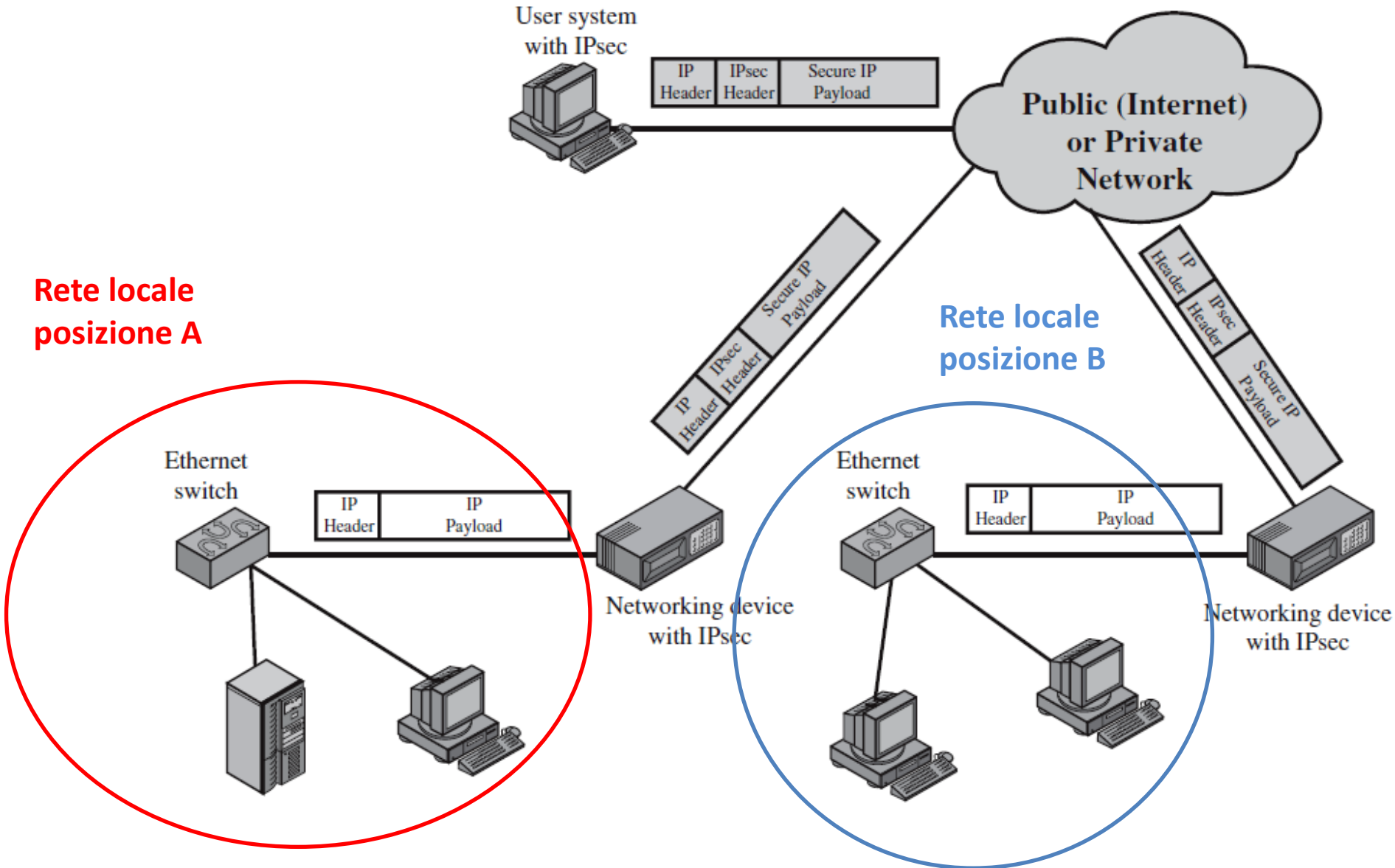
Esempi di uso di IPsec

- Realizzazione di una rete privata virtuale (**VPN**) tramite Internet o altra rete pubblica, evitando la necessità di reti dedicate (non ci sono cavi, ma cavi virtuali che si agganciano alle connessioni internet in modo sicuro)

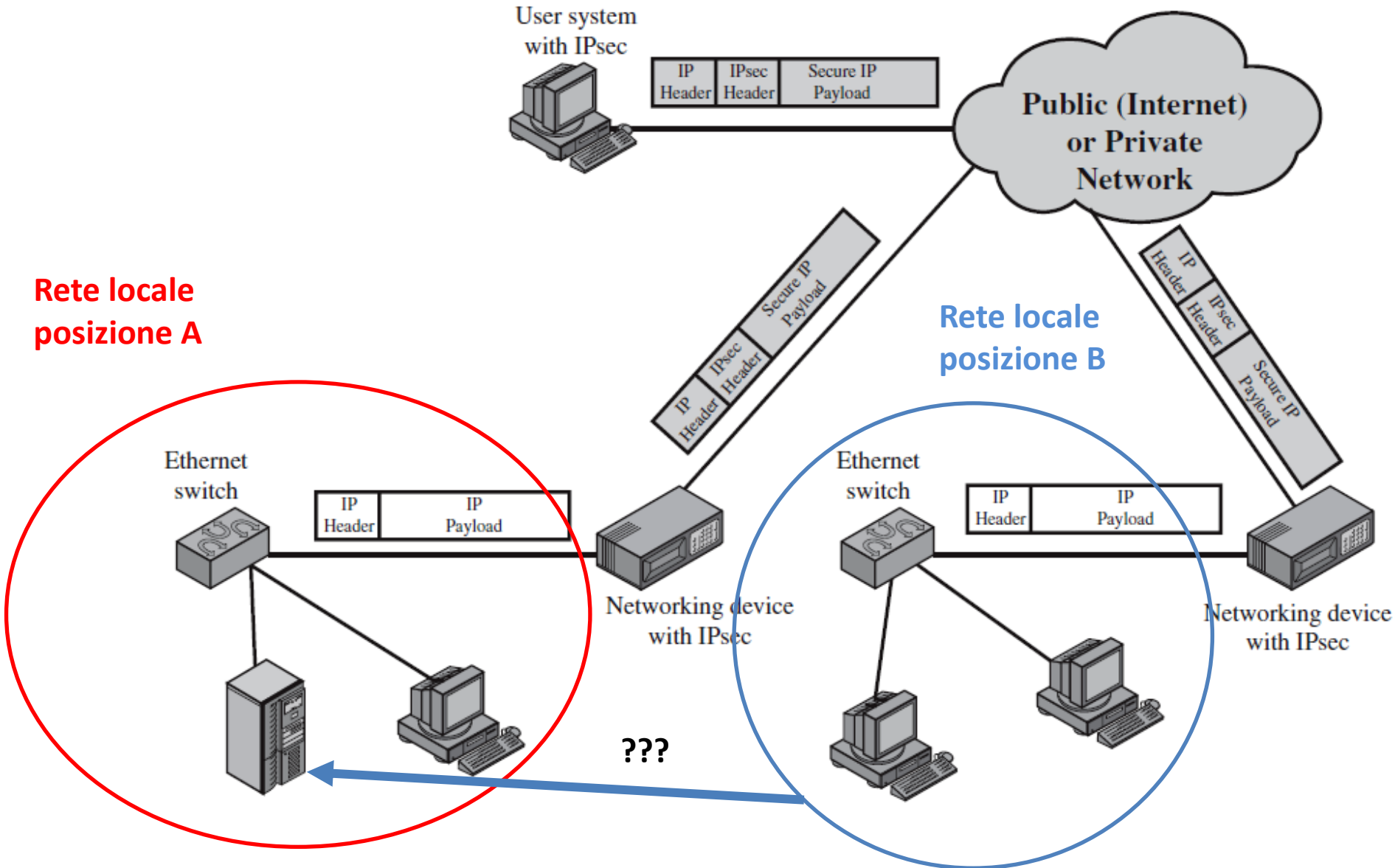
- Accesso remoto sicuro tramite Internet ad una rete privata

- Aumento della sicurezza nelle applicazioni di commercio elettronico e altri servizi online

Uso tipico di IPsec (VPN)

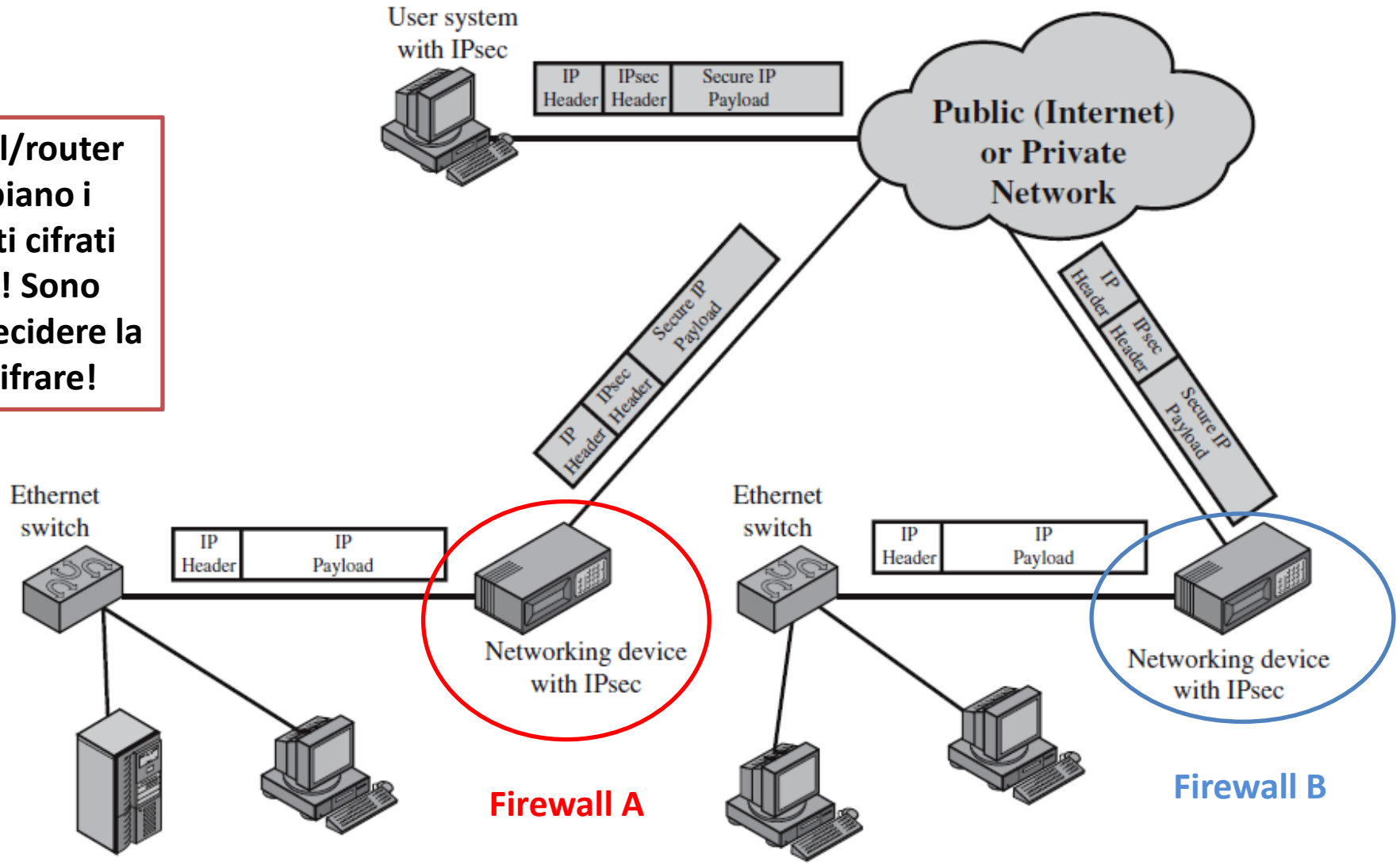


Uso tipico di IPsec (VPN)



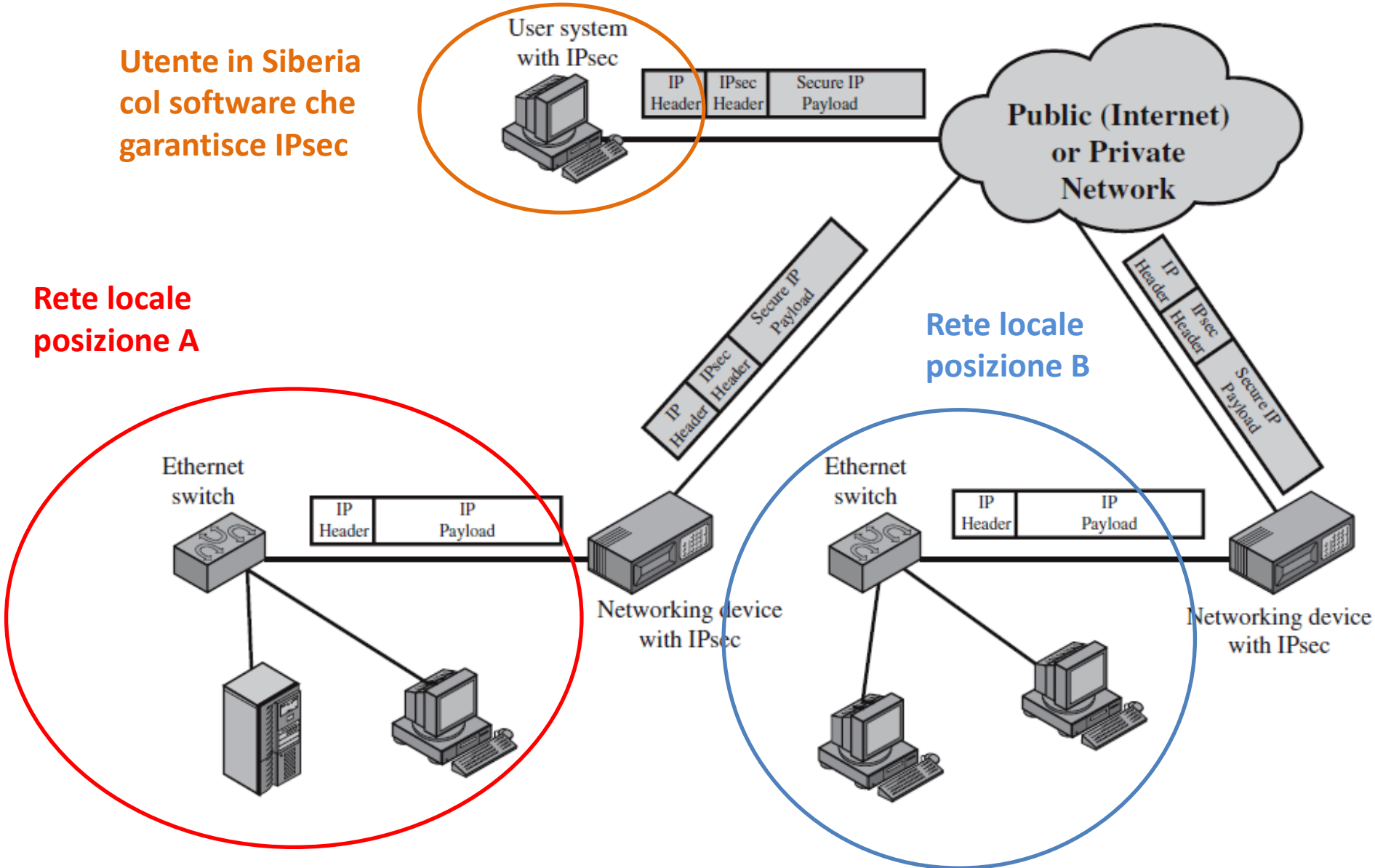
Uso tipico di IPsec (VPN)

I firewall/router si scambiano i pacchetti cifrati da A a B! Sono loro a decidere la suite e cifrare!



Uso tipico di IPsec (VPN)

Utente in Siberia col software che garantisce IPsec

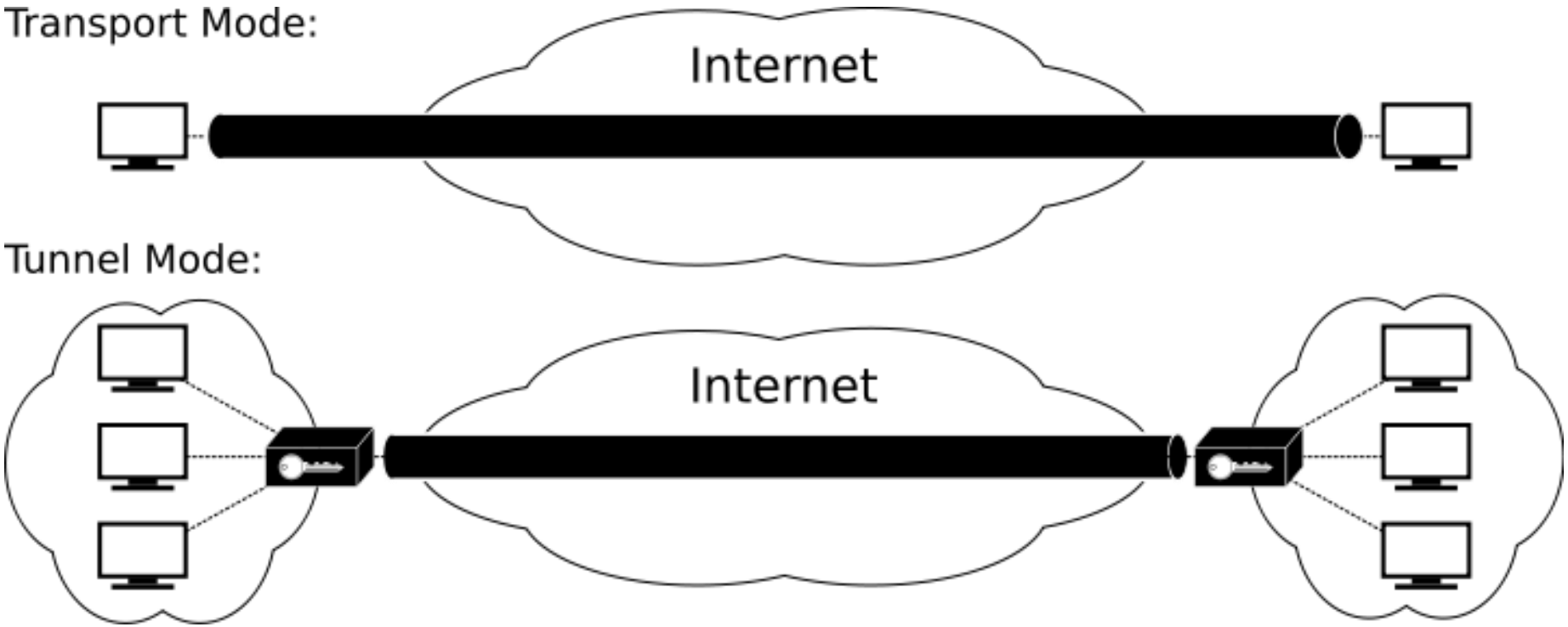


Vantaggi di IPsec

- IPsec fornisce sicurezza a livello IP, quindi coinvolge tutto il **traffico di rete**, senza bisogno di overhead a livelli più alti
- I dispositivi IPsec (router e firewall) perimetrali sono difficili da bypassare
- Lavorando a livello IP, **IPsec è trasparente** per le applicazioni ed i software di livello superiore
- Non serve la conoscenza e gestione di tecniche di sicurezza da parte dell'utente
- Si può utilizzare IPsec anche per singoli utenti o gruppi di utenti all'interno di una rete

Modalità operative IPsec

Si codificano solo i dati, le intestazioni no



Si codifica tutto il pacchetto (VPN)

Sicurezza a livello dati e fisico

- A livello dati: standard IEEE 802.1x che si occupa di controllo accessi dei soggetti (deve accedere alla connessione solo chi può) nelle LAN– poi migliorato nell'IEEE 802.1aa

- A livello fisico: ancora argomento di ricerca

Sicurezza delle Reti Wireless

IEEE 802.11 e SICUREZZA

- Le reti radio sono intrinsecamente meno sicure di quelle cablate
- Lo standard IEEE 802.11 prevedeva come primo protocollo di sicurezza il **WEP** (Wired Equivalent Privacy)
- Il WEP è stato definitivamente abbandonato nel 2001 proprio perché si è dimostrato che non era in grado di garantire la sicurezza delle reti
- Il protocollo che sostituisce e supera WEP è **802.11i**

Attacco al WEP (2001)

Weaknesses in the Key Scheduling Algorithm of RC4

Scott Fluhrer[1], Itsik Mantin[2], and Adi Shamir[2]

[1] Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134
sfluhrer@cisco.com
[2] Computer Science department, The Weizmann Institute, Rehovot 76100, Israel.
{itsik,shamir}@wisdom.weizmann.ac.il

Abstract. In this paper we present several weaknesses in the key scheduling algorithm of RC4, and describe their cryptanalytic significance. We identify a large number of weak keys, in which knowledge of a small number of key bits suffices to determine many state and output bits with non-negligible probability. We use these weak keys to construct new distinguishers for RC4, and to mount related key attacks with practical complexities. Finally, we show that RC4 is completely insecure in a common mode of operation which is used in the widely deployed Wired Equivalent Privacy protocol (WEP, which is part of the 802.11 standard), in which a fixed secret key is concatenated with known IV modifiers in order to encrypt different messages. Our new passive ciphertext-only attack on this mode can recover an arbitrarily long key in a negligible amount of time which grows only linearly with its size, both for 24 and 128 bit IV modifiers.

Crollo del WEP

- Adam Stubblefield, John Ioannidis ed Avi Rubin, nello stesso mese, portarono a termine con successo un attacco ad una rete wireless protetta con WEP. L'esperimento portò alla determinazione in breve tempo di tutti i 40 bit della chiave segreta

- Entro la fine del mese Jeremy Bruestle e Blake Hegerle avevano già rilasciato **AirSnort**, il primo applicativo open source per il recupero delle chiavi in una rete wireless

- A seguito di questi eventi, IEEE istituì un gruppo di lavoro che aveva il compito di elaborare un nuovo standard per la sicurezza delle reti wireless

Il dopo-WEP

- La **Wi-Fi Alliance** è una associazione di produttori che certifica col proprio logo dispositivi WLAN
- Fondata nel **1999** con lo scopo di certificare l'interoperabilità dei dispositivi IEEE 802.11
- Un dispositivo conforme allo standard IEEE 802.11 può (ma non deve necessariamente) essere certificato Wi-Fi
- Dopo il crollo del WEP, la Wi-Fi alliance ha sviluppato tre nuove soluzioni per la sicurezza nelle WLAN:
  - Wi-Fi Protected Access (**WPA**)
  - Wi-Fi Protected Access 2 (**WPA2**)
  - Wi-Fi Protected Access 3 (**WPA3**)

WPA

- Wi-Fi Protected Access (**WPA**):
  - Disponibile dal **2003**, corrisponde a **IEEE 802.11i "draft"**
  - Richiede modifiche contenute rispetto a WEP
  - Introduce Temporal Key Integrity Protocol (TKIP) per avere una diversa chiave di 128 bit per ciascun pacchetto
  - Sostituisce CRC con un message authentication code (MAC)

- Wi-Fi Protected Access 2 (**WPA2**):
  - Disponibile dal **2004**, corrisponde a **IEEE 802.11i-2004**
  - Sostituisce RC4 con AES usato in modalità **CCM** (counter mode with cipher block chaining message authentication code (**CBC-MAC**))
  - Combina la modalità **CTR** per la confidenzialità con il **CBC-MAC** per l'autenticazione dei messaggi

Key Reinstallation Attack

- 2017: attacco di successo contro WPA2

WPA 3

- Annunciato a Gennaio 2018
- Usa cifratura a 128 bit in modalità WPA3-Personal ed a 192 bit in modalità WPA3-Enterprise
- Sostituisce il 4-way handshake con il protocollo di handshake chiamato «Dragonfly», che implementa “Simultaneous Authentication of Equals” (IEEE 802.11-2016)
- Garantisce forward secrecy: se una chiave di cifratura a lungo termine viene compromessa, le chiavi di sessione generate da essa rimangono riservate