Host Identity Protocol

Seminario per il corso di Sicurezza
2004/2005

Guido Vicino

Università del Piemonte Orientale
Amedeo Avogadro

Perché l'indirizzo IP non basta più

- Protocollo TCP/IP formalizzato negli anni 70/80.
- Indifferenza verso le tematiche di sicurezza, privatezza e autenticazione dei dati.
- Ideato per sistemi statici e non mobile.
- Incongruenze semantiche tra identità e locazione.

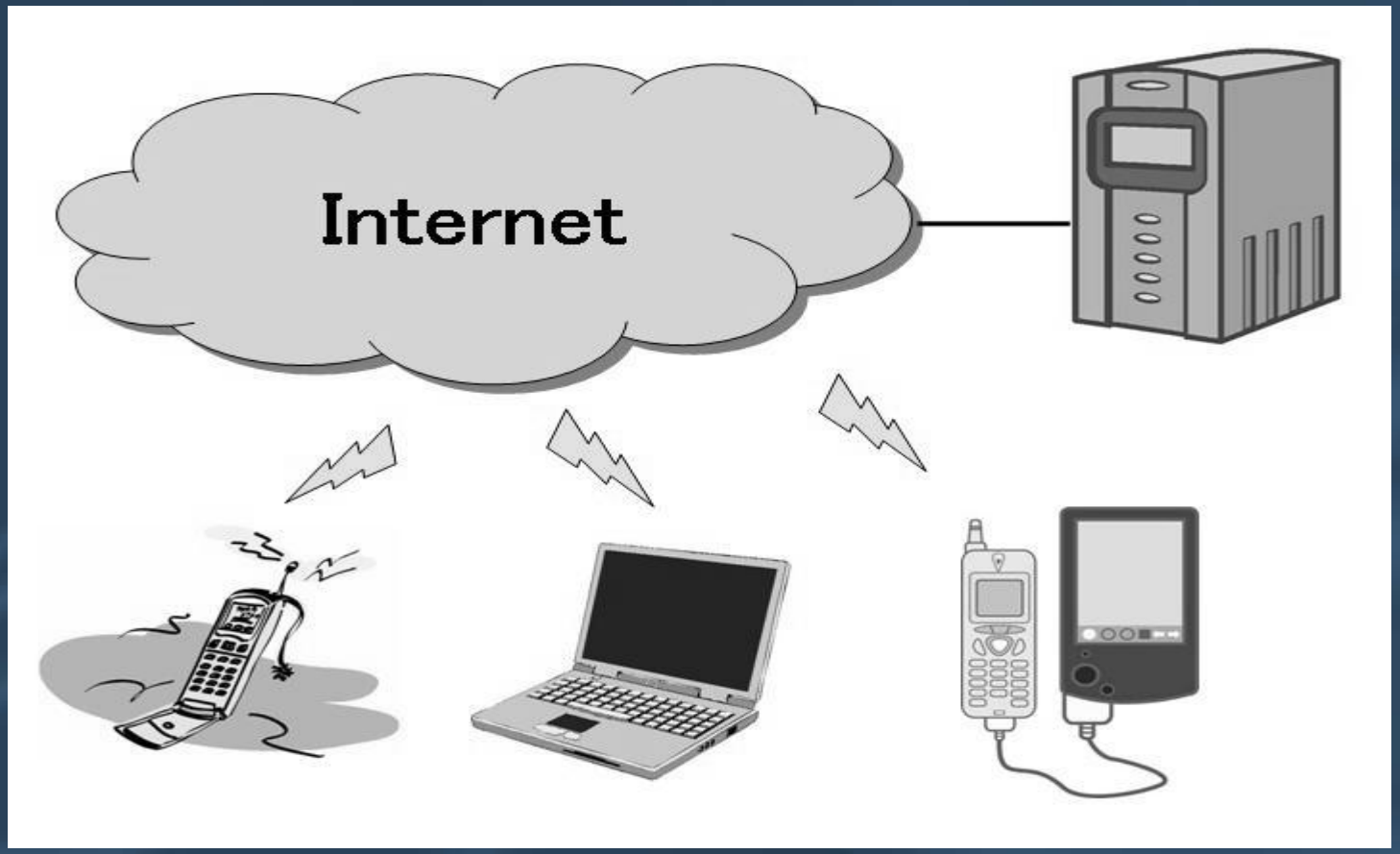
Quello che abbiamo...

Quello che vogliamo...

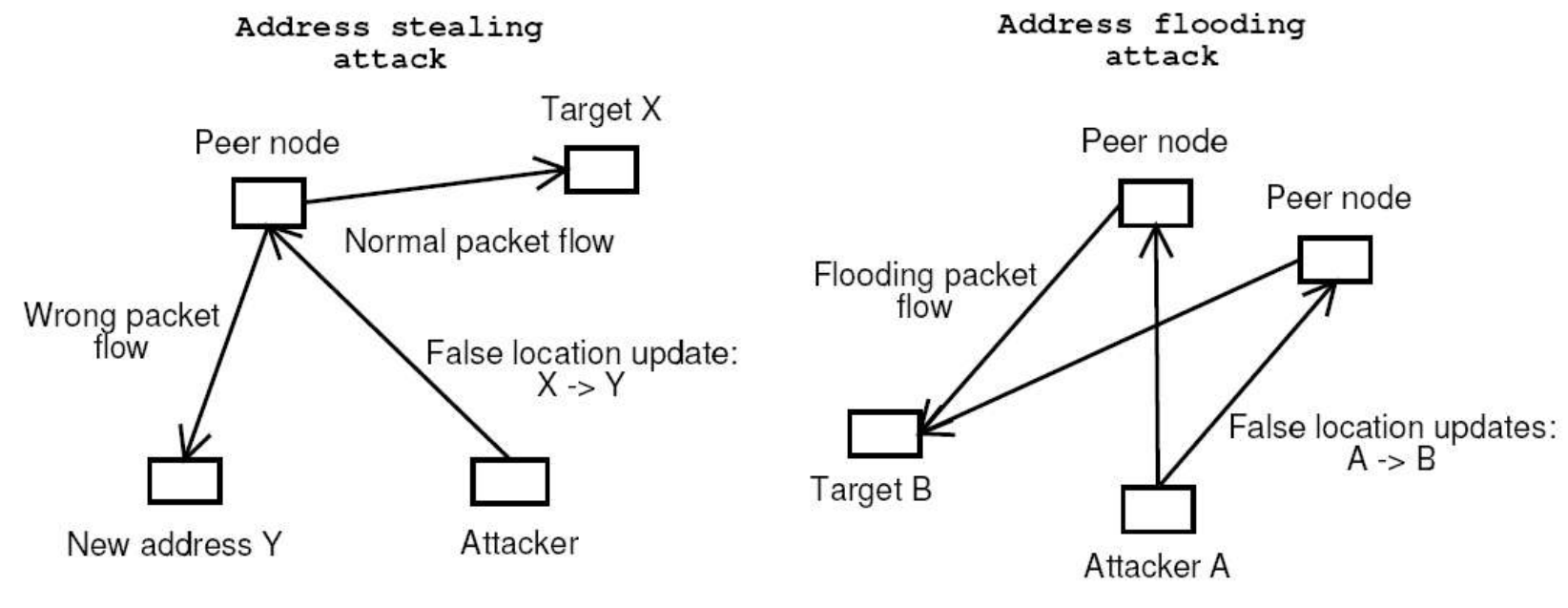
Perché vogliamo separare i due livelli?

- Reti e mobilità
- Grande diffusione di tecnologie wireless
- Supporto per sistemi multi-homed
- Bisogno di maggiore anonimità!
- Bisogno di maggiore identità!
- Protezione da attacchi address based

Esempio di rete mobile



Attacchi address based



Host Identify Protocol

- Host Identity Namespace
  Si vuole un nuovo spazio dei nomi sostitutivo a quello fornito dal protocollo IP e dal protocollo DNS.
- Semantic overloading and functionality complicated these namespaces.
  Moskowitz [1]

Host Identifiers (HI)

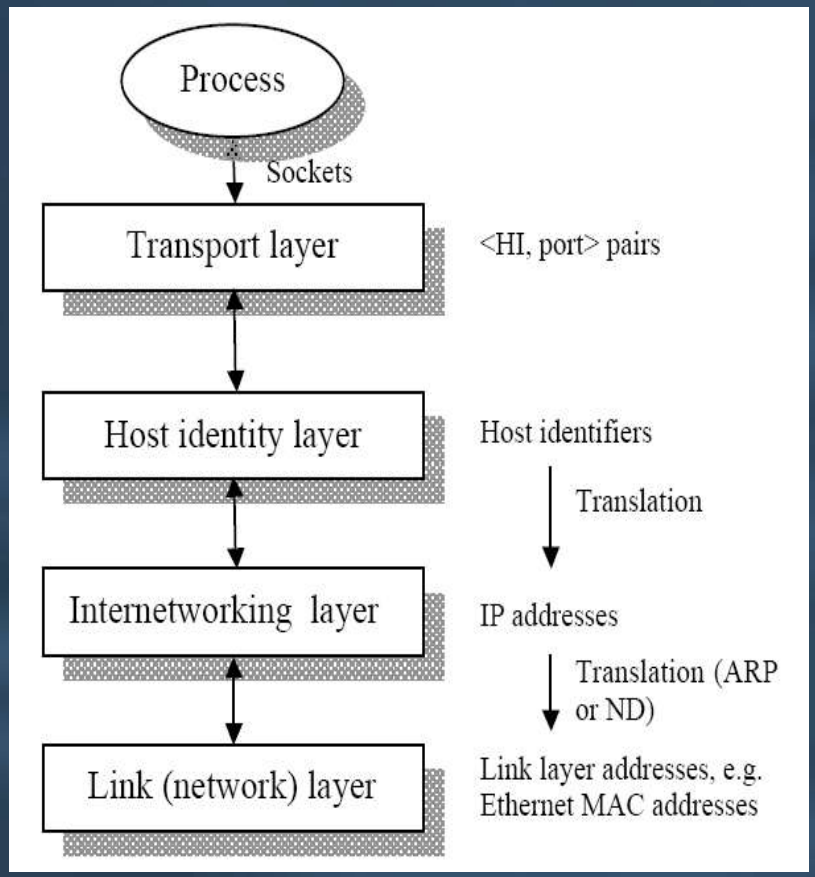
- Host Identity vs Host Identifier.
- L'Host Identity viene fornita tramite una chiave pubblica denominata Host Identifier e verificata tramite un opportuna chiave privata.
- L'HI può essere pubblica e indicizzata tramite Directory/DNS oppure privata.

Host Identity Tag & Local Scope Identity

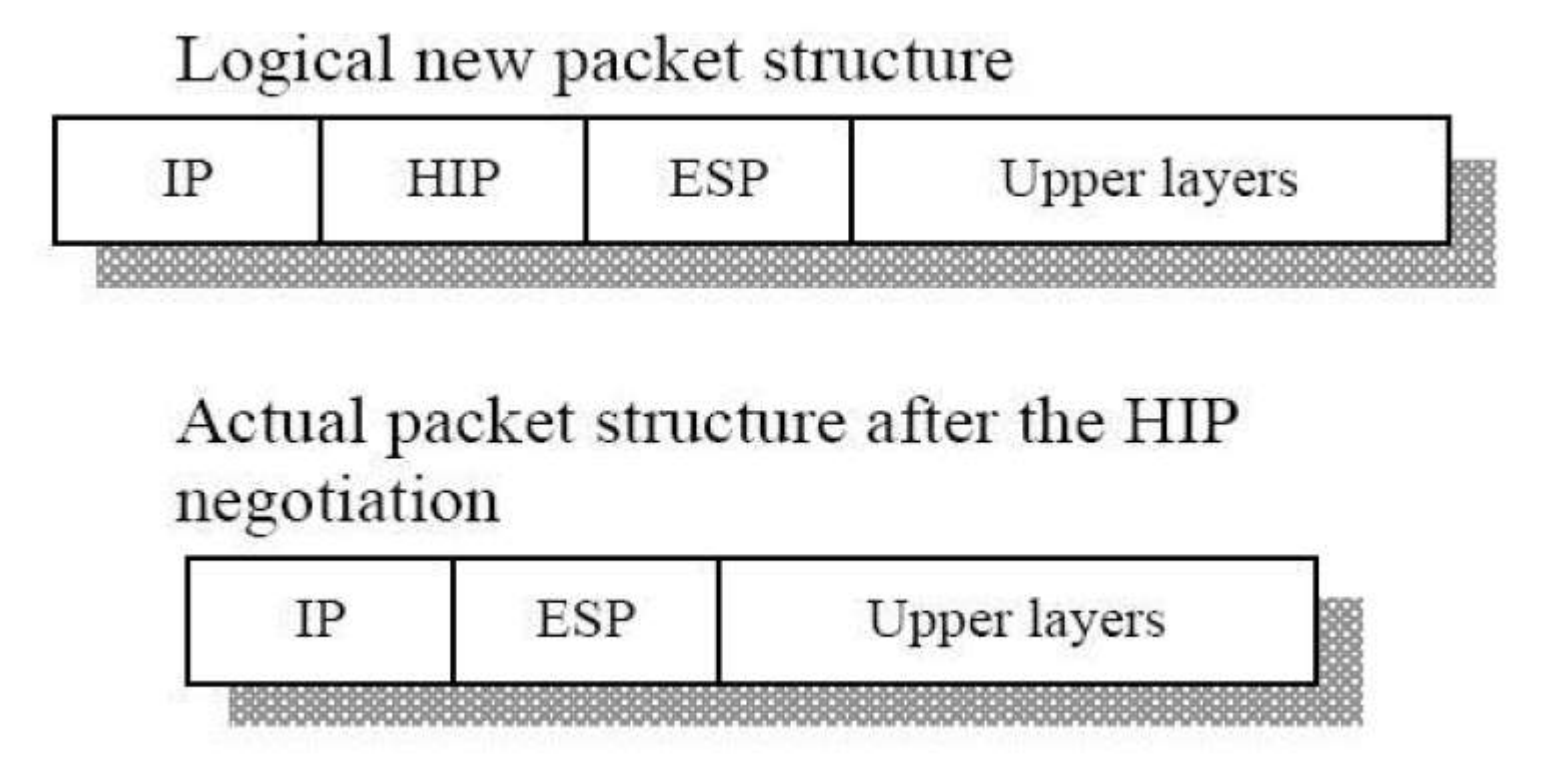
- Host Identity Tag: hash a 128 bit della chiave pubblica per l'uso all'interno delle intestazioni dei pacchetti.
- Local Scope Identity: hash a 32 bit della chiave pubblica per compatibilità con vecchie API e sistemi IPv4. Utilizzata solo localmente, a causa dei rischi di collisione.

Architettura HIP

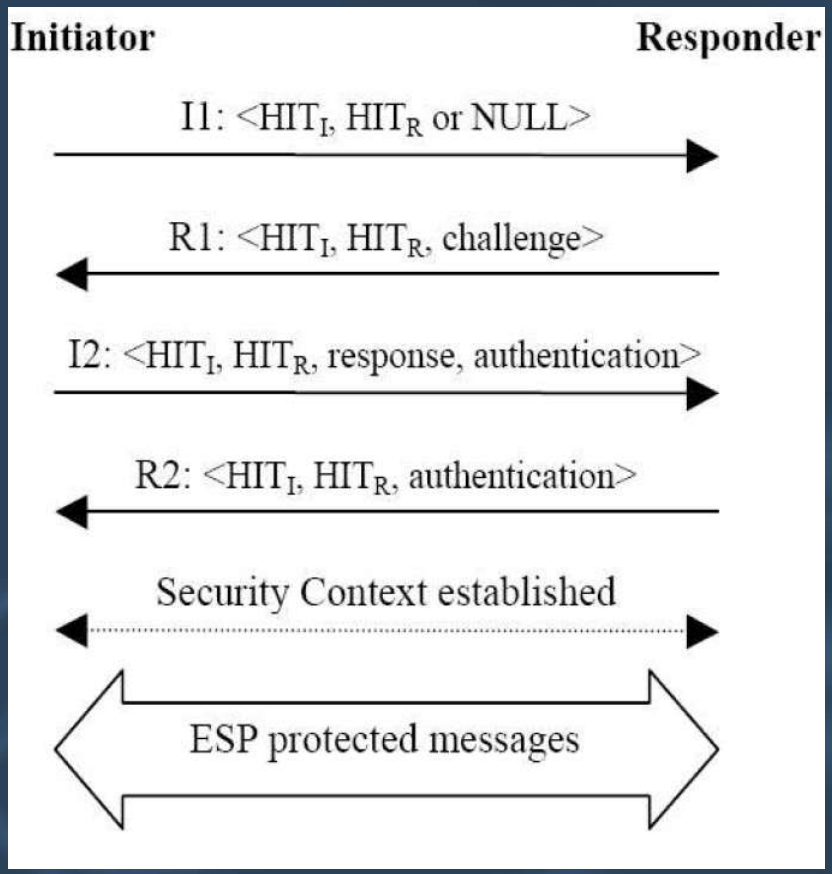
- Nuovo livello nello stack.
- Vecchia coppia: indirizzoIP : porta
- Nuova coppia: hostIdentifier: porta
- Crittografia e autenticazione tramite IPsEC



Pacchetto HIP

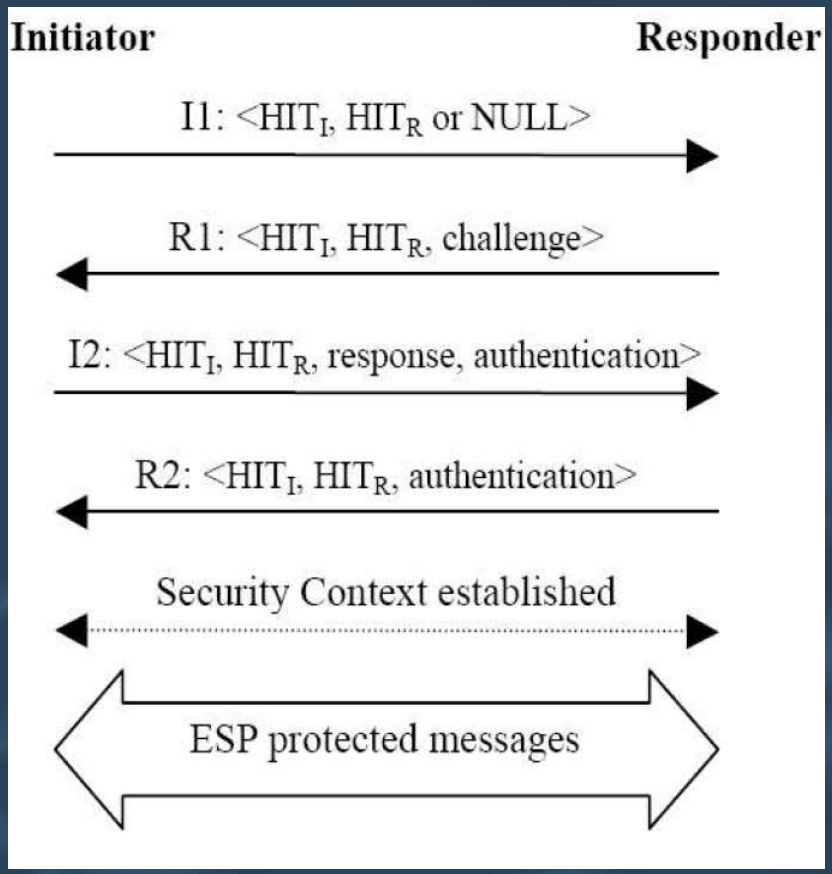


Sessione HIP Features



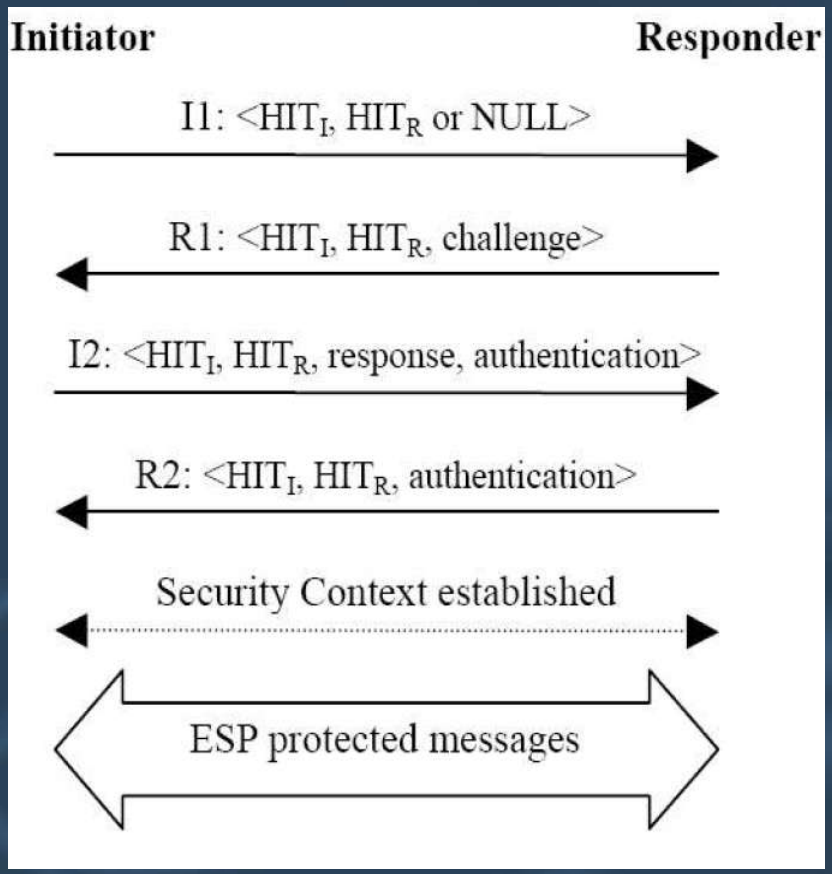
- Four-way Handshaking.
- Scambio sicuro tramite Diffie Hellman.
- Associazioni SA tramite IPSec.
- Messaggi protetti tramite ESP.
- Protezione da DoS tramite il “challenge system”.

Sessione HIP
Initiator e Responder



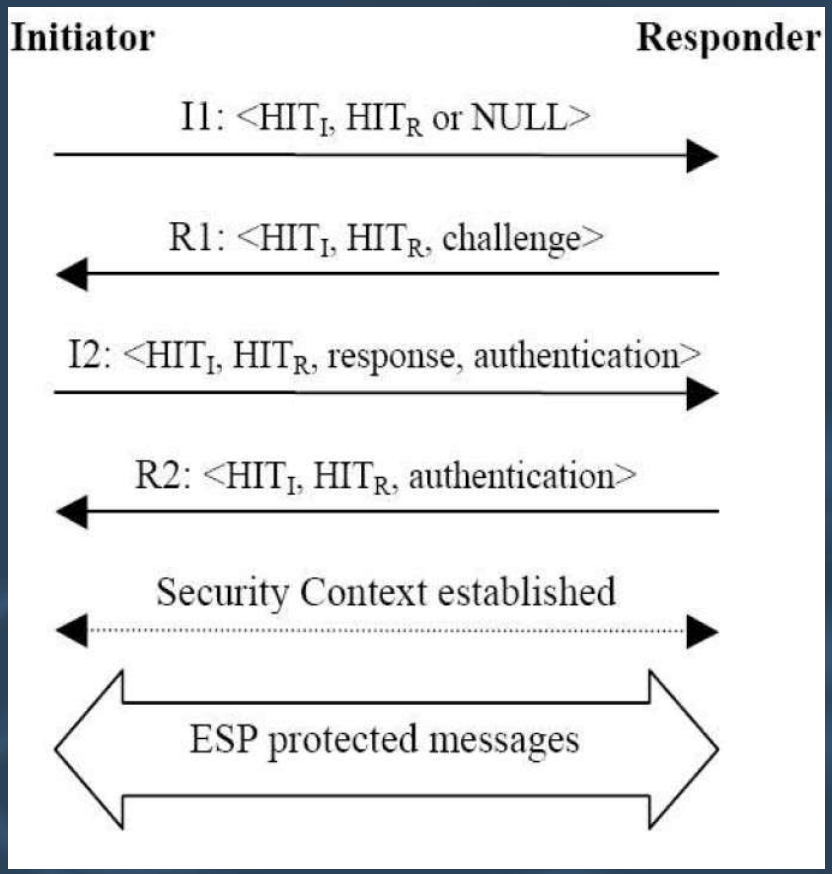
- L'Initiator è colui che richiede lo scambio di messaggi.
- Il Responder è colui che risponde.
- La protezione da DoS, viene offerta spostando il carico di lavoro dal Responder all'Initiator.

Sessione HIP four-way handshaking



1. L'Initiatior invia il pacchetto I1 contenente la richiesta e gli HIT del mittente e del destinatario.

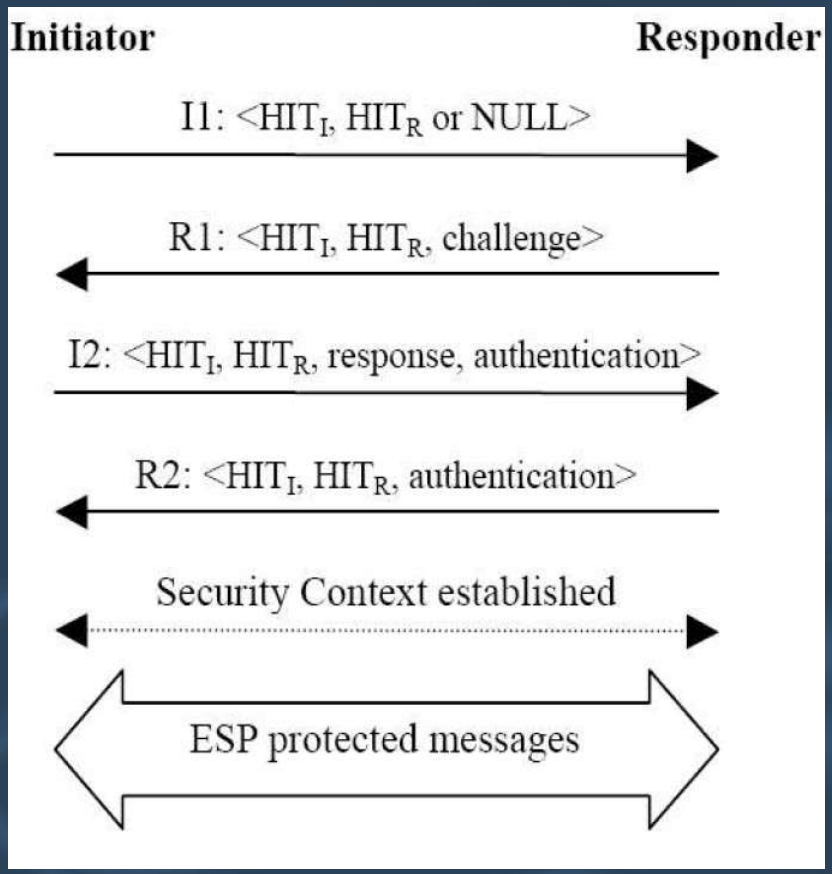
Sessione HIP four-way handshaking



2. Il Responder invia questo pacchetto in risposta all'R1, inizia Diffie Hellman e spedisce i dati riguardanti la connessione ESP.

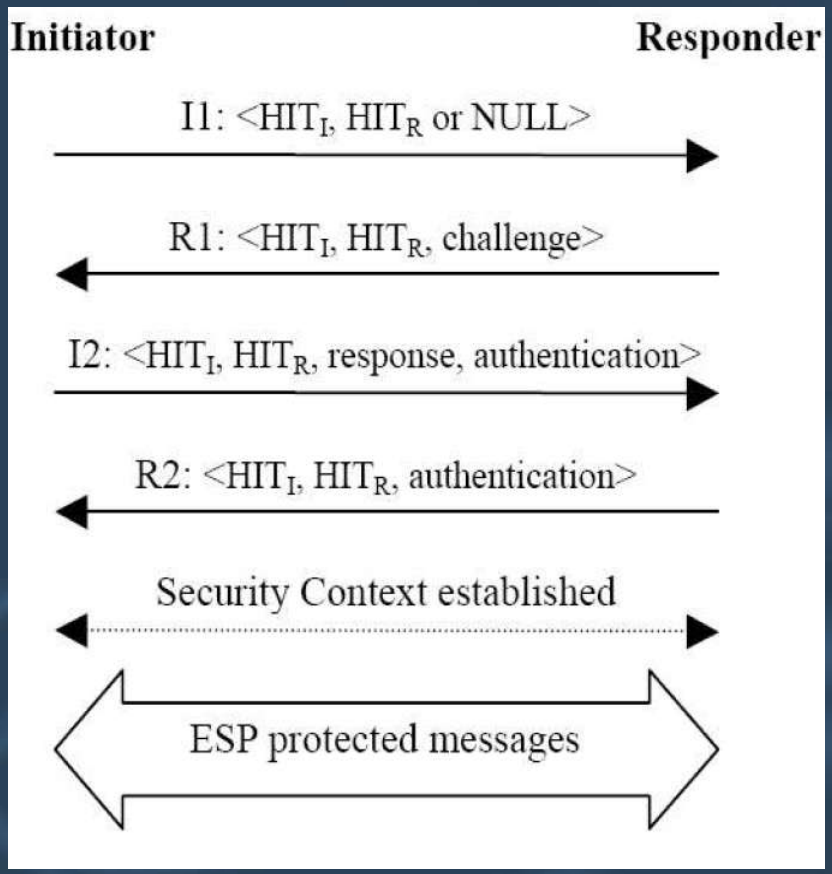
   Invia inoltre un indovinello crittografico…

Sessione HIP four-way handshaking



3. L'initiator deve rispondere al puzzle crittografico inviato nel pacchetto R1, inviare le preferenze ESP.
2. Nel caso la risposta al puzzle sia corretta si stabilisce la connessione con R2.

Sessione HIP four-way handshaking



...altrimenti il Responder continua ad inviare un numero predefinito di pacchetti R1 contenenti i challenge puzzle.

HIP e Denial of Services

- La protezione da attacchi di tipo Denial of Service (DoS) viene fornita tramite il sistema di challenge.
- I DoS normalmente sfruttano il maggior carico di lavoro richiesto dal destinatario di una connessione rispetto al lavoro quasi nullo del richiedente.

HIP e Denial of Services

- Il sistema di Challenge ribalta questo paradigma, spostando il carico maggiore verso il richiedente.
- Ci si protegge da vecchi attacchi ma se ne introducono di nuovi..

HIP e DoS: Nuovi problemi (1)

- Dopo che l'Initiator ha inviato la risposta al challenge, si inviano pacchetti I2 multipli con payload e firme non valide, al fine di sovraccaricare la macchina.
- Come difesa, si scartano i pacchetti I2 dopo un certo numero di errori.

HIP e DoS: Nuovi problemi (2)

- Sfruttare il recupero delle associazioni dopo un crash di sistema.
- HIP utilizza degli stati, se uno scambio viene inizializzato le parti si trovano in ESTABLISHED fino a quando non viene fatta una CLOSE.
- Si possono inviare pacchetti di resume per confondere e causare Denial of Service

HIP e DoS: Nuovi problemi (3)

Altri due possibili attacchi:

- ICPMP Parameter Problem e Reflection Attacks. Causati dall'invio di pacchetti CLOSE errati.
- Perdita della sincronizzazione nel caso di un Responder malevolo che sfrutti il challenge come sistema di attacco.

HIP e Man-in-the-Middle

- Problemi di Man-in-the-middle risolti se c'e' un Address Directory che mi certifica i miei HI.
- Spesso però gli HI sono anonimi e non si vuole un così alto livello di protezione per connessioni saltuarie.
- Problema parzialmente risolto.

Riferimenti

[1]: R. Moskowitz, P. Nikander, "Host Identity Protocol Architecture" Internet Draft, IETF 2004, draft-ietf-hip-arch-02.

[2]: R. Moskowitz, P. Nikander, P. Jokela, T. Henderson, "Host Identity Protocol", Internet Draft, IETF 2005, draft-ietf-hip-base-02.

[3]: P. Jokela, P. Nikander, J. Melen, J. Ylitalo, J. Wall "Host Identity Protocol – Extended Abstract" in *Proceedings of WWRF8bis (electronic),* Beijing, China, February 26-27, 2004.

[4]: K. Kostiainen "Host Identity Payload for Mobility and Security", Helsinki University of Technology, Department of Computer Science and Engineering, 2003.