Lecture 12 - Network Security

CSE497b - Spring 2007
Introduction Computer and Network Security
Professor Jaeger
www.cse.psu.edu/~tjaeger/cse497b-s07/
Idea

• Why don’t we just integrate some of these neat crypto tricks directly into the IP protocol stack?

• This is called transport security
IPsec

- IP layer security protocol
  - Integrated directly into protocol stack
  - Defined as an extension to the network layer
  - Transparent to the above layers and application

- Provides
  - confidentiality
  - integrity
  - authenticity
  - replay protection
  - DOS protection
Tunnel vs. Transport Mode

• Transport mode
  – default mode of IPsec -- protects transport layer packet
  – end-to-end encapsulation of data
  – useful when both endpoints are configured to use/manage IPsec

• Tunnel mode
  – encapsulates all of the IP data over a new IP level packet
  – useful when the device applying IPsec to the packet is not the originating host, e.g., at a gateway
  – Also known as, “ip over ip”

• IPsec provides the mechanism, you provide the policy
IPsec Processing

Start

IKE Phase 1:
Negotiate Session
ISAKMP Keys

IKE Phase 2:
Negotiate SA
Keys

Processing
Policy

Yes

Yes

ESP

No

No

AH

Process Using AH
Encoding and Policy

ESP

Process Using ESP
Encoding and Policy

SA Keys Exist?

IKE

AH

Processing Policy

Yes

AH

Esp

No

IKE Phase 1: Negotiate Session
ISAKMP Keys

IKE Phase 2: Negotiate SA Keys

ISAKMP Keys Exist?

Language: en
Internet Key Exchange (IKE)

- Built on of ISAKMP framework
- Two phase protocol used to establish parameters and keys for session
  - Phase 1: negotiate parameters, authenticate peers, establish secure channel
    - ISAKMP keys
  - Phase 2: Establish a security association (SA)
    - SA keys used to process user traffic
- The details are unimaginably complex
- The SA defines algorithms, keys, and policy used to secure the session
IPsec Implementation

- User: ISAKMP framework
- Kernel: IPsec processing

![IPsec Implementation Diagram]
Authentication Header (AH)

• Authenticity and integrity
  – via HMAC
  – over IP headers and data

• Advantage: the authenticity of data and IP header information is protected
  – it gets a little complicated with *mutable* fields, which are supposed to be altered by network as packet traverses the network
  – some fields are *immutable*, and are protected

• Confidentiality of data is *not* preserved

• Replay protection via AH sequence numbers
  – note that this replicates some features of TCP (good?)
Authentication Header (AH)

- Modifications to the packet format

![Diagram showing IP Header, AH Header, MAC, and Payload]

- IP Header
- AH Header
- MAC
- Payload

- AH Packet
- Authenticated
- Encrypted
IPsec Authentication

• SPI: (spy) identifies the security association for this packet
  – Type of crypto checksum, how large it is, and how it is computed
  – Really the policy for the packet

• Authentication data
  – Hash of packet contents include IP header as as specified by SPI
  – Treat transient fields (TTL, header checksum) as zero

• Keyed MD5 Hash is default
Encapsulating Security Payload (ESP)

• Confidentiality, authenticity and integrity
  – via encryption and HMAC
  – over IP payload (data)

• Advantage: the security manipulations are done solely on user data
  – TCP packet is fully secured
  – simplifies processing

• Use “null” encryption to get authenticity/integrity only

• Note that the TCP ports are hidden when encrypted
  – good: better security, less is known about traffic
  – bad: impossible for FW to filter/traffic based on port

• Cost: can require many more resources than AH
Encapsulating Security Payload (ESP)

- Modifications to packet format

![Diagram of ESP packet structure]

- ESP Packet
- Authenticated
- Encrypted
Is AH necessary?

• Some argue that AH is subsumed by ESP
  – Header protection can be achieved by tunnel mode ESP
  – Protection of header has limited utility

• Should we allow firewalls (and eavesdroppers) to look at layer 4 (TCP) information
  – e.g., filter on ports
  – exposes a lot of information

• In practice, the protocol AH is generally not used.
IPsec Tunnel Mode

- Encapsulate IP packet
Practical Issues and Limitations

• IPsec implementations
  – Often not compatible (ungh.)
  – Large footprint
    • resource poor devices are in trouble
    • New standards to simplify (e.g., JFK, IKE2)
  – Slow to adopt new technologies

• Issues
  – IPsec tries to be “everything for everybody at all times”
    • Massive, complicated, and unwieldy
  – Policy infrastructure has not emerged
  – Large-scale management tools are limited (e.g., CISCO)
  – Often not used securely (common pre-shared keys)
Network Isolation: VPNs

• Idea: I want to create a collection of hosts which operate in a coordinated way
  – E.g., a virtual security perimeter over physical network
  – Hosts work as if they are isolated from malicious hosts

• Solution: Virtual Private Networks
  – Create virtual network topology over physical network
  – Use communications security protocol suites to secure virtual links “tunneling”
  – Manage networks as if they are physically separate
  – Hosts can route traffic to regular networks (split-tunneling)
VPN Example: RW/Telecommuter

Internet

LAN

Physical Link

Logical Link (IPsec)
VPN Example: Hub and Spoke

Internet

LAN

(network edge)

Physical Link

Logical Link (IPsec)
VPN Example: Mesh

Internet

LAN

(network edge)

Physical Link

Logical Link (IPsec)
Virtual LANs (VLANs)

• VPNs build with hardware
  – No encryption – none needed
  – “wire based isolation”
  – Switches increasingly support VLANs
  – Allows networks to be reorganized without rewiring

• Example usage: two departments in same hallway
  – Each office is associated with department
  – Configuring the network switch gives physical isolation
  – Note: often used to ensure QoS