Boeing HIP Secure Mobile Architecture - update

IETF 73 HIPRG Meeting (November 21, 2008)

Tom Henderson (thomas.r.henderson@boeing.com), presenting for the Boeing SMA team
Overview

Engineering, Operations & Technology | Phantom Works

E&IT | Networked Systems Technology

- Boeing is using HIP as part of a Secure Mobile Architecture (SMA) implementation
  - [http://www.opengroup.org/bookstore/catalog/e041.htm](http://www.opengroup.org/bookstore/catalog/e041.htm)
- Provides secure connectivity to SCADAnet equipment over an untrusted factory wireless network

- 777 assembly line, Everett WA
- Supported by HIP overlays
• Provide layer-2 connectivity between SCADAnet (IPv4) devices
• Overlay provides a “layer-2 VPN”-like service to legacy IPv4 devices
  • Illusion of a single L2 flooding domain (unicast, multicast)
  • IP traffic only
  • A given device may be reachable from more than one overlay interface
  • Ethernet MTU (1500 bytes) is supported

![Diagram](Image)
• Instance of an “IP-Only LAN Service”

A Virtual Private LAN Service (VPLS) [VPLS] is used to interconnect systems across a wide-area or metropolitan-area network, making it appear that they are on a private LAN. The systems which are interconnected may themselves be LAN switches. If, however, they are IP hosts or IP routers, certain simplifications to the operation of the VPLS are possible. We call this simplified type of VPLS an "IP-only LAN Service" (IPLS).
Implementation view

Engineering, Operations & Technology | Phantom Works

Copyright © 2007 Boeing. All rights reserved.

• Secure tunneling between end points
  • HIP gateway-- a PE device implementing HIP for secure tunneling
  • Requires directory services for tunnel endpoint discovery (overlay definition) and DNS (rendezvous) functions
  • Some directory services circumvented by configuration files (for now)
**Naming view**

- **Multiple overlays supported**
  - Each overlay has a unique name
- **Each PE device has a name (an asset tag)**
  - Also, a DNS name of form `<asset-tag>.domain.com`
- **IP address ranges are allowed to overlap in the two domains**
Differences from standard HIP

• HIP is deployed as a “bump-in-the-wire” (BITW) instead of “bump-in-the-stack” (BITS)

• Unlike IPsec BITW gateways, we do not decrement TTL

• Host identities in the system are bound via certificates to Boeing names (asset tags)
  • Could be integrated to enterprise PKI
Recent progress

- Integration with LDAP server for storing configuration data
- Support for HIP mobile router
Configuration requirements

- Certificates binding “management friendly” distinguished name (e.g. gateway asset tag) to a host identity public key

- Legacy end devices are named by IPv4 address

- Additional configuration needed:
  1) End device IP address to LSI
     - which HIP gateway fronts for which end device
  2) LSI to underlay IP address
  3) Access control lists
Walk-through

Initiator

Scadaneet devices

10.0.0.13

10.0.0.10

10.0.0.12

layer-2 switch

possible cross-connect

HIP gateway

bcwin

A56

A34

Responder

DNS/LDAP

A78

layer-2 switch

10.0.0.21

10.0.0.20

A12

10.0.0.11

10.0.0.10

10.0.0.13

10.0.0.20
ARP must be proxied or carried over the overlay.
Walk-through

Engineering, Operations & Technology | Phantom Works

Copyright © 2007 Boeing. All rights reserved.

Networked Systems Technology

**Responder**

10.0.0.21

**Initiator**

ARP response (10.0.0.21 is at [A34 MAC])

at least one gateway needs to respond
Data to 10.0.0.21

remote IP address maps to a particular HIP gateway

HIP gateway maps to an underlying IP address

Access controls applied (can A34 talk to A78?)

configuration data may be stored locally or fetched from an LDAP DB
Access controls may also be applied here
Ethernet frame is encapsulated and tunneled through HIP SA

Data to 10.0.0.21

Responder
10.0.0.21

HIP gateway
bcwin

DNS/LDAP

layer-2 switch
10.0.0.20

layer-2 switch
10.0.0.12

10.0.0.13

Initiator

devices
Benefits of using HIP

• Mobility (overlay nodes can change address without breaking security associations)

• Access controls tied to PKI and use of certificates

• DoS-resistance on the security underlay (via HIP base exchange)
SMA/SCADANet Endbox

Networked Systems Technology

Engineering, Operations & Technology | Phantom Works

Copyright © 2007 Boeing. All rights reserved.
Related Work

• L2VPN IP-only LAN Service (IPLS)
  • Build a virtual LAN using HIP tunnels instead of GRE tunnels

• Secure Pseudowire with IPsec/L2TPv3

• Microsoft Server and Domain Isolation

• OpenVPN project, supports ethernet bridging:

• ISI X-Bone

• HIP BONE
• A large set of contributors in Boeing are responsible for this work:

  - Richard Paine
  - Steven Venema
  - David Mattes
  - Orlie Brewer
  - Jin Fang
  - Jeff Meegan