More on Network Security
CS 239
Security for Networks and System Software
April 31, 2002

Outline

- IPSEC
- Firewalls
- Virtual private networks

IPSEC

- Until recently, the IP protocol had no standards for how to apply security
- Encryption and authentication layered on top
  - Or provided through ad hoc extensions
- Increasing security needs mandated a standard method of securing IP traffic

How Was This Handled?

- The usual way that enhancements to standard Internet protocols are handled
  - The RFC/IETF mechanism
- Smart people worked out a proposal
- They published the proposal and requested comments
- Eventually agreement was reached

IP Security RFCs

- RFC 1825
  - Security Architecture for the Internet Protocol
- RFC 1826
  - IP Authentication Header
- RFC 1827
  - IP Encapsulating Security Payload

Other Related RFCs

- RFC 1828 - IP Authentication Using Keyed MD5
- RFC 1829 - The ESP DES-CBC Transform
- RFC 1851 - The ESP Triple DES Transform
- RFC 1852 - IP Authentication Using Keyed SHA
- RFC 2085 - HMAC-MD5 IP Authentication With Replay Prevention
- And many, many others

RFC 1825

- Defined the basics of security for the Internet Protocol
- Briefly, add per-packet encryption and authentication standards
- Basically, two mechanisms
  - A way to authenticate IP packets
  - A way to encrypt IP packets

What Is Covered

- Message integrity
- Message authentication
- Message confidentiality

What Isn't Covered

- Non-repudiation
- Digital signatures
- Key distribution
- Traffic analysis
- Handling of security associations
- Some of these covered in later RFCs and related standards

Some Important Terms for IPSEC

- Security Association - "A set of security information related to a given network connection or set of connections"
  - Basically, a secure channel
- SPI (Security Parameters Index) - "An unstructured opaque index which is used in conjunction with the Destination Address to identify a particular Security Association"
  - Basically, a unique identifier

General Structure of IPSEC

- Really designed for end-to-end encryption
  - Though could do link level
- Designed to operate with either IPv4 or IPv6
- Meant to operate with a variety of different encryption protocols
- And to be neutral to key distribution methods

Security Associations

- Groups of entities that legitimately are cooperating in use of IPSEC for a particular connection
  - Hosts, applications, gateways, etc.
- Uniquely identified by:
  - Destination address
  - Plus a Security Parameter Index
    - Basically a pseudo-random number

Creating Security Associations

- Setting them up properly is a major task in itself
- Not covered in basic IPSEC RFCs
  - But being heavily studied
- Normally one way
  - Two way traffic requires two Security Associations

New IPSEC Headers

- The RFCs define two new types of headers for IP packets
  - The Authentication Header
  - The Encapsulating Security Payload

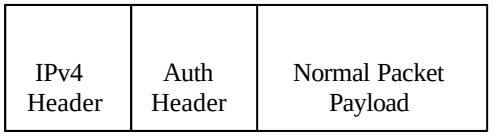
IP Authentication Header

- Provides integrity and authentication
  - Not confidentiality
- Calculated using all fields in the IP datagram
  - Except those that change in transit
  - So both data and headers are authenticated

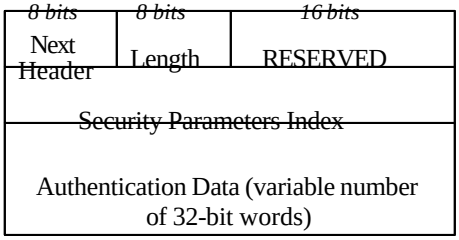
IP Authentication and Backwards Compatibility

- The authentication header is carried in the packet payload
- Non-participating routers can ignore it
- Participating routers know its payload location and can extract and check it as necessary

IPv4 Version of Packet With Authentication Header



What's In the Authentication Header?



Authentication Header Fields

- **Next header** identifies the next header in the packet
  - Possibly unrelated to IPSEC
- **Length** is length of this header's Authentication Data
- **Reserved** is, well, reserved
- **SPI** identifies the Security Association
- **Authentication data** is the actual "signature"

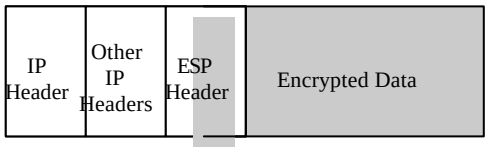
IP Encapsulating Security Payload (ESP)

- Encrypt the data and place it within the ESP
- The ESP has normal IP headers
- Can be used to encrypt just the real data of the packet
- Or the entire IP packet

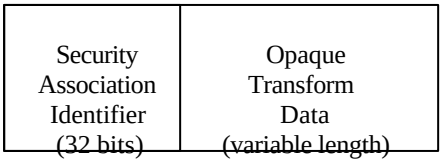
ESP Modes

- Tunnel mode
  - Original IP datagram is encrypted and placed in ESP
  - Unencrypted headers wrapped around ESP
- Transport mode
  - Encrypt just the transport-level data in the original packet
  - No IP headers encrypted

Secure IP Datagram Example



The ESP Header



Using ESP in Tunnel Mode

- Encrypt the IP datagram
  - The entire datagram
- Encapsulate it in a cleartext IP datagram
- Routers not understanding IPSEC can still handle it
- Receiver reverses the process

ESP in Transport Mode

- Extract the transport-layer frame
  - E.g., TCP, UDP, etc.
- Encapsulate it in an ESP
- Encrypt it
- The encrypted data is now the last payload of a cleartext IP datagram

What's the Status of IPSEC?

- The standard is done
- Widely implemented and used
  - In both Unix and Windows products
- The architecture doesn't require everyone to use it
- Generally considered to be a successful extension to IP

What More Is Needed?

- Key distribution
  - E.g., IKE
- Security association handling
  - Also dealt with by IKE
- Implementations of IPSEC and IKE are freely available
- More work on broadcast/multicast use

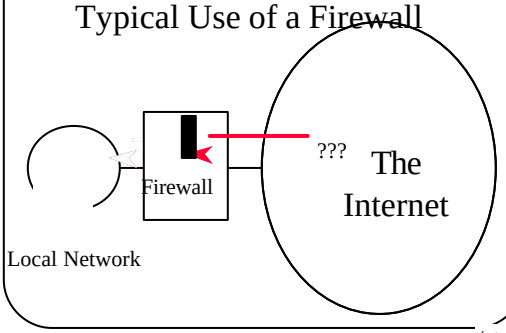
IPSEC and the AES Ciphers

- IPSEC is being adapted to use the new AES
- Currently, an Internet Draft memo describes using AES with IPSEC
- Further drafts looking at different modes/aspects of AES
- Expected that AES will become default for ESP in IPSEC

Firewalls

- "A system or combination of systems that enforces a boundary between two or more networks" - NCSA Firewall Functional Summary
- Usually, a computer that keeps the bad guys out

Typical Use of a Firewall



What Is a Firewall, Really?

- Typically a machine that sits between a LAN/WAN and the Internet
- Running special software
- That somehow regulates network traffic between the LAN/WAN and the Internet

Firewalls and Perimeter Defense

- Firewalls implement a form of security called *perimeter defense*
- Protect the inside of something by defending the outside strongly
  - The firewall machine is often called a *bastion host*
- Control the entry and exit points
- If nothing bad can get in, I'm safe, right?

Weaknesses of Perimeter Defense Models

- Breaching the perimeter compromises all security
- Windows passwords are a form of perimeter defense
  - If you get past the password, you can do anything
- Perimeter defense is part of the solution, not the entire solution

Types of Firewalls

- Filtering gateways
  - AKA screening routers
- Circuit gateways
  - Also a kind of screening router
- Application level gateways
  - AKA proxy gateways
- Hybrid (complex) gateways

Filtering Gateways

- Based on packet routing information
- Look at information in the incoming packets' headers
- Based on that information, either let the packet through or reject it

Example Use of Filtering Gateways

- Allow particular external machines to telnet into specific internal machines
  - Denying telnet to other machines
- Or allow full access to some external machines
- And none to others

A Fundamental Problem

- Today's IP packet headers aren't authenticated
  - And are pretty easy to forge
- If your filtering firewall trusts packet headers, it offers little protection
- Situation may be improved by IPSEC
  - But hasn't been yet

One Exception to This Problem

- Checking internal addresses
- Safety procedures inside the security perimeter may limit some services to LAN members
- The firewall can check that incoming packets don't claim to be internal to the LAN

Filtering Based on Ports

- Most incoming traffic is destined for a particular machine and port
  - Which can be derived from the IP and TCP headers
- Only let through packets to select machines at specific ports
- Makes it impossible to externally exploit flaws in little-used ports
  - If you configure the firewall right . . .

Pros and Cons of Filtering Gateways

+ Fast
+ Cheap
+ Flexible
+ Transparent
– Limited capabilities
– Dependent on header authentication
– Generally poor logging
– May rely on router security

Circuit Gateways

- Another kind of filtering firewall
- Used when internal machines request service from machines outside the firewall
- Makes it look like the request came from the firewall
  - Concealing internal system details

Application Level Gateways

- Also known as proxy gateways
- Firewalls that understand the application-level details of network traffic
  - To some degree
- Traffic is accepted or rejected based on the probable results of accepting it

How Application Level Gateways Work

- The firewall serves as a general framework
- Various proxies are plugged into the framework
- Incoming packets are examined
  - And handled by the appropriate proxy

Firewall Proxies

- Programs capable of understanding particular kinds of traffic
  - E.g., FTP, HTTP, videoconferencing
- Proxies are specialized
- A good proxy must have deep understanding of the network application

An Example Proxy

- A proxy to audit email
- What might such a proxy do?
  - Only allow email from particular hosts through
  - Or from particular users
  - Or filter out email with unsafe inclusions (like executables)

What Are the Limits of Proxies?

- Proxies can only test for threats they understand
- Either they must permit a very limited set of operations
- Or they must have deep understanding of the program they protect
  - If too deep, they may share the flaw

Pros and Cons of Application Level Gateways

+ Highly flexible
+ Good logging
+ Content-based filtering
+ Potentially transparent
– Slower
– More complex and expensive
– A good proxy is hard to find

Hybrid Gateways

- A combination of two or more other types
  - Typically filtering gateways and proxy gateways
- Are they better?
  - If in parallel, no
  - If in series, maybe

Firewall Characteristics

- Statefulness
- Transparency
- Firewalls and authentication
- Firewalls and encryption
- Firewalls and viruses

Stateful Firewalls

- Much network traffic is connection-oriented
  - E.g., telnet and videoconferencing
- Proper handling of that traffic requires the firewall to maintain state
- But handling information about connections is more complex

Firewalls and Transparency

- Ideally, the firewall should be invisible
  - Except when it vetoes access
- Users inside should be able to communicate outside without knowing about the firewall
- External users should be able to invoke internal services transparently

Firewalls and Authentication

- Many systems want to allow specific sites or users special privileges
- Firewalls can only support that to the extent that strong authentication is available
  - At the granularity required
- For general use, may not be possible
  - In current systems

Firewalls and Encryption

- Firewalls provide no confidentiality
  - For data they pass back and forth
- Unless the data is encrypted
- But if the data is encrypted, the firewall can't examine it
- So typically the firewall must be able to decrypt
  - Or only work on unencrypted parts of packets

Firewalls and Link Encryption

- Inter-firewall encryption is essentially link level encryption
  - With all inherent problems
  - Except (presumably) that only trusted machines encrypt and decrypt
- More encryption can be applied at the application level
  - Limiting the firewall's options

Firewalls and Viruses

- Firewalls are an excellent place to check for viruses
- Virus detection software can be run on incoming executables
- Requires that firewall knows when executables come in
- And must be reasonably fast

Firewall Configuration and Administration

- Again, the firewall is the point of attack for intruders
- Thus, it must be extraordinarily secure
- How do you achieve that level of security?

Firewall Hardening

- Devote a special machine only to firewall duties
- Alter OS operations on that machine
  - To allow only firewall activities
  - And to close known vulnerabilities
- Strictly limit access to the machine
  - Both login and remote execution

Firewalls and Logging

- The firewall is the point of attack for intruders
- Logging activities there is thus vital
- The more logging, the better
- Should log what the firewall allows
- And what it denies
- Tricky to avoid information overload

Closing the Back Doors

- Firewall security is based on assumption that all traffic goes through the firewall
- So be careful with:
  - Modem connections
  - Wireless connections
  - Portable computers
- Put a firewall at every entry point to your network
- And make sure all your firewalls are up to date

Virtual Private Networks

- VPNs
- What if your company has more than one office?
- And they're far apart?
  - Like on opposite coasts of the US
- How can you have secure cooperation between them?

Leased Line Solutions

- Lease private lines from some telephone company
- The phone company ensures that your lines cannot be tapped
  - To the extent you trust in phone company security
- Can be expensive and limiting

Another Solution

- Communicate via the Internet
  - Getting full connectivity, bandwidth, reliability, etc.
  - At a lower price, too
- But how do you keep the traffic secure?
- Encrypt everything!

Encryption and Virtual Private Networks

- Use encryption to convert a shared line to a private line
- Set up a firewall at each installation's network
- Set up shared encryption keys between the firewalls
- Encrypt all traffic using those keys

Is This Solution Feasible?

- A VPN can be half the cost of leased lines (or less)
- And give the owner more direct control over the line's security
- If IPSEC succeeds, deployment and interoperation should be easy

Key Management and VPNs

- All security of the VPN relies on key secrecy
- How do you communicate the key?
  - In early implementations, manually
  - Modern VPNs use something like IKE
- How often do you change the key?
  - IKE allows frequent changes

VPNs and Firewalls

- VPN encryption is typically done between firewall machines
- Do I need the firewall for anything else?
- Probably, since I still need to allow non-VPN traffic in and out