

Today's Topics

- **SSL/TLS**
 - Server Certificates
 - Client Certificates
- **Certification Authorities**
 - Trust
 - Registration Authorities
- **VPN**
 - IPSec
 - Client tunnels
 - LAN-to-LAN tunnels

Secure Sockets Layer

- Secure Sockets Layer (version 3.0)
- According to the specification...
 - “The primary goal of the SSL Protocol is to provide privacy and reliability between two communicating applications.
 - The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. ”

Secure Sockets Layer

- Designed with four basic goals
 - Cryptographic security
 - Interoperability
 - Extensibility
 - Relative efficiency

Secure Sockets Layer

- SSL has three basic properties:
 - The connection is private. Encryption is used after an initial handshake to define a secret key. Symmetric cryptography is used for data encryption (e.g., DES, RC4, etc.)
 - The peer's identity can be authenticated using asymmetric, or public key, cryptography (e.g., RSA, DSS, etc.).
 - The connection is reliable. Message transport includes a message integrity check using a keyed MAC. Secure hash functions (e.g., SHA, MD5, etc.) are used for MAC computations.

SSL/TLS

- Well then, what is TLS?
 - Transport Layer Security (version 1.0)
- SSL was developed by Netscape.
 - The standards community wanted their own version, free from any patents/restrictions
- Thus was born TLS
 - IETF changed the name to avoid showing bias
 - I'll use the two terms interchangeably

SSL/TLS

- <ftp://ftp.isi.edu/in-notes/rfc2246.txt>
 - “The TLS protocol provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. “
- Sound familiar?
- TLS v1.0 == SSL v3.1

SSL/TLS

- Users want to connect to servers without the connection being listened to
 - Electronic commerce
 - Grades
 - Health care
 - Other...
- Every server has a certificate
 - Basically a public key
 - Signed by a trusted third party

Server Certificates

- X509 version 3 is the current specification
- Certs hold three important bits of info
 - Name of Server
 - Public Key of Server
 - Issued by a *trusted* organization

X509 Certificates: example

Version
Serial Number
Algorithm ID
Issuer (DN)
Period of Validity
Subject
Subject's Public Key
Extensions
Issuers Signature

3
04:60:00:00:02
md5WithRSAEncryption
C=US,O=FooBar, OU=my CA
Not Before: Nov 17 00:00:00 1999 GMT Not After : Nov 17 00:00:00 2003 GMT
C=US,O=MyDomain,CN=www.domain.com
00:e1:73:65:2d:00:77...
CA:False
51:e4:df:76:c3:97:20:6c...

So, What does a certificate look like?

Certificate:

Data: Version: 3 (0x2)

Serial Number: 1234567 (0xabcdef)

Signature Algorithm: sha1WithRSAEncryption

Issuer: C=US, ST=Massachusetts, O=Trusted CA Company,
CN=Trusted CA v0.1/Email=pkimaster@trust.com


Validity: Not Before: Mar 4 17:55:21 2002 GMT
Not After : Nov 28 17:55:21 2004 GMT

Subject: C=US, ST=Massachusetts, O=My Enterprises,
CN=www.myent.com/Email=pki@myent.com

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

RSA Public Key: (2048 bit)

 Modulus (2048 bit): 00:cc:4d:
97:a7:c6:<.....>:f9:35:47:83

 Exponent: 65537 (0x10001)

X509v3 Basic Constraints: CA:FALSE

Certificate:

Signature Algorithm: sha1WithRSAEncryption c8:fc:eb:
35:2d:ce:95:<.....>:6e:71:31:3f:6a:10:e3

RSA

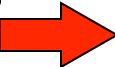
- Public key = (n,e)
- Private key = (n,d)

- Encryption of a character M_i
 - $C_i = M_i^e \pmod n$
- Decryption of a cipher character C_i
 - $M_i = C_i^d \pmod n$

n 

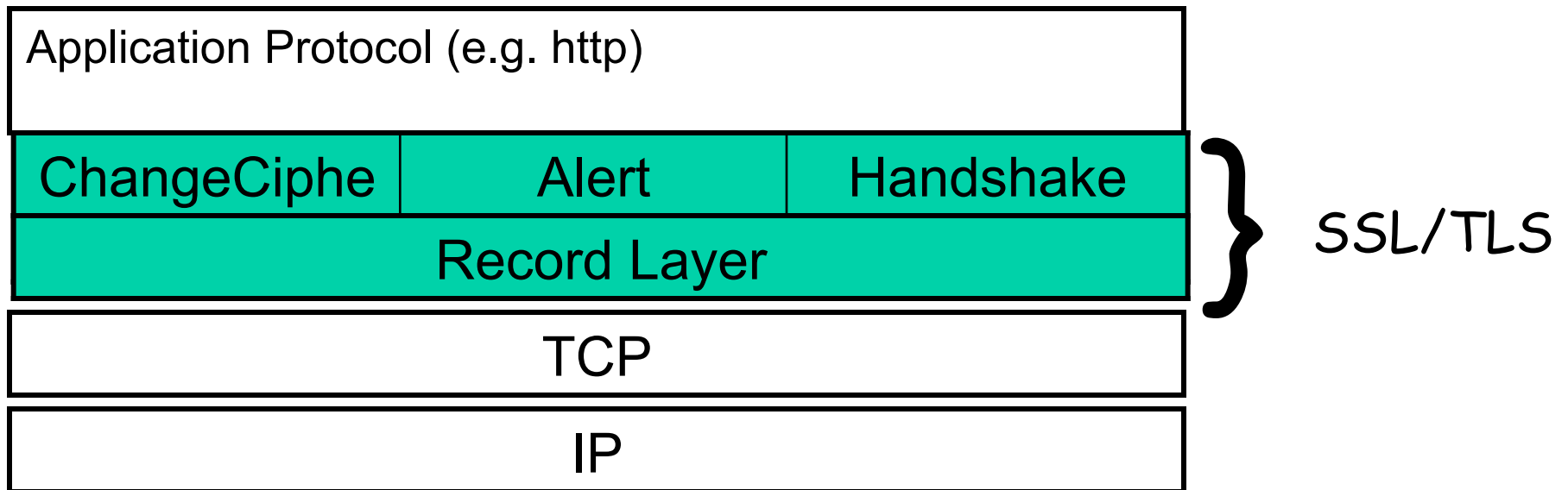
Modulus (2048 bit):

00:e2:62:13:dc:ab:73:f8:42:d8:13:bb:6e:09:19:
75:2e:d8:2b:9f:31:d7:d4:7e:b3:12:84:21:d3:91:
5d:46:99:be:eb:eb:94:38:b5:15:cd:29:4f:e2:20:
8e:01:c9:ce:a9:20:cc:99:1f:33:e5:6b:51:fe:c7:
99:54:31:73:ab:f5:19:92:79:46:a4:7e:da:74:ad:
66:d2:77:ce:85:9f:be:b8:27:2f:77:d4:5d:c2:41:
b7:f4:06:10:ea:6d:d0:1d:07:c4:d5:41:fe:28:9f:
a7:0e:b2:ed:7b:14:18:3f:1d:af:81:65:97:16:ad:
63:f6:e0:2f:5e:84:75:8a:d3:67:21:c4:ba:a4:5b:
24:d7:34:2c:7a:4a:c7:b4:76:e3:d8:f0:ab:50:81:
e8:d0:fc:10:2b:33:56:7b:74:03:d9:31:d5:f1:f4:
e4:f2:e5:db:29:ba:7a:29:5f:ac:07:f7:f2:84:4d:
4a:2b

e 

Exponent: 65537 (0x10001)

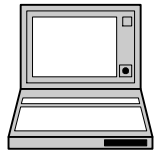
SSL/TLS



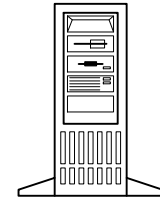
SSL consists of two protocol layers

- The Record Layer encapsulates all messages
 - The ChangeCipherSpec protocol indicates the channel is ready for secure communications
 - The Alert protocol indicates errors or other caution conditions have occurred in the connection
 - The Handshake protocol negotiates all options of the session

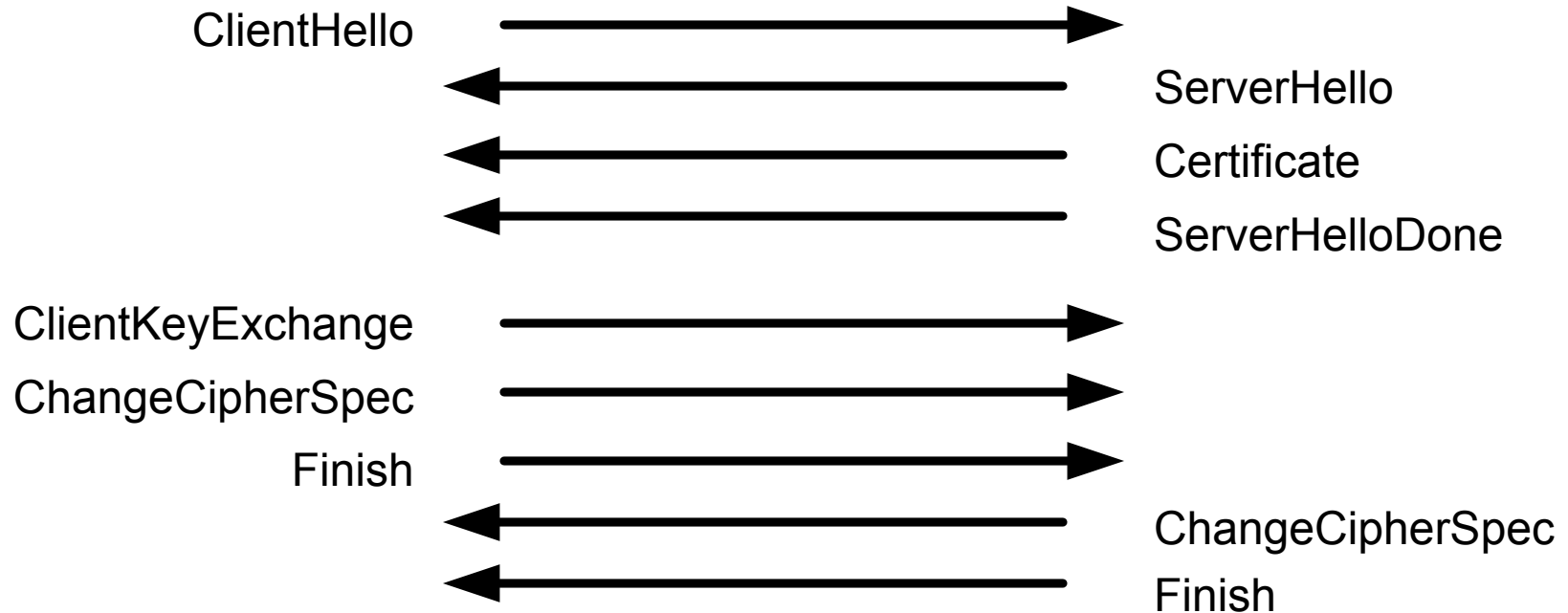
SSL Session Negotiation: Server Authentication



Client



Server



Client is responsible for checking:

- If the Issuer's signature on the certificate is valid
- If the certificate is within the period of validity
- If the Subject (CN) is identical to the server DNS name

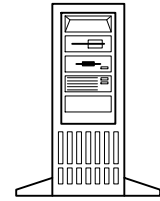
Client Certificates

- Basically they are the same as server certs
 - Are you really any different than a server?
- Again, they need to be signed by a trusted third party (the Issuer)
 - Who do you trust?
- But, how do we name everyone uniquely?
 - Problem, big problem...

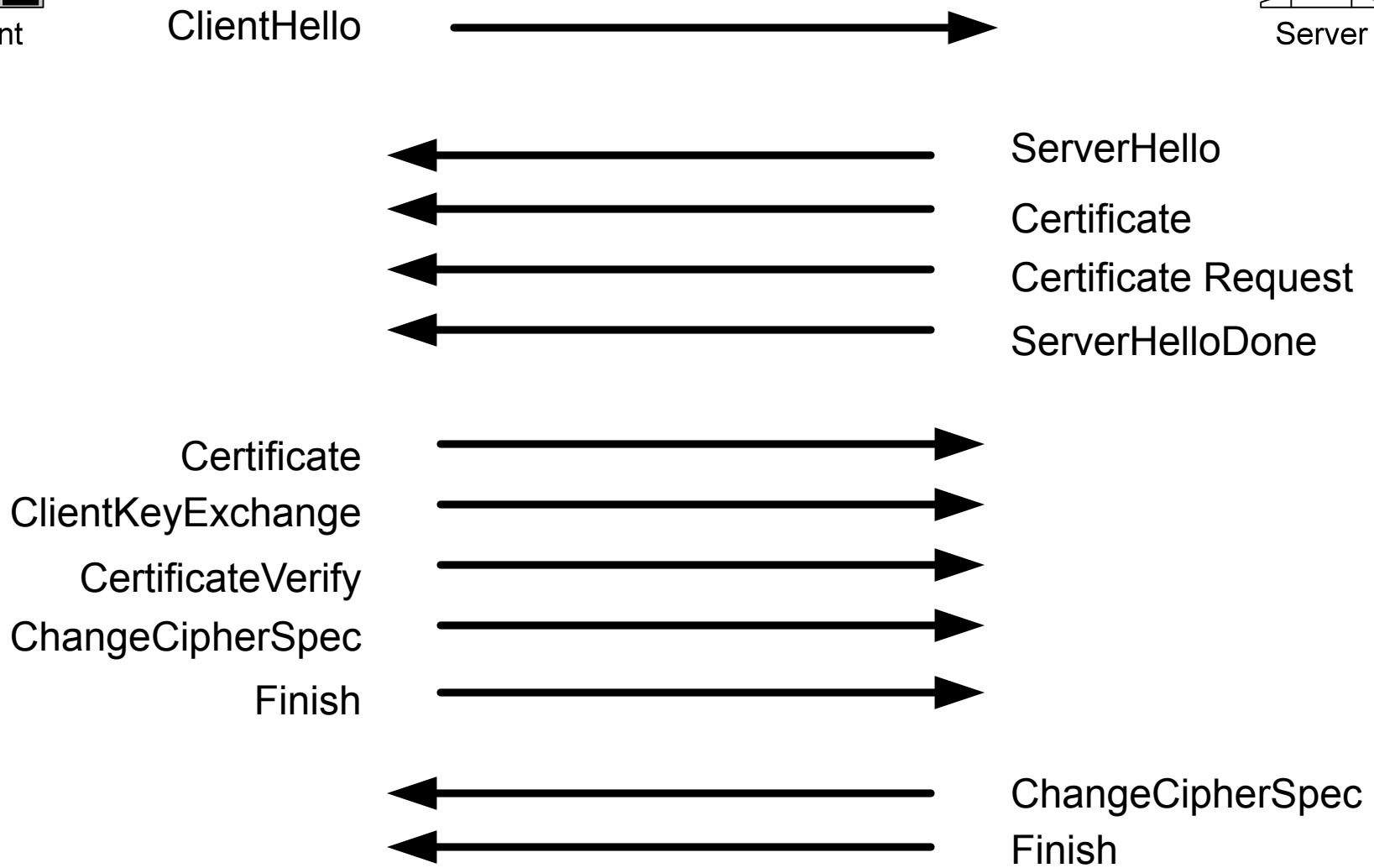
SSL Session Negotiation: Client and Server Authentication



Client



Server



Certification Authority (CA)

- The CA is the trusted third party
 - We've talked about trust before
- All certificates are signed with the CA's private key
 - Including the CA's signing cert...
- Better protect that private key pretty well
 - Can you spell liability?
 - CP/CPS

Who do you trust?

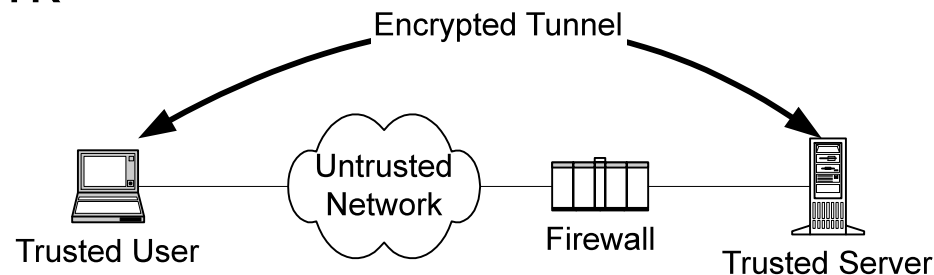
- subject=/C=US/O=VeriSign, Inc./OU=Class 1 Public Primary Certification Authority - G2/OU=(c) 1998 VeriSign, Inc. - For authorized use only/OU=VeriSign Trust Network issuer= /C=US/O=VeriSign, Inc./OU=Class 1 Public Primary Certification Authority - G2/OU=(c) 1998 VeriSign, Inc. - For authorized use only/OU=VeriSign Trust Network
- subject=/L=Internet/O=VeriSign, Inc./OU=VeriSign Individual Software Publishers CA issuer= /L=Internet/O=VeriSign, Inc./OU=VeriSign Individual Software Publishers CA
- subject=/C=ZA/ST=Western Cape/L=Cape Town/O=Thawte Consulting cc/OU=Certification Services Division/CN=Thawte Server CA/Email=server-certs@thawte.com issuer= /C=ZA/ST=Western Cape/L=Cape Town/O=Thawte Consulting cc/OU=Certification Services Division/CN=Thawte Server CA/Email=server-certs@thawte.com
- subject=/C=US/O=RSA Data Security, Inc./OU=Secure Server Certification Authority issuer= /C=US/O=RSA Data Security, Inc./OU=Secure Server Certification Authority
- subject=/CN=Root SGC Authority issuer= /CN=Root SGC Authority
- subject=/OU=Copyright (c) 1997 Microsoft Corp./OU=Microsoft Corporation/CN=Microsoft Root Authority issuer= /OU=Copyright (c) 1997 Microsoft Corp./OU=Microsoft Corporation/CN=Microsoft Root Authority
- subject=/C=US/O=MSFT/CN=Microsoft Authenticode(tm) Root Authority issuer= /C=US/O=MSFT/CN=Microsoft Authenticode(tm) Root Authority
- subject=/C=US/O=MCI/OU=internetMCI/OU=MALL issuer= /C=US/O=MCI/OU=internetMCI/OU=MALL
- subject=/C=CA/CN=Keywitness Canada Inc. keywitness@keywitness.ca issuer= /C=CA/CN=Keywitness Canada Inc. keywitness@keywitness.ca
- subject=/C=US/O=KeyWitness International, Inc./dnQualifier=OID.1.2.840.113549.1.1.1/CN=KeyWitness 2048 Root issuer= /C=US/O=KeyWitness International, Inc./dnQualifier=OID.1.2.840.113549.1.1.1/CN=KeyWitness 2048 Root
- subject=/C=US/O=GTE Corporation/CN=GTE CyberTrust Root issuer= /C=US/O=GTE Corporation/CN=GTE CyberTrust Root
- subject=/C=US/O=GTE Corporation/OU=GTE CyberTrust Solutions, Inc./CN=GTE CyberTrust Global Root issuer= /C=US/O=GTE Corporation/OU=GTE CyberTrust Solutions, Inc./CN=GTE CyberTrust Global Root
- subject=/C=US/O=AT&T/OU=Directory Services issuer= /C=US/O=AT&T/OU=Directory Services
- subject=/O=Microsoft Trust Network/OU=Microsoft Corporation/OU=Microsoft Time Stamping Service Root/OU=Copyright (c) 1997 Microsoft Corp. issuer= /O=Microsoft Trust Network/OU=Microsoft Corporation/OU=Microsoft Time Stamping Service Root/OU=Copyright (c) 1997 Microsoft Corp.
- subject=/C=US/O=VeriSign, Inc./OU=Class 1 Public Primary Certification Authority issuer= /C=US/O=VeriSign, Inc./OU=Class 1 Public Primary Certification Authority
- subject=/C=US/O=AT&T/OU=Certificate Services issuer= /C=US/O=AT&T/OU=Certificate Services

Courtesy Netscape...



Virtual Private Networks (VPN)

- What is a VPN?
 - “...a group of two or more computer systems, typically connected to a private network with limited public-network access, that communicates ‘securely’ over a public network.”
 - “A combination of tunneling, encryption, authentication and access control technologies and services used to carry traffic over an IP network”



Virtual Private Networks (VPN)

- What makes a VPN secure?
 - Encryption
 - Strong authentication of remote users and hosts.
 - Mechanisms for hiding or masking information about the private network topology from potential attackers
- Three basic types:
 - Hardware-based
 - Firewall-based
 - Standalone/Software-based

IPSec

- IPSec is the *IP Security* standard from the IETF (the people that standardize the Internet)
 - rfc1825
- IPSec consists of two different headers
 - Authentication Header (AH) protocol
 - Encapsulating Security Payload (ESP) protocol
- Both protocols assume the peers using the protocol have a shared key.

IPSec

- Both protocols assume the peers using the protocol share authentication information.
- In addition there is a protocol for distributing keys called **IKE**.
 - **Internet Key Exchange**
- Why was IPSec designed as two protocols?
 - To encourage wide deployment, even where there are import, export, and usage restrictions on encryption.
 - **Cryptography is covered under ITAR.**

IP Authentication Header (AH)

- Designed to provide
 - Integrity
 - Authentication
- **Does not provide**
 - **Confidentiality**

AH header includes:

- connection identifier
- authentication data: signed message digest, calculated over original IP datagram, providing source authentication, data integrity.
- Next header field: specifies type of data (TCP, UDP, ICMP, etc.)

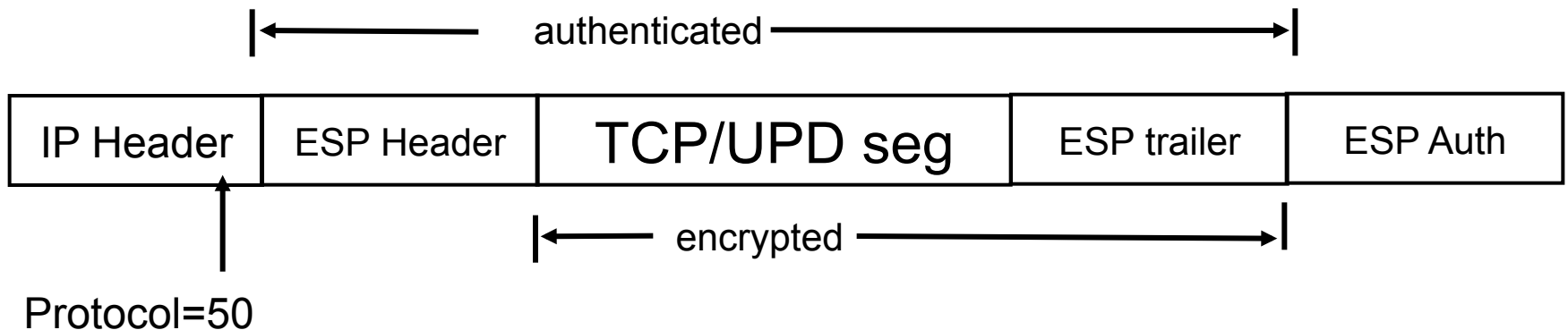


Protocol=51

This is a network-layer protocol! Not an application-level protocol.

IP Encapsulating Security Payload (ESP)

- Designed to provide
 - Integrity
 - Authentication
 - Confidentiality
- Data, ESP trailer encrypted.
- Next header field is in ESP trailer.
- ESP authentication field is similar to AH authentication field.
- Protocol = 50.



IKE

- A hybrid protocol designed to negotiate and provide authenticated keying material for **security associations (SA)** in a protected manner.
 - An SA is a set of policy and keys used to protect information
- **Based on three previous protocols**
 - **ISAKMP** – A framework for authentication and key exchanges, but does not define them.
 - **Oakley** – A described series of key exchanges and the services provided by them.
 - **SKEME** – A versatile key exchange technique providing anonymity, repudiability, and quick key refreshment.
- **IKE is a protocol using part of Oakley and part of SKEME in conjunction with ISAKMP to obtain authenticated keying material.**
 - IKE is one implementation of ISAKMP to be used with IPSec

IPSec Security

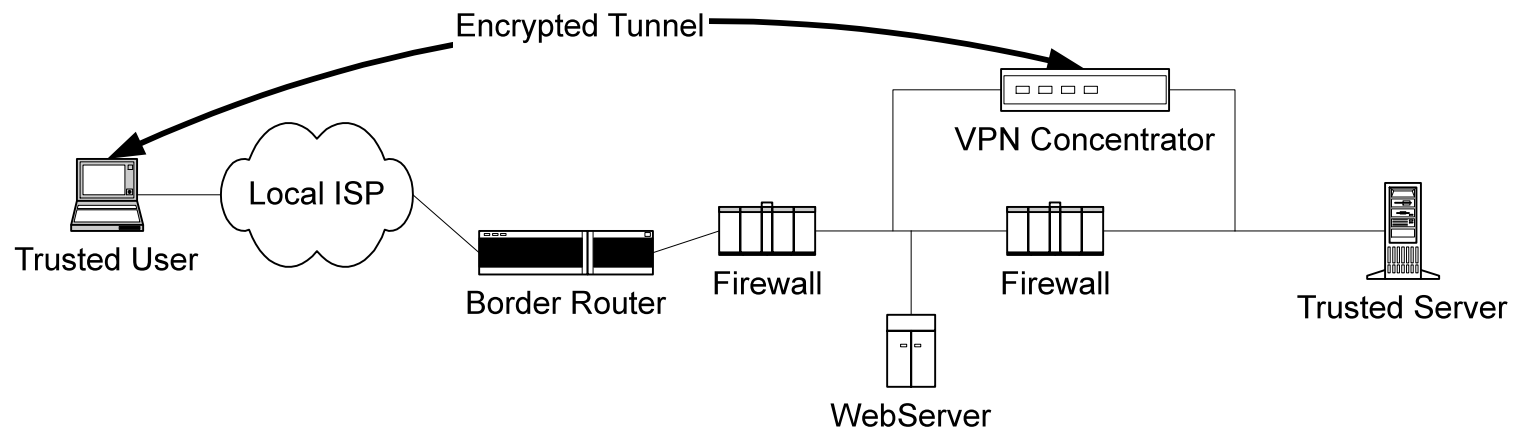
- Why don't we cover IKE? The protocol is *very complex*
 - “Security’s worst enemy is complexity”
 - “...(the) chief complaint in this tract is the min-numbing complexity of the IPSec standards document, and indeed in the protocol itself”
- There is a great deal of known plaintext in IPSec traffic
 - Encrypted TCP/IP header field data.

IPSec Security

- The protocol is *very complex*
 - “Security’s worst enemy is complexity”
 - “...(the) chief complaint in this tract is the min-numbing complexity of the IPSec standards document, and indeed in the protocol itself”
- There is a great deal of known plaintext in IPSec traffic
 - Encrypted TCP/IP header field data.

Client Tunnels

- Client runs VPN software
- IP traffic between Trusted user and VPN concentrator
 - Can establish normally blocked connections between trusted user and server
 - Border firewall only needs to allow VPN traffic destined for the VPN concentrator



Client Tunnels

- Authentication
 - Shared secret
 - All the standard scalability problems...
 - Client certificates
 - Storage of client certificates potentially insecure
 - Requires a Certification Authority.
 - Trust???

Other VPN Protocols

- In addition to IPSec, there are a few other protocols worth mentioning
 - PPTP
 - L2F
 - L2TP

PPTP

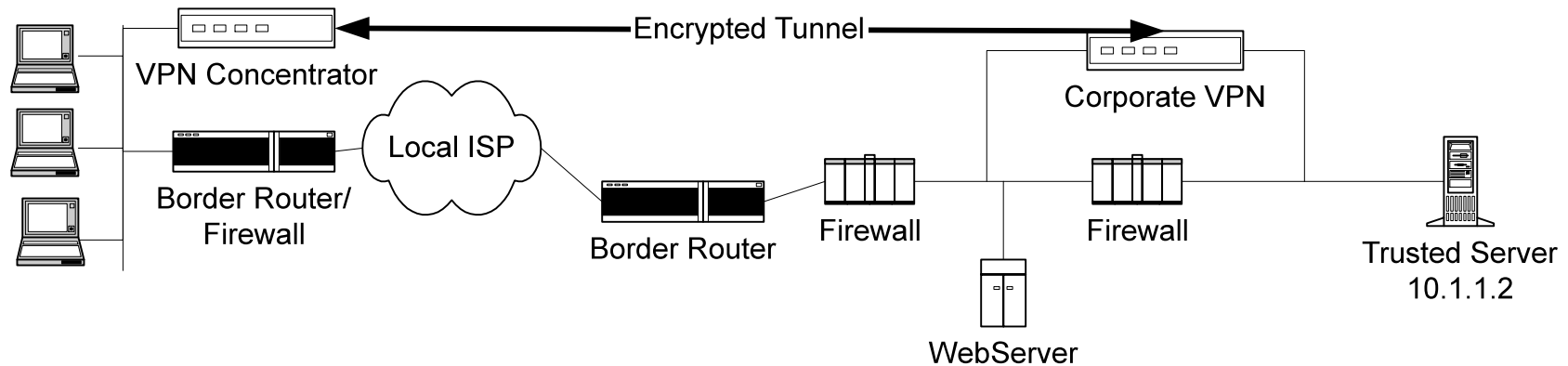
- Point-to-Point Tunneling protocol
 - PPP encapsulated over IP
 - PPTP was originally developed by a consortium including Microsoft.
 - The protocol was originally designed as an encapsulation mechanism, to allow the transport of non-TCP/IP protocols (such as IPX) over the Internet using Generic Routing Encapsulation (GRE).
 - Version 1 was full of security holes
 - Flawed encryption mechanism – non-random keys, session keys weak hash of user password, key lengths too short (non-configurable)
 - Bad password management in mixed Win95/NT environment; static passwords easily compromised
 - Vulnerable to server spoofing attacks because packet authentication not implemented, easy denial-of-service attacks even inside firewalls

Other Protocols

- **L2F -- Layer 2 Forwarding**
 - Media independent layer 2 tunneling protocol from Cisco
 - A standards based tunneling mechanism for transporting link-layer frames (e.g. HDLC, PPP, SLIP over higher-layer protocols)
- **L2TP – Layer 2 Transport Protocol**
 - Encapsulates PPP frames to be sent over IP, X25, Frame Relay or ATM networks.
 - Requires IPSec to secure underlying IP transport
 - Take one part PPTP, one part L2F, shake liberally...

LAN-to-LAN Tunnels

- Sometimes we want to tunnel more than one computer over a single logical link
 - Only the remote concentrator needs a routable IP
 - Generally, this is a whole lot cheaper than leased lines to n different remote offices
 - Sometime referred to as node-to-node tunnels



VPN Summary

- There are a lot of products out there, the trick is picking the good ones.
- Encryption is a necessary, but not sufficient condition for security
- Security is a process, not a product...
- Don't trust vendors claims (PPTP)
- A VPN is not a substitute for policies and auditing
- Better make sure you secure that VPN concentrator.