*Corso “DOMOTICA ED EDIFICI INTELLIGENTI” – UNIVERSITA’ DI URBINO*
*Docente: Ing. Luca Romanelli*
*Mail: romanelli@baxsrl.com*

# Accesso remoto ad impianti domotici

## Problemi legati alla sicurezza e soluzioni

## Informatica: analisi dei rischi associati ad un'intrusione

- Downtime
- System manager’s time
- Clean-up costs
- Immagine
- Disclosure of trade secrets, cartelle cliniche, informazioni finanziarie
- Rischio troppo elevato: no Internet connection

## Domotica: Analisi dei rischi associati ad un'intrusione

Si sommano altri rischi ancora più gravi:

- Accesso ad impianti
- Accesso a sistemi antintrusione
- Violazione della privacy (TVCC)
- …
- Rischio troppo elevato: no Internet connection

# Internet Security

- La sicurezza su Internet e' difficile perche' i datagram che viaggiano dalla sorgente alla destinazione spesso passano attraverso molte reti intermedie e attraverso router che non appartenegono ne' sono controllati dal mittente o dal ricevente
- I datagram possono essere intercettati o compromessi e percio' i contenuti non possono essere fidati
- Se un server richiede una autenticazione del client che richiede un determinato servizio (***source authentication***), puo' basarsi sull'indirizzo IP sorgente di ogni datagram in ingresso ed accettare solamente le richieste dai client di una lista autorizzata
- Questo schema di autenticazione pero' risulta debole in una internet insicura poiche' e' possibile intercettare il traffico da router e ottenere l'accesso impersonando un client autorizzato

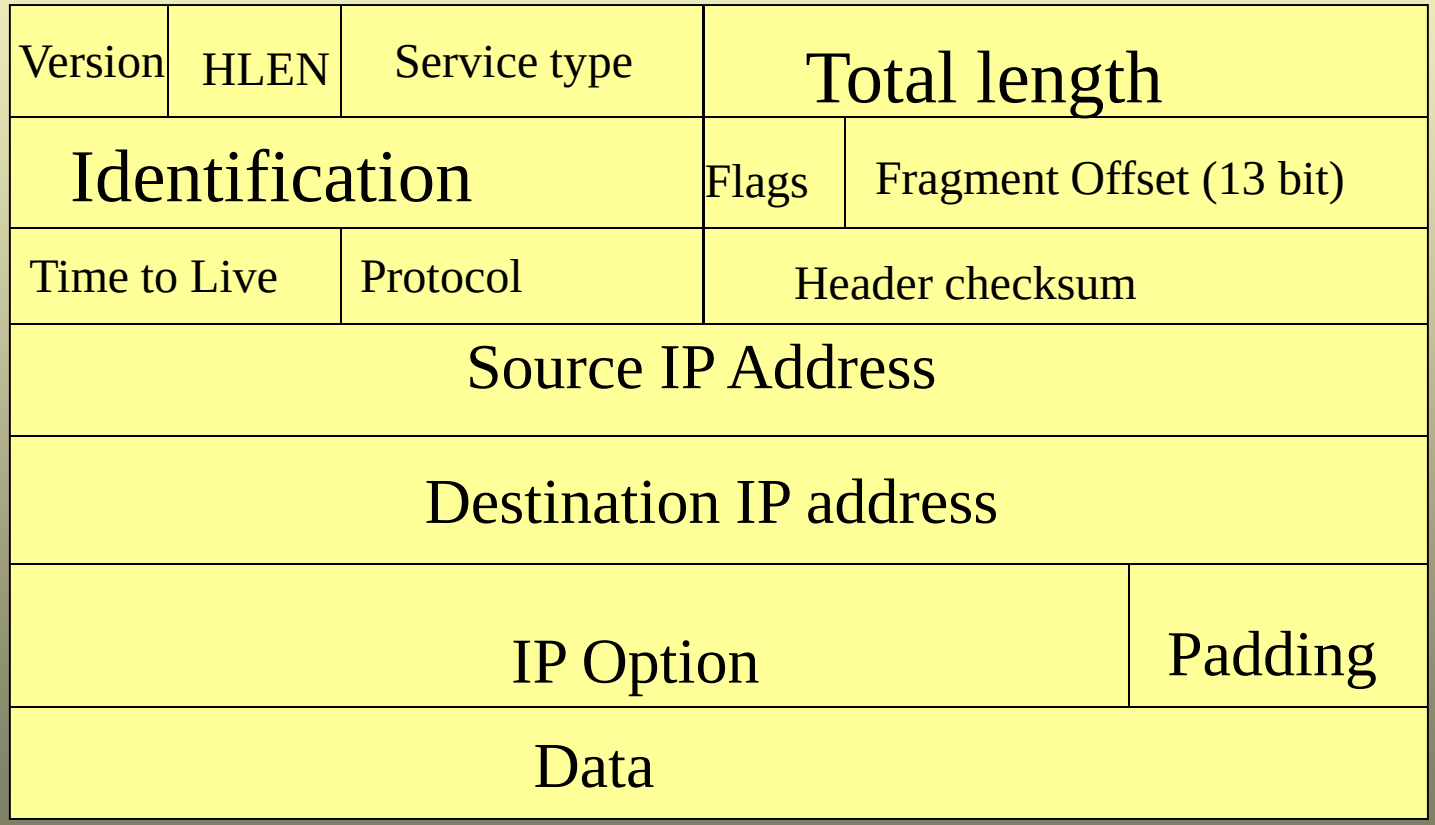
## Internet Security

- Per impedire tali intercettazioni e' necessario adottare un sistema di ***autenticazione forte*** (strong authentication) basato sull'uso della crittografia
- L'ente di standardizzazione del mondo Internet IETF ha individuato un insieme di protocolli che forniscono una comunicazione su Internet sicura
- **IPsec (IP security)** e' l'insieme dei protocolli che offrono servizi di autenticazione e di privacy a livello IP e che possono essere usati sia con IPv4 che con IPv6

# IPsec

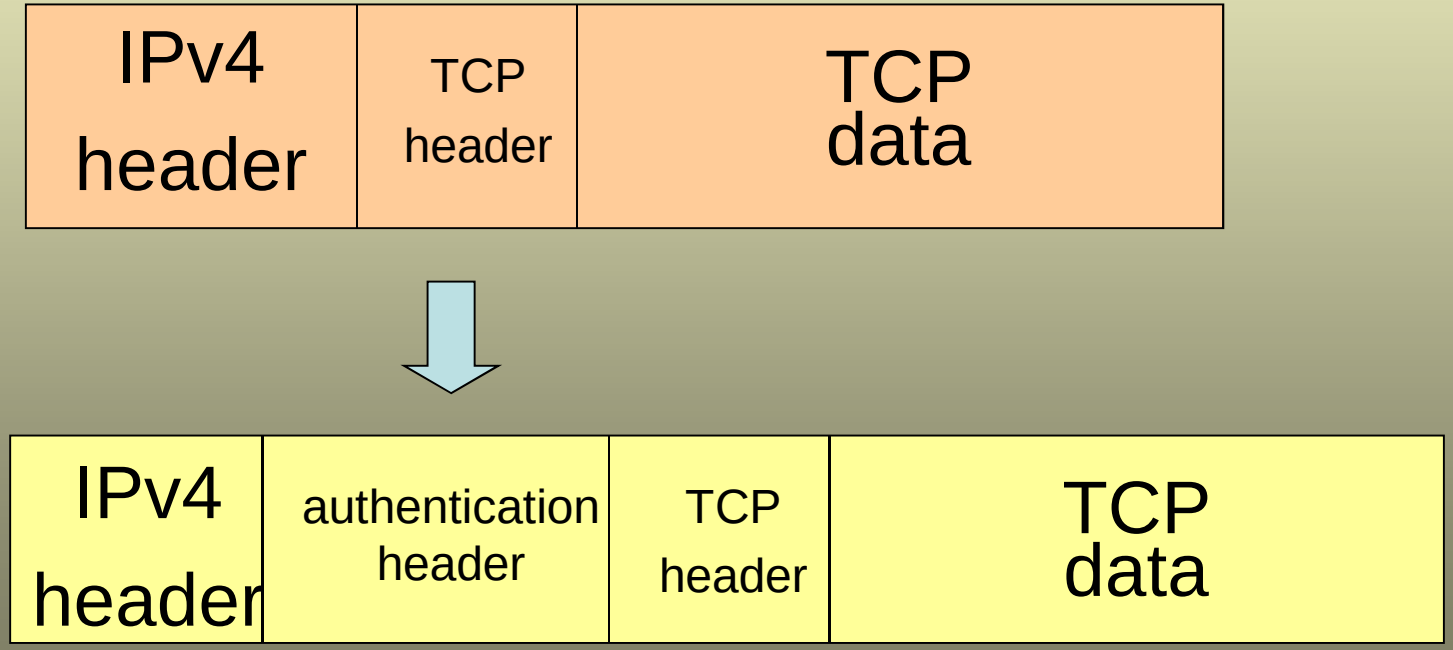
- Un’applicazione che usa IPsec puo’ scegliere se usare una facility di autenticazione che valida il mittente o usare un meccanismo di crittografia che assicuri la confidenzialita’ dei dati; le scelte possono essere anche assimetriche
- IPsec non e’ un singolo protocollo di sicurezza e  non vincola l’utente ad usare uno specifico algoritmo di crittografia o di autenticazione, ma fornisce un framework generale che permette ad ogni coppia di soggetti comunicanti di scegliere algoritmi e parametri (ad esempio la dimensione della chiave)
- *Per assicurare **l’interoperabilita’** Ipsec include un insieme di algoritmi di cifratura che tutte le implementazioni devono riconoscere*.

# Header IP


Version
HLEN
Service type
Total length
Identification
Flags
Fragment Offset (13 bit)
Time to Live
Protocol
Header checksum
Source IP Address
Destination IP address
IP Option
Padding
Data

## IPsec

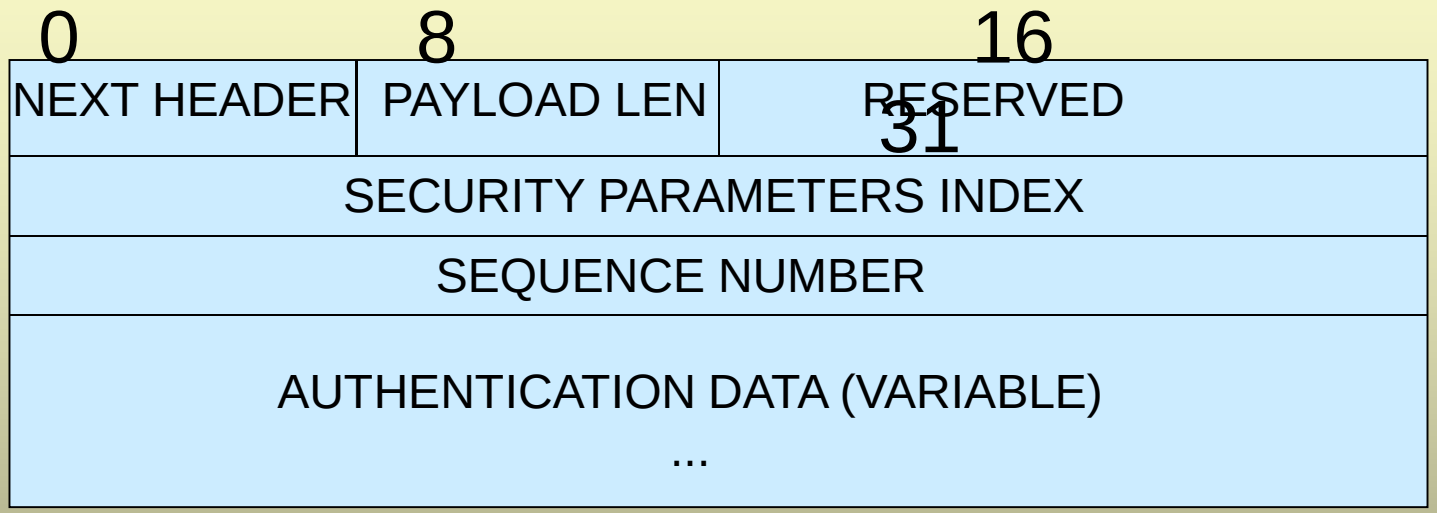
- Invece di cambiare l'header del datagram IP, Ipsec usa un **authentication header (AH)** separato per portare informazioni di autenticazione



## IPsec

- L’authentication header si trova immediatamente dopo l’header IP originale ma prima del transport header.
- Il campo **PROTOCOL** dell’header IP e’ cambiato al valore **51**, indicando la presenza di un header di autenticazione
- Il destinatario determina il tipo di informazione nel datagram attraverso il campo NEXT HEADER dell’AH che specifica il tipo del protocollo originario
- Quando il datagram arriva il destinatario usa l’informazione di security dall’AH per verificare il mittente e usa il valore del campo NEXT HEADER per demultiplexare il datagram

# IPsec header




- **PAYLOAD LEN**: specifica la lunghezza dell'authentication header
- **SEQUENCE NUMBER**: sequence number univoco per ogni pacchetto inviato; il numero inizia da zero quando un algoritmo di sicurezza particolare viene selezionato e aumenta in modo monotonico
- **SECURITY PARAMETERS INDEX**: specifica lo schema di sicurezza usato
- **AUTHENTICATION DATA**: contiene i dati per lo schema di sicurezza selezionato

## Security association

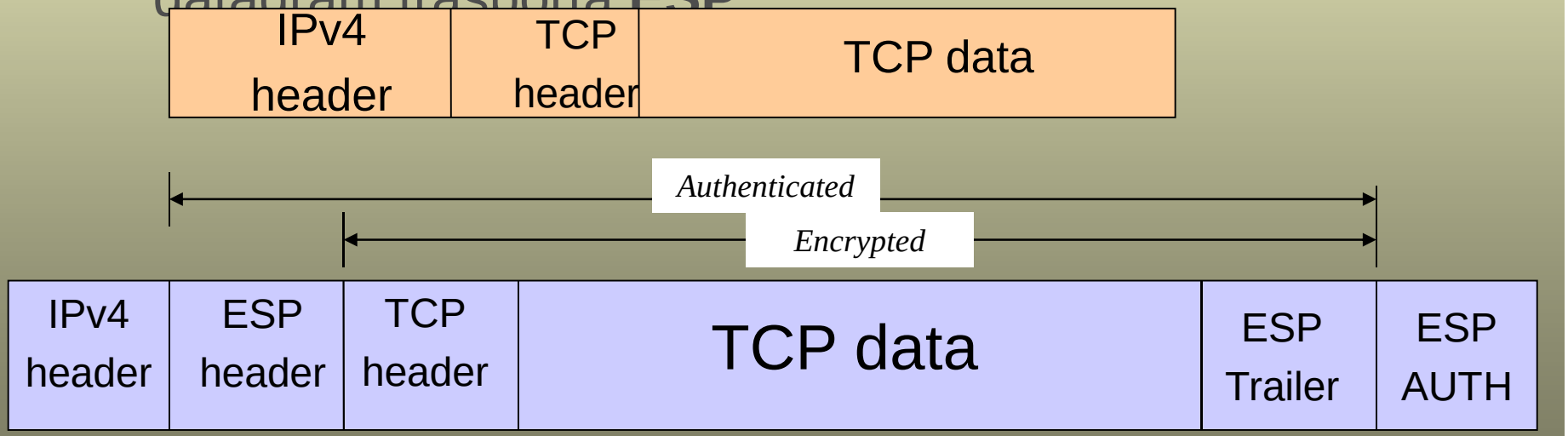
- Per salvare spazio nell'header, IPsec permette ad ogni receiver di raccogliere tutti dettagli su uno schema di sicurezza (algoritmo di autenticazione, chiavi, durata di validità della chiave, tempo in cui la destinazione si accorda di usare l'algoritmo, lista di indirizzi sorgenti autorizzati ad usare lo schema di sicurezza) in una astrazione conosciuta come **security association (SA)**
- Ad ogni SA viene dato un numero conosciuto come Security parameters index, attraverso cui e' identificato
- Prima che un mittente possa usare IPsec per comunicare con un destinatario, il mittente deve conoscere il valore dell'indice per un particolare SA che verra' da lui messo nel campo SECURITY PARAMETERS INDEX di ogni datagram in uscita

## Security Association

- I valori degli indici non sono specificati globalmente: ogni destinazione crea tanti SA quanti ne ha bisogno ed assegna un valore dell'indice a ciascuno
- La destinazione puo' specificare un tempo di vita per ogni SA e riusare valori degli indici
- Una destinazione usa il security parameters index per identificare l'SA per un  pacchetto. I valori non sono globali; una combinzaione di indirizzo di destinazione e security parameters index e' necessario per identificare un SA

## IPsec encapsulating security payload

- Per trattare sia la confidenzialita' che l'autenticazione, IPsec usa una **Encapsulating Security Payload (ESP)** che e' piu' complesso di un authentication header
- Un valore **50** nel campo PROTOCOL specifica che il datagram trasporta **ESP**



## IPsec encapsulating security payload

- ESP usa molti item gia’ presenti nell’authentication header ma con un ordine diverso.
- ESP HEADER consiste di 8 ottetti che identificano i security parameters index e un numero di sequenza
- ESP TRAILER consiste di un padding opzionale, un campo padding length e un NEXT HEADER che e’ seguito da dati di autenticazione varabili

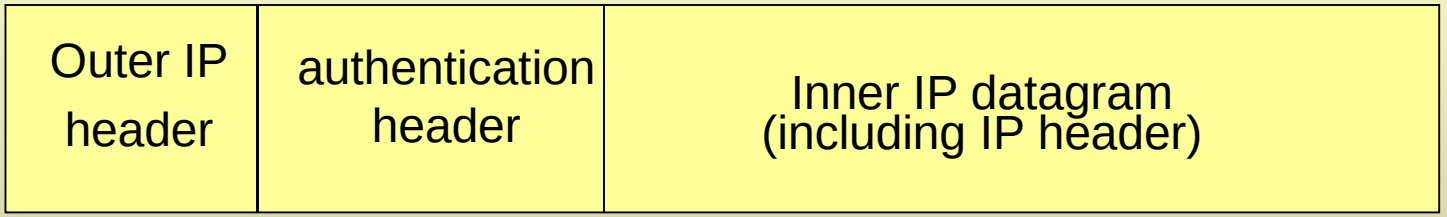
# Authentication and mutable header fields

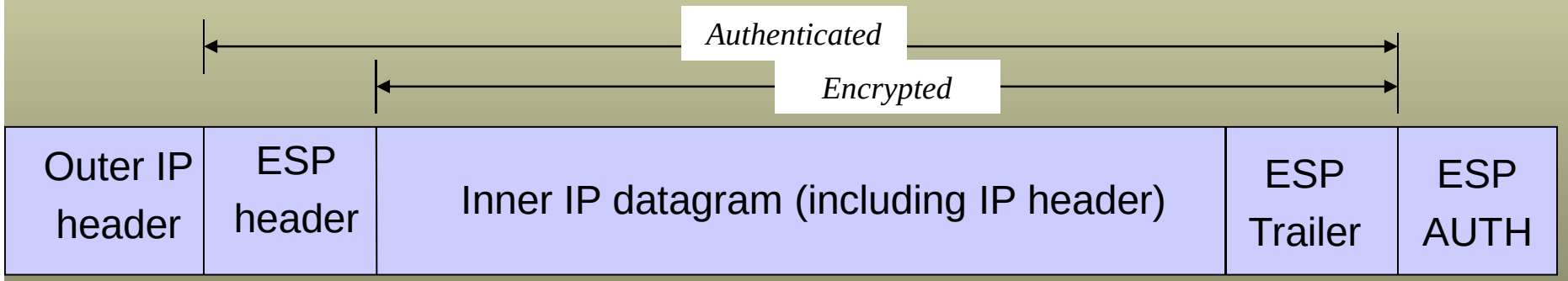
- Il meccanismo di IPsec e' stato progettato per assicurare che i datagram in arrivo siano identici a quelli inviati dalla sorgente.
- Questa garanzia e' impossibile: l'IP, infatti, e' di livello macchina-a-macchina, significando che il principio del layer si applica solo attraverso un hop; in particolare ogni sistema intermedio decrementa il campo time to live e ricalcola il checksum
- IPsec usa il termine ***mutable fields*** per riferirsi ai campi dell'header IP modificati durante il transito
- Per prevenire tali modifiche, che possono causare errori di autenticazione, IPsec omette specificatamente tali campi dal calcolo dell'autenticazione
- IPsec, quando arriva il datagram, autentica percio' solo i campi immutabili (source address e protocol type)

# IPsec Tunneling

- La tecnologia VPN usa la crittografia in un tunnelling IP-in-IP per mantenere i trasferimenti inter-site privati
- L'IPsec e' stato specificatamente progettato per per realizzare un tunnel criptato
- In particolare lo standard definisce versioni tunnelled sia dell'authentication header che del encapsulating security payload

# IPsec Tunneling




In questo caso il datagram IP intero incapsulato viene protetto

## Required security algorithms

- IPsec specifica un insieme minimo di algoritmi obbligatori per tutte le implementazioni

| |
|---|
| *Authentication* |
| HMAC with MD5 RFC 2403 |
| HMAC with SHA-1 RFC 2404 |
| *Encapsulationg Security Payload* |
| DES IN CBC MODE RFC 2405 |
| HMAC with MD5 RFC 2404 |
| HMAC with SHA-1 |
| Null Authentication |
| Null Encryption |

## Secure Socket Layer (SSL)

- De facto standard
- SSL e’ una tecnologia sviluppata originariamente da Netscape, Inc
- SSL risiede nello stesso livello del socket API
- Quando un client usa SSL per contattare un server, il protocollo SSL permette ad ogni lato di autenticare se stesso con l’altro
- le due parti negoziano per selezionare un algoritmo di crittografia che entrambi supportano
- SSL infine permette alle due parti di stabilire una connessione crittografata

# Uso della crittografia: SSL

- Secure Socket Layer