CWC Oulu
CENTRE FOR WIRELESS COMMUNICATIONS
University of Oulu

Comparison and Analysis of Secure Mobile Architecture and Evolved Packet System

Jani Pellikka, Marek Skowron, Andrei Gurtov

Motivation

- Two separate worlds of protocol development
  - IETF and 3GPP
- 3GPP moves towards all-IP in LTE specs
  - IP Mobility, security, IPv4/6
- Currently 3GPP uses standard-track protocols
  - DSMIPv6, PMIPv6, IKEv2, MOBIKE
- Can HIP be a useful solution in 3GPP?
  - OpenGroup Secure Mobile Architecture vs. Evolved Packet Core (EPC) by 3GPP
  - Compare and find pros and cons of both worlds
  - Propose a common way forward

Evolved Packet System (EPS) (1/2)

- Realizes a common all-IP framework for voice and data
  - High-performance core network: Evolved Packet Core (EPC)
  - Offers connectivity to various Packet Data Networks (PDNs)
  - Multiple heterogeneous Radio Access Technologies (RATs)
    - WiFi, WiMAX, HRPD, LTE, LTE-A, ...
- Two primary gateways: S-GW and PDN GW
  - S-GW provides access for LTE-based mobile devices
  - PDN GW connects external IP networks (e.g. Internet and non-3GPP services) with the core network (EPC)
  - Both gateways act as an anchor point in mobility:
    - Intra-LTE mobility (S-GW)
    - IP mobility (PDN GW)
- Voice services realized via IP Multimedia Subsystem (IMS)
  - Voice over IP (VoIP) support and cooperation with PSTNs
  - Use of Session Initiation Protocol (SIP) in signaling
- Location services provided by Location Services (LCS)
  - Centralized entity provides clients with location (e.g. coordinates)
  - Possibility to define custom logical areas based geographical location

Evolved Packet System (EPS) (2/2)

- Network access security provides secure access to EPS
  - 3GPP-based mutual authorization and authentication
  - Use of EPS AKA and EAP AKA allows AAA features with the same credentials regardless of the access technology used
  - IP traffic protection used for non-trusted non-3GPP accesses
    - IPSec ESP tunnels established between UE and PDN GW (ePDN)
    - Security Associations (SAs) negotiated by the IKEv2 protocol
- IP mobility based upon two Mobile IP (MIP) schemes
  - Host-based mobility by Dual Stack MIPv6 (DSMIPv6)
  - Network-based mobility via Proxy Mobile IP (PMIPv6)
  - Route Optimization (RO) not supported by EPS
  - PDN GW or other network node near the EPC border acts as a Home Agent (HA) for the mobile host
- Policy and Charging Control (PCC)
  - Session-level policies enforced by the network gateways
  - User-specific policies based on profile information and decided by centralized Policy and Charging Rules Function (PCRF)

Secure Mobile Architecture (1/2)

- Addresses business needs of having a secure network connection over disparate wireless technologies and a capability of seamless roaming between them

- Standardization effort of The Open Group (TOG)
  - Integration architecture of Internet and roaming protocols
  - Vision of how wireless systems need and can be secure
  - Existing and emerging standards from IETF and IEEE

- Security based on Host Identity (HI) – not IP address
  - The IP layer is treated as an insecure transport layer
  - Each and every packet is associated with an identity
  - Host Identity Protocol (HIP) provides cryptographic HIs
  - End-to-end security enforced by the network

Secure Mobile Architecture (2/2)

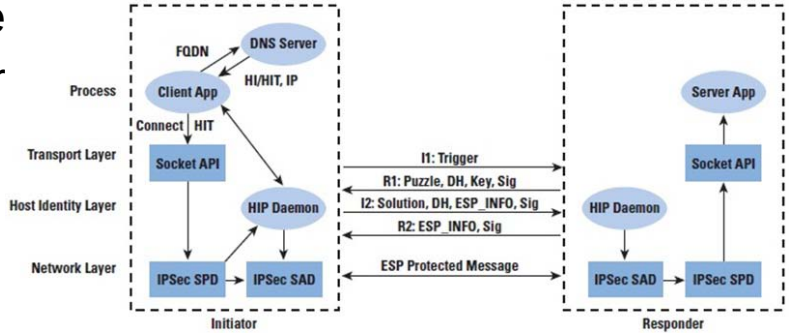
- Treats multimedia merely as an IP-based application
  - Addresses VoIP traffic
  - Voice and multimedia signaled and carried over the IP transport
  - Use of UDP and SIP

- Design principles in short
  1. Use of IP protocol
  2. IP-level security
  3. Seamless mobility
  4. Policy enforcement
  5. Security zones

Description	Principles
IP-only	Only IP is addressed. The IP protocol is assumed to be the future protocol most data and voice are carried over with in the Internet.
Security	Security is based on the host identity instead of IP and MAC addresses. Authentication, authorization, and encryption are guaranteed between the end points of communication. The security of the user is provided on the basis of communication session.
Mobility	Mobile device is able to seamlessly and transparently migrate across disparate network technologies, while maintaining the ongoing communication sessions and established security parameters. Hand-offs and transfers must be fast enough for VoIP traffic.
Policy Enforcement	There is a policy engine, which determines policies and employs them based on predefined rules for attributes such as user role and location. Policies can be enforced at network and application level.
Location	Location information is utilized to enable security zones. Host authorization is managed by the policy engine, which decides to deny or grant service to hosts based on their current location.

Host Identity Protocol (HIP)

- Host identified by cryptographic identity
  - Implements the ID/locator split scheme
  - Public/private key pair as host identifier
  - Host Identity Tag (HIT) used by apps



A. Gurtov, M. Komu, R. Moskowitz, Host Identity Protocol (HIP) : Identifier/Locator Split for Host Mobility and Multihoming, Internet Protocol Journal, 12(1): 27-32, March 2009.

- Authentication over Internet protocols
  - Mutual authentication via public keys
  - Opportunistic negotiation of SA pairs
  - Data protected over ESP (SPI as flow ID)

- Support for host mobility and multihoming
  - Mobility events handled via HIP UPDATE messages (part of IP stack)
  - Additional infrastructure to aid host tracking and reachability needed, e.g. dynamic DNS, Rendezvous Server (SRV) park or/and a fully distributed DHT-based Hi^3 system
  - ID/locator split enables seamless interoperability between the IPv4 and IPv6 applications and multihoming between the IPv4 and Ipv6 interfaces assigned to a host

Comparison of the Architectures (1/2)

- IP-Only
  - Both are in alignment with the all-IP paradigm
  - Address VoIP applications and SIP-based signaling
  - Both support IPv4 and IPv6 protocol interoperability
    - HIP in SMA allows for seamless simultaneous use of interfaces (multihoming) of both protocol families
    - EPS allows IPv4 and IPv6 applications to communicate with each other through the use of DSMIPv6 scheme; no support for simultaneous use between IPv4/6 addresses
- Security
  - Mutual AKA-based authentication (pre-shared symmetric key) in EPS ***VS.*** HIP's asymmetric public/private key-based mutual authentication in SMA
  - HIP requires an additional Public Key Infrastructure (PKI) to guarantee the identities; in EPS, the possession of the shared secret is enough
  - EPS = end-to-middle security, SMA = end-to-end security
  - Both secure control and user plane traffic with IPSec ESP, and provide a similar degree of security against DoS and MitM attacks
  - In EPS, MOBIKE maintains SAs in mobility, but only one pair of IP addresses allowed for an SA at a time (i.e. no simultaneous multihoming)
  - Standard HIP has no support for identity privacy; extensions exist

Comparison of the Architectures (2/2)

- IP Mobility
  - SMA relies on HIP combined with a seamless handover mechanism, e.g. a Context Transfer Protocol (CTP) and dynamic DNS (or other real-time database infrastructure) for host tracking and reachability
  - EPS relies on MIP-based schemes, which suffer from a scalability problem due to the suboptimal routing of user traffic
  - Mobility through SIP possible in both architectures; in SMA HIP is combined with SIP for complimentary mobility (i.e. host mobility handled by HIP, user and session mobility handled by SIP)
- Location-based Security Zones and Policy Enforcement
  - EPS includes support for network enforced policy control, but does not take geographical location information into account *per se*
  - EPS provides a means for defining logical and geographical zones via LCS, but is not currently utilized in the policy enforcement
  - → A communication between LCS and PCRF need to be realized
  - → A storage and decision logic for the policy rules on security zones

Conclusions and Future Work

- EPS and SMA provides security of roughly the same degree; however more scalable authentication can be realized if HIP is combined with PKI and support for identity privacy is included
- SMA is able to provide more efficient and scalable mobility with simultaneous multihoming with both IPv4 and IPv6 addresses
- EPS has no support for the business need of location-based security zones and policy enforcement by default, but it can be implemented as all required components are already in place

- Future work includes studying possible issues in integrating the two architectures and building a convergent EPS-SMA system; also the joint use of HIP and SIP is investigated

Thank you!