

Secure Teleconference over SSL

Inja Youn

ECE 746 Project
May 17, 2005 Spring

Outline

- Purpose
- Background (OpenSSL)
- Software Architecture
- Experiments and Results
- Contribution
- Conclusion

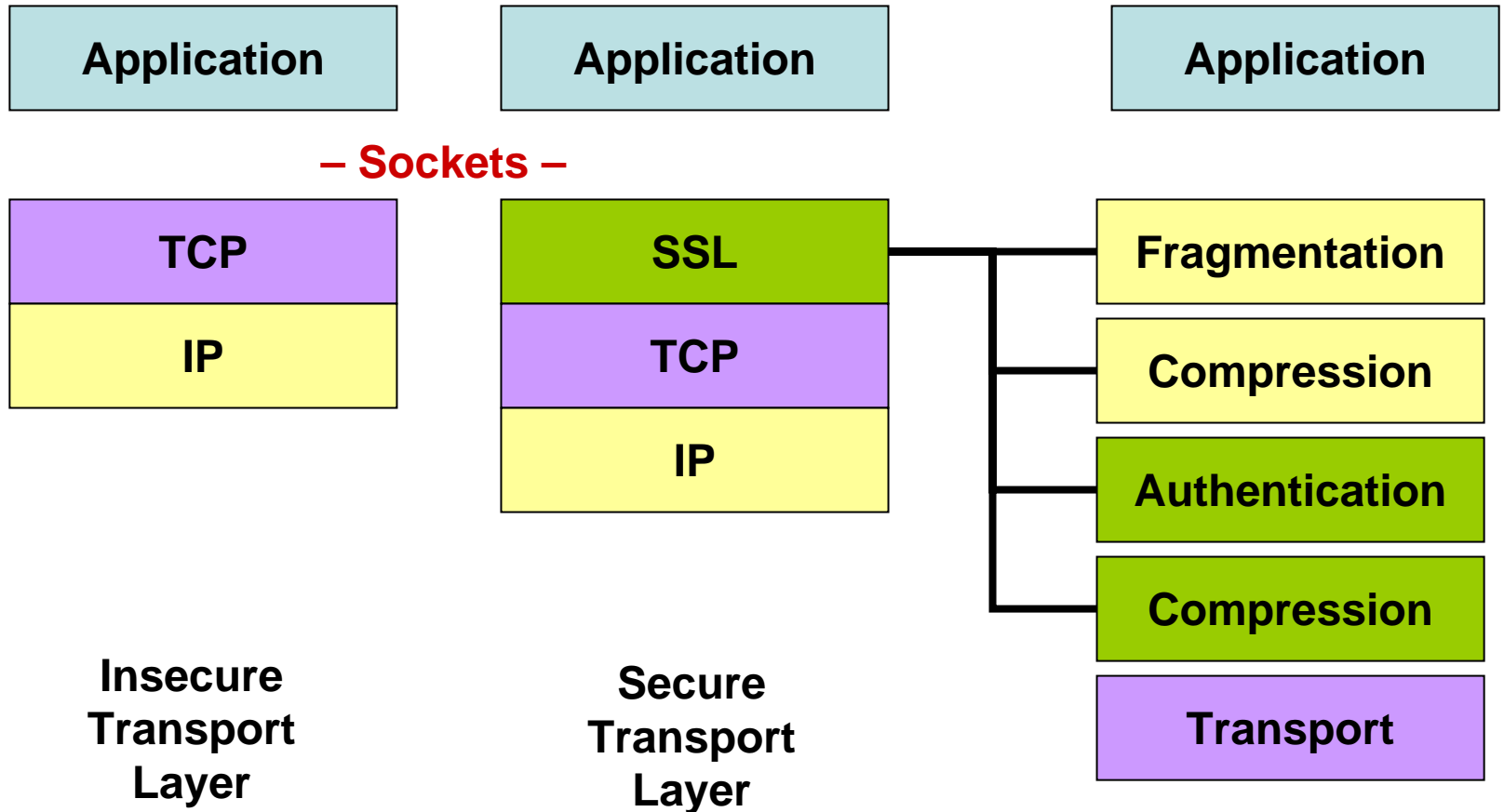
Purpose

- Provide **reliable security services** for teleconference using OpenSSL
- Address the performances represented by the following categories:
 - Certificate schemes
 - Key agreement schemes
 - Encryption algorithms
 - Comparison

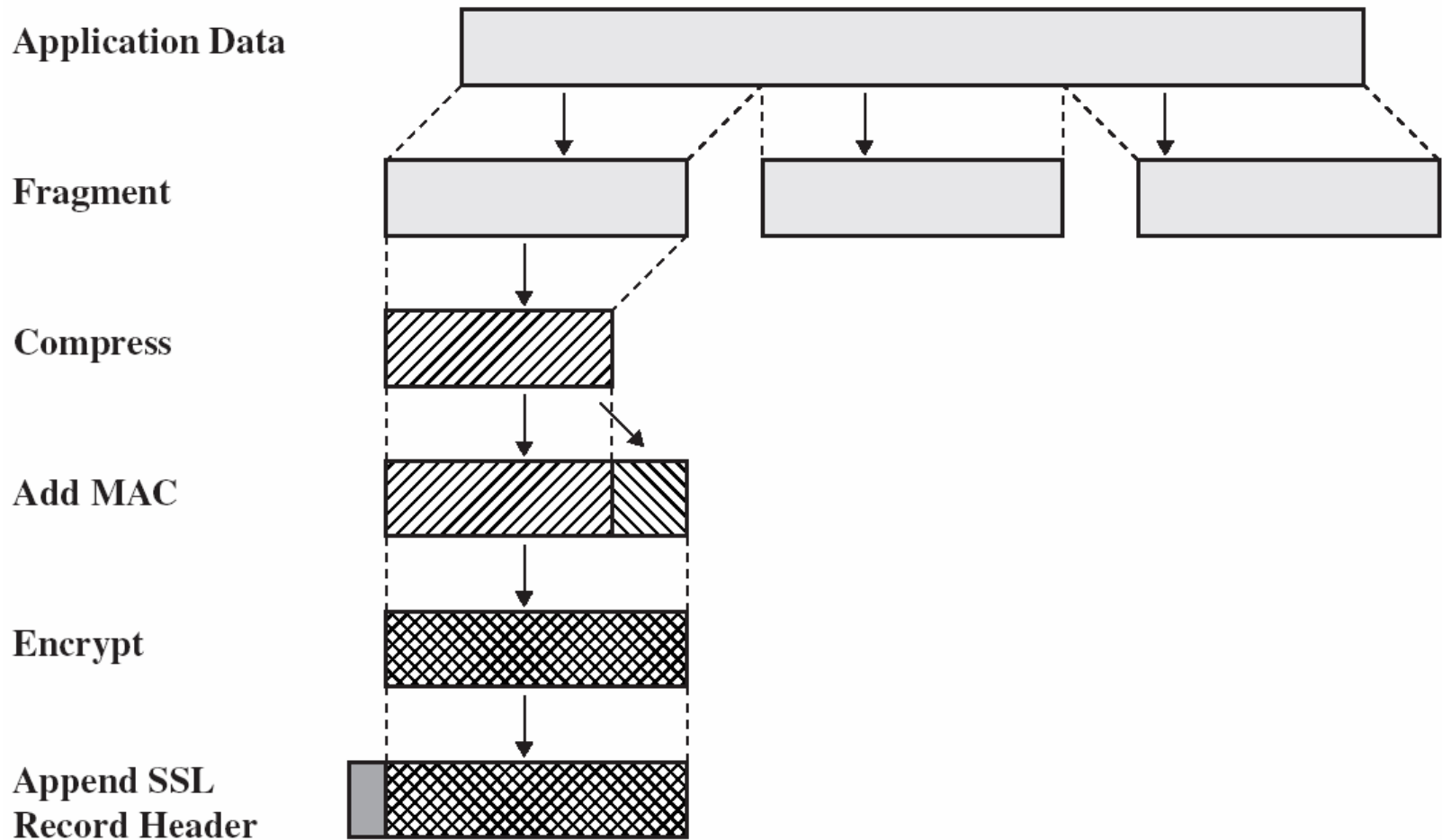
Background

- OpenSSL - Good Enough?
 - Open source (free of charge)
 - Fully Featured SSL implementation
 - Provides strong cryptographic combinations of PKI, key exchange algorithms, symmetric key algorithms, message authentication codes
- Secure Sockets Layer (SSL)
 - Capability of authentication of both client and server
 - Application independent
 - Capability of key agreement
 - Encryption, authentication and message authentication codes (MAC) for achieving the integrity of the transmission

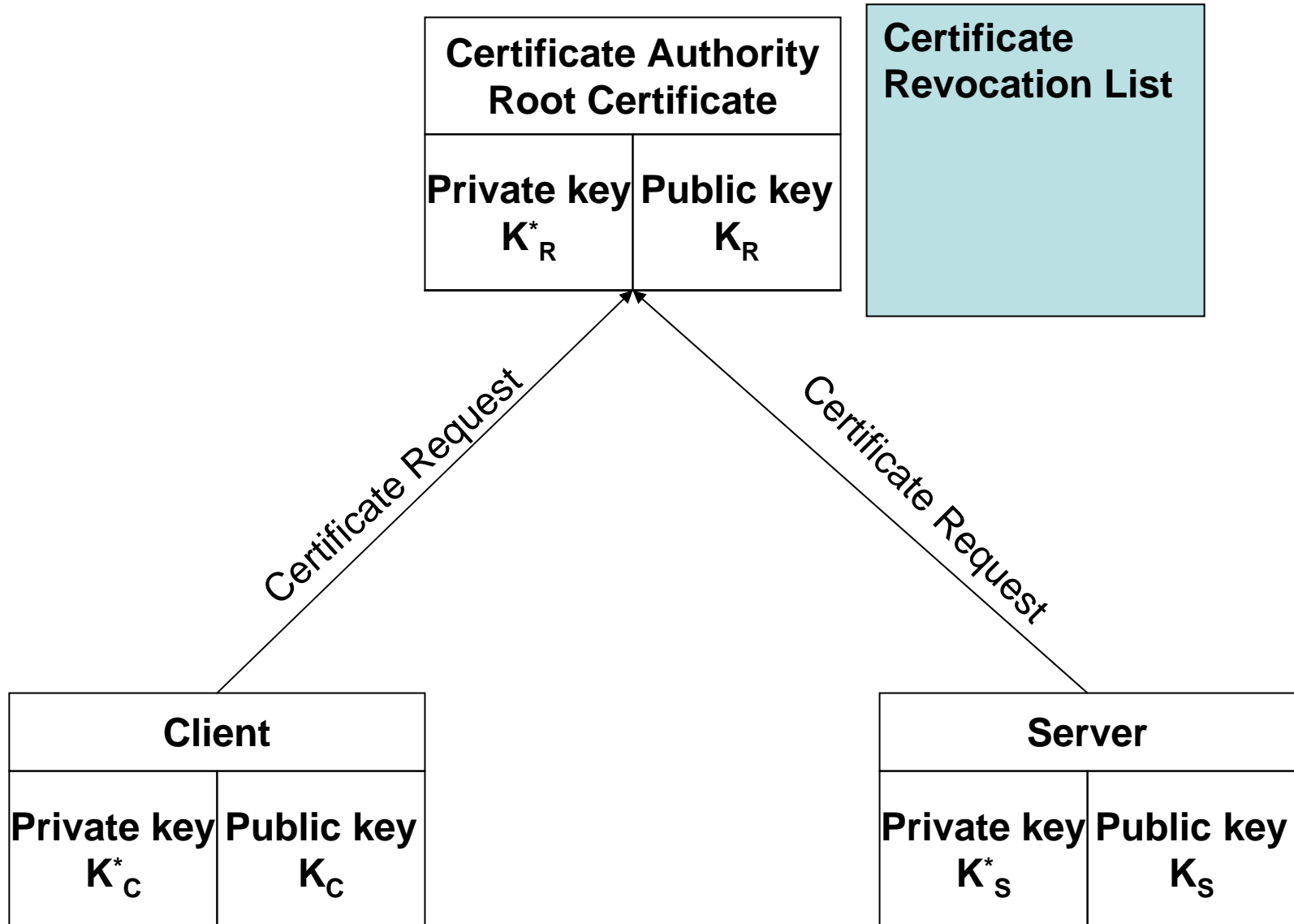
OpenSSL Protocol Layers



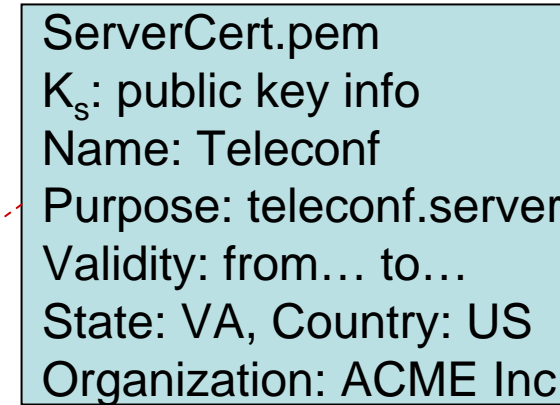
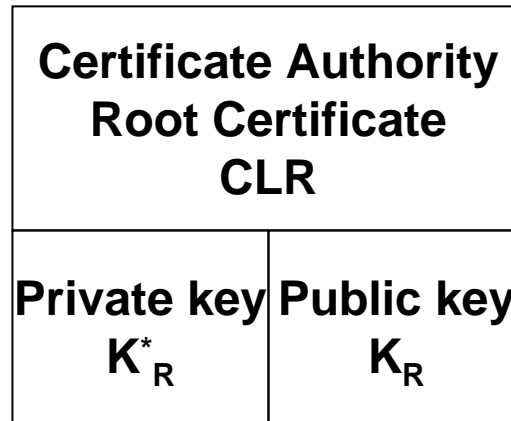
SSL Record Structure



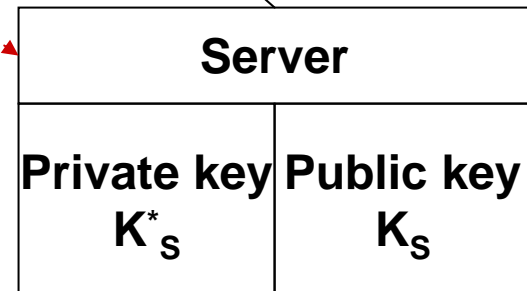
Certificate Checking



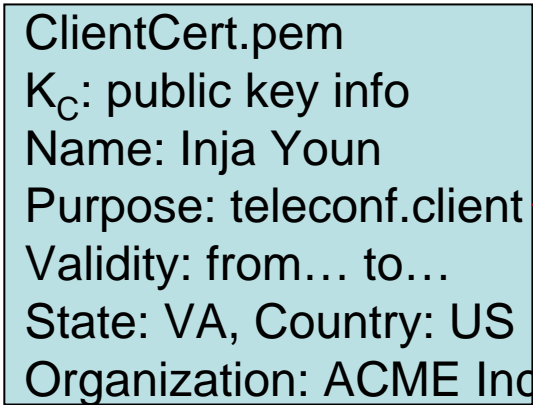
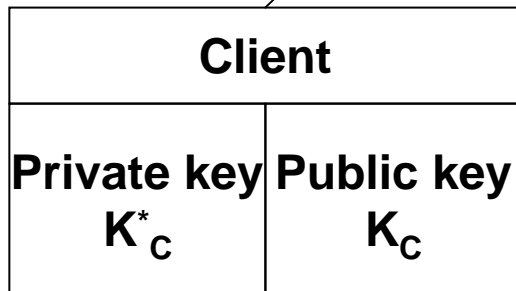
Certificate Checking



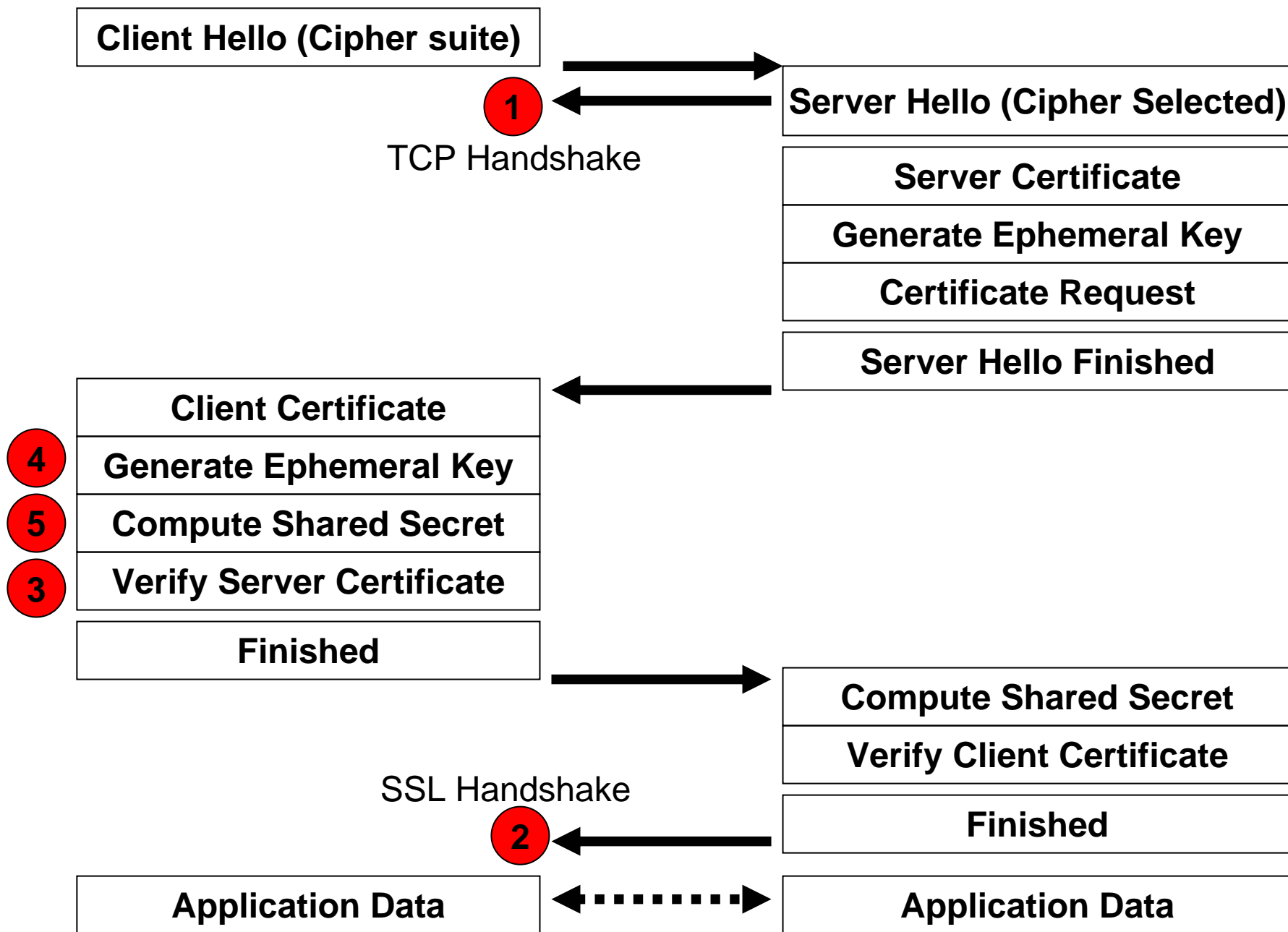
Signed Certificate



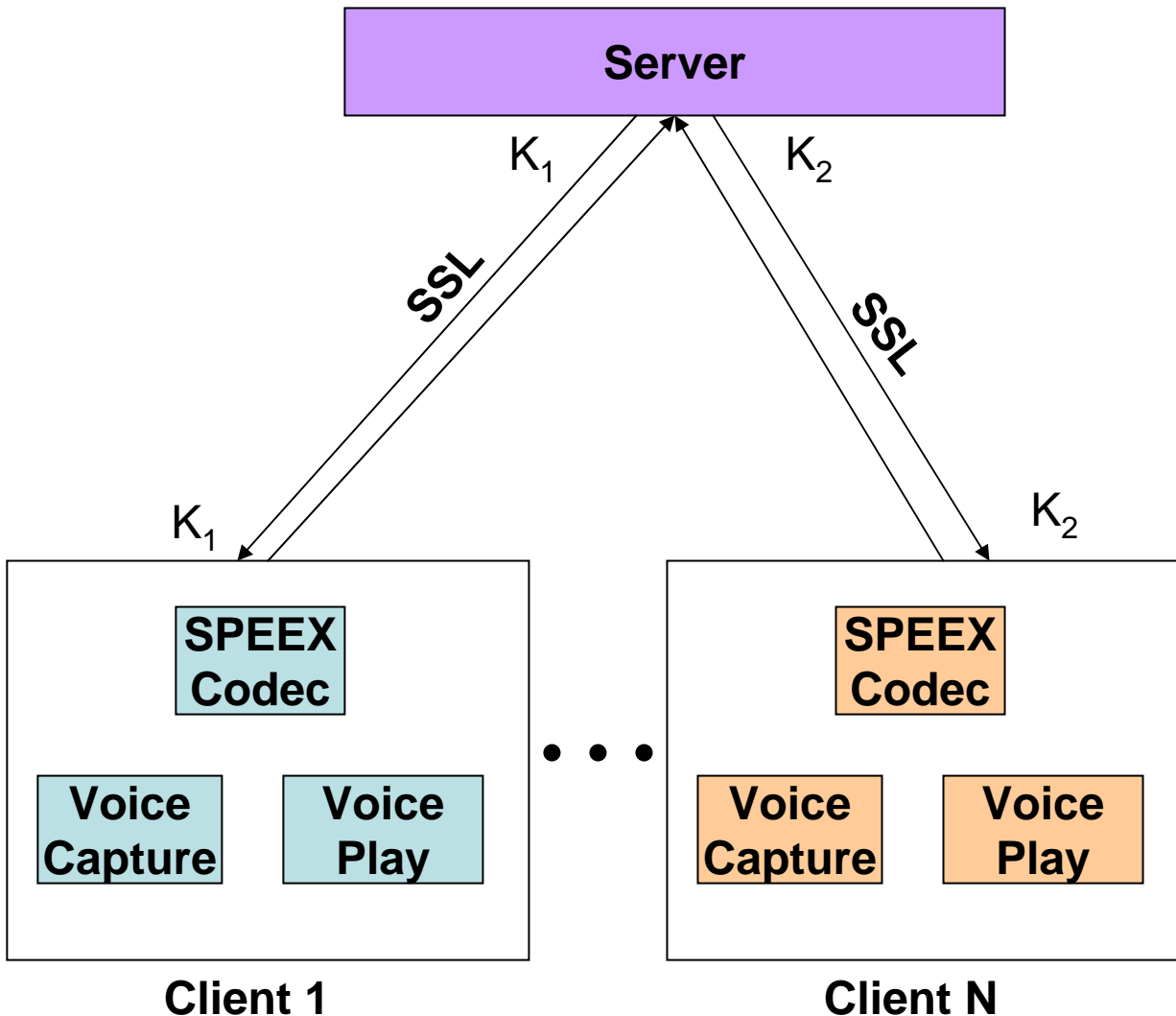
Signed Certificate



OpenSSL Messages



Software Architecture



Transmission Steps

- Capture voice
- Compress
- Encrypt with K_1
- Send to server
- Decrypt with K_1
- Encrypt with K_2, K_1
- Forward to destinations
- Decrypt with K_2
- Decompress
- Play
- Decrypt with K_1
- Decompress
- Play

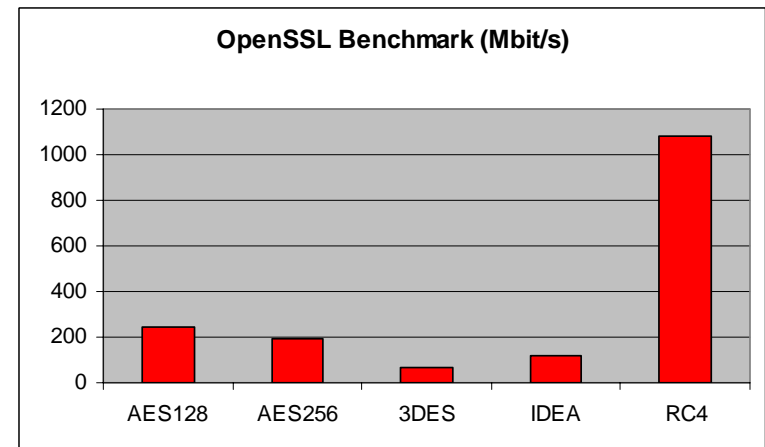
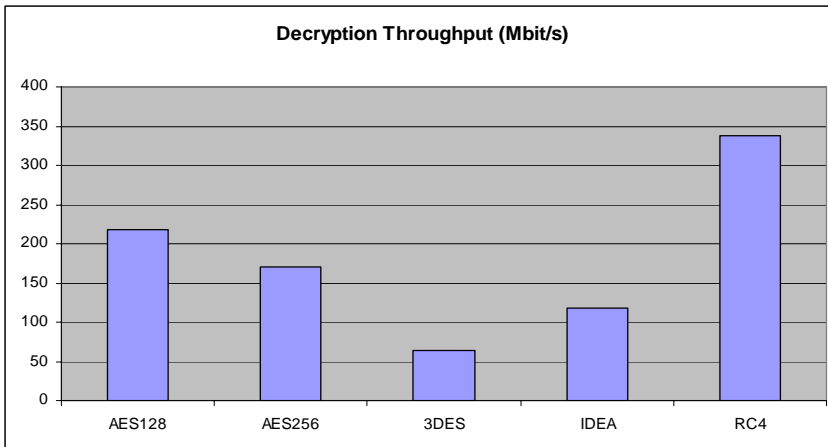
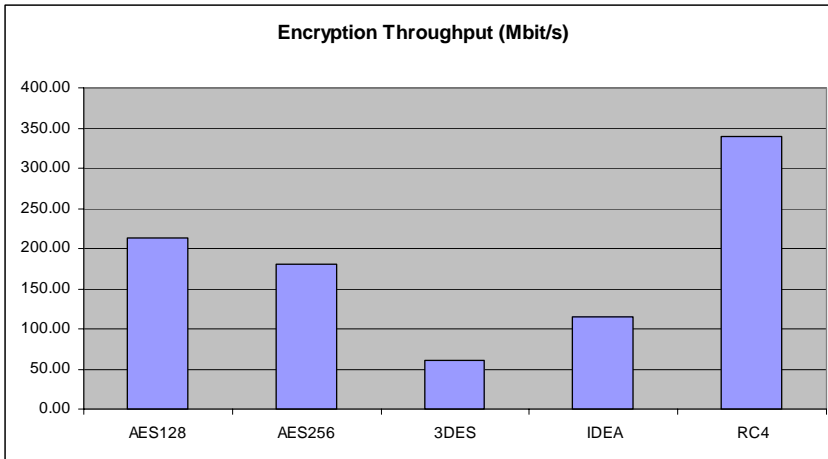
Environment/Compiler

- Compiler: Visual C++.Net 2003 (7.1)
- Install binary distribution for windows of OpenSSL
<http://www.slproweb.com/products/Win32OpenSSL.html>
 - Copy the OpenSSL/include directory in Visual C++ /include directory
 - Copy the OpenSSL/lib/VC directory in Visual C++ /lib directory
- Install Ms DirectX 9.0 SDK (summer 2004 update) for voice play and voice capture

Other components

- Secure RNG
 - Included in SSL
 - 255 random bits needed for initialization
 - Options
 - Linux: /dev/random
 - Windows: EGADS (slow)
 - Native Windows Cryptographic context (PROV_RSA_FULL)
- Multimedia Codec
 - **SPEEX** open source codec (free of charge)
 - Patent free software
 - 7:1 compression rate
 - 8kHz sampling mono, 16-bit/sample in PCM
- High resolution CPU tick counter
 - Created by J.M. McGuinness and P.J. Naughter
 - Benchmark of CPU speed is saved in the registry for later use

Performance metrics (1): Throughput of different symmetric ciphers

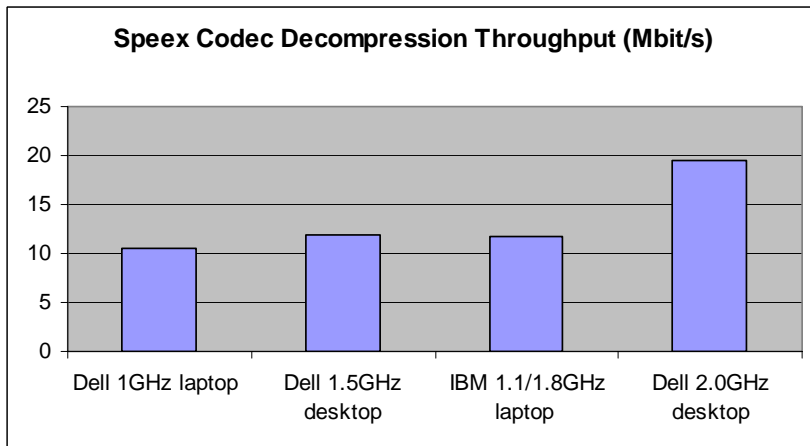
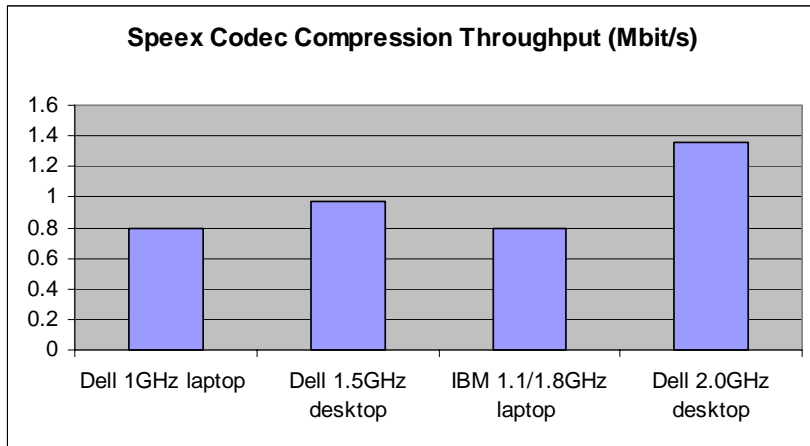


Performance metrics (2):

The effect of the 1-bit transmission error

Cipher	Mode	# Bytes Changed Raw file	#Bytes Changed .spx file	
AES 128	ECB	16	16	<ul style="list-style-type: none">• Saved the voice in raw (.wav) and compressed (.spx) format• Encrypt the file with different ciphers in different operation modes• Flip the 2nd bit of the 10,000th byte of the file• Measured the effect of bit error for each cipher and operation mode
	CBC	17	17	
	CBF	17	17	
	OBF	1	1	
AES 256	ECB	16	16	<ul style="list-style-type: none">• Decrypt/decompress (if necessary) and listen to the malformed file• The effect was as expected (1 block changed for ECB, 1 block and 1 byte changed for CBC and CFB and 1 byte changed for OFB mode)
	CBC	17	17	
	CBF	17	17	
	OBF	1	1	
3DES EEE	CBC	9	9	<ul style="list-style-type: none">• Surprisingly, the effect of an 1-bit change on the encrypted raw file (a click sound) can be heard when playing the file• I couldn't hear any effect of an 1-bit change on the encrypted .spx file
	ECB	9	9	
	CBF	9	9	
	OBF	1	1	
RC4 128	ECB	1	1	

Performance metrics (3): Codec Throughput



- Measured the compression/decompression time on an about 10 seconds voice stream
- The voice compression throughput is almost 10 times smaller than the voice decompression throughput
- Even when working with slow ciphers (3DES), the compression delay is still a bottleneck of the software
- Faster hardware platform is recommended to reduce compression time.

Four Given Different CPUs and Three Operating Systems

- IBM 1.1 GHz laptop, Windows 2000, Pentium4
- Dell 2.0 GHz desktop, Windows XP, Pentium4
- 1.0 GHz laptop, Windows XP, Pentium3
- 1.5 GHz desktop, Windows 2000 server, Pentium4

Performance metrics (4):

Authentication and key exchange delay

IBM 1.1 GHz, RSA 3072 certificate

Cipher combination	TCP Handshake	SSL Handshake	Certificate validation	Generate ephemeral key	Compute shared secret
DHE-RSA-AES128-SHA	7.82	864.19	4.01	26.77	31.06
DHE-RSA-AES256-SHA	7.41	747.48	4.11	26.91	32.44
AES128-SHA	7.83	1348.2	4.11	4.49	215.3
AES256-SHA	7.34	643.79	4.12	4.53	204.4
EDH-RSA-DES-CBC3-SHA	7.61	751.06	4.01	26.89	31.08
DES-CBC3-SHA	7.41	614.74	4.01	4.57	204.5
IDEA-CBC-SHA	7.96	644.03	4.01	4.52	205.7
RC4-SHA	7.35	680.92	4.13	4.84	203.1

Performance metrics (4):

Authentication and key exchange delay

Dell 2.0 GHz, RSA 3072 certificate

Cipher combination	TCP Handshake	SSL Handshake	Certificate validation	Generate ephemeral key	Compute shared secret
DHE-RSA-AES128-SHA	5.44	558.30	2.28	14.36	16.76
DHE-RSA-AES256-SHA	5.50	459.82	2.28	14.28	16.49
AES128-SHA	5.44	896.75	2.83	2.71	119.0
AES256-SHA	5.48	407.24	2.30	2.72	118.4
EDH-RSA-DES-CBC3-SHA	5.44	461.77	2.28	14.22	16.66
DES-CBC3-SHA	5.47	407.58	2.28	2.73	120.1
IDEA-CBC-SHA	5.45	406.43	2.28	2.73	118.4
RC4-SHA	5.46	405.19	2.28	2.72	18.7

Performance metrics (4):

Authentication and key exchange delay

IBM 1.1 GHz, DSA 3072 certificate

Cipher combination	TCP Handshake	SSL Handshake	Certificate validation	Generate ephemeral key delay	Compute shared secret
DHE-DSS-AES128-SHA	7.64	614.32	4.12	26.03	30.41
DHE-DSS-AES256-SHA	7.32	480.95	3.98	26.11	31.27
EDH-DSS-DES-CBC3-SHA	7.24	494.61	3.99	26.61	30.93
DHE-DSS-RC4-SHA	7.21	496.34	4.01	26.16	30.75

Performance metrics (4):

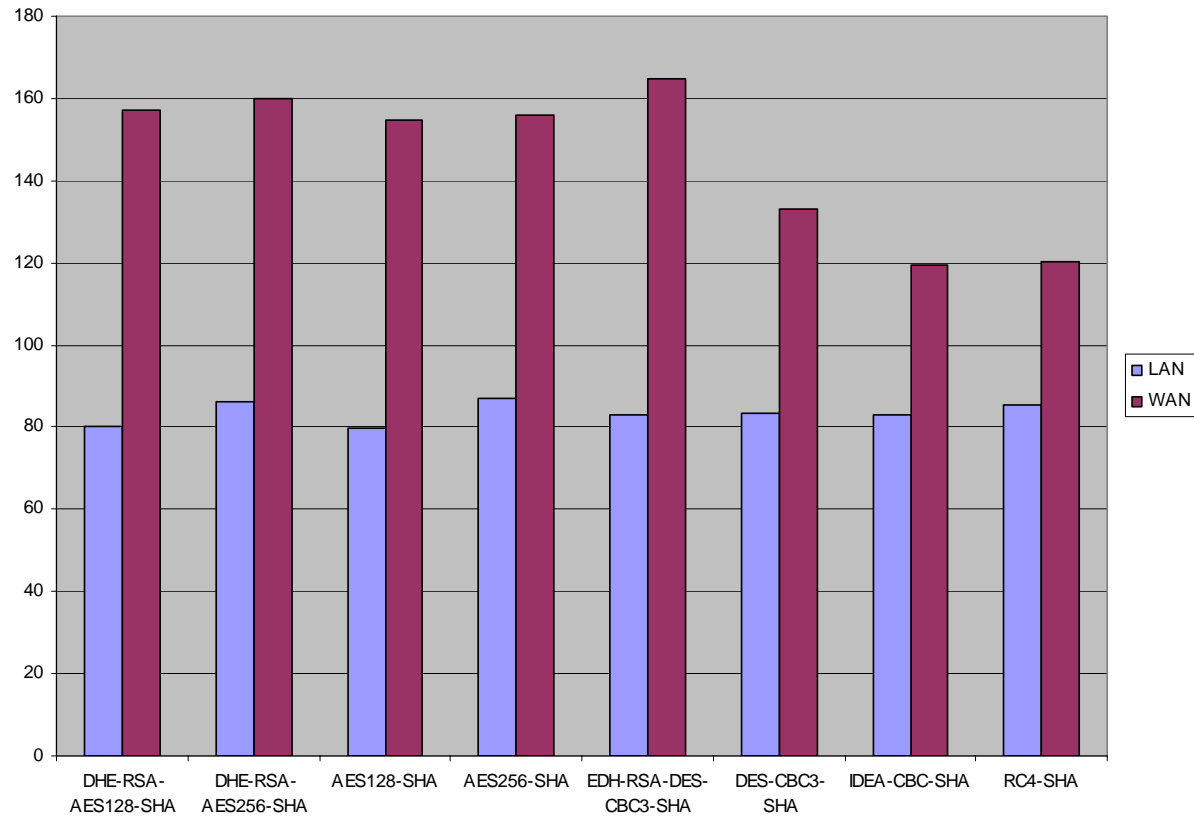
Authentication and key exchange delay

Dell 2.0 GHz, DSA 3072 certificate

Cipher combination	TCP Handshake	SSL Handshake	Certificate validation	Generate ephemeral key delay	Compute shared secret
DHE-DSS-AES128-SHA	5.47	469.20	2.32	14.29	17.22
DHE-DSS-AES256-SHA	5.47	341.92	2.32	14.36	16.79
EDH-DSS-DES-CBC3-SHA	5.50	345.19	2.31	14.51	16.75
DHE-DSS-RC4-SHA	5.49	349.19	2.30	20.87	16.96

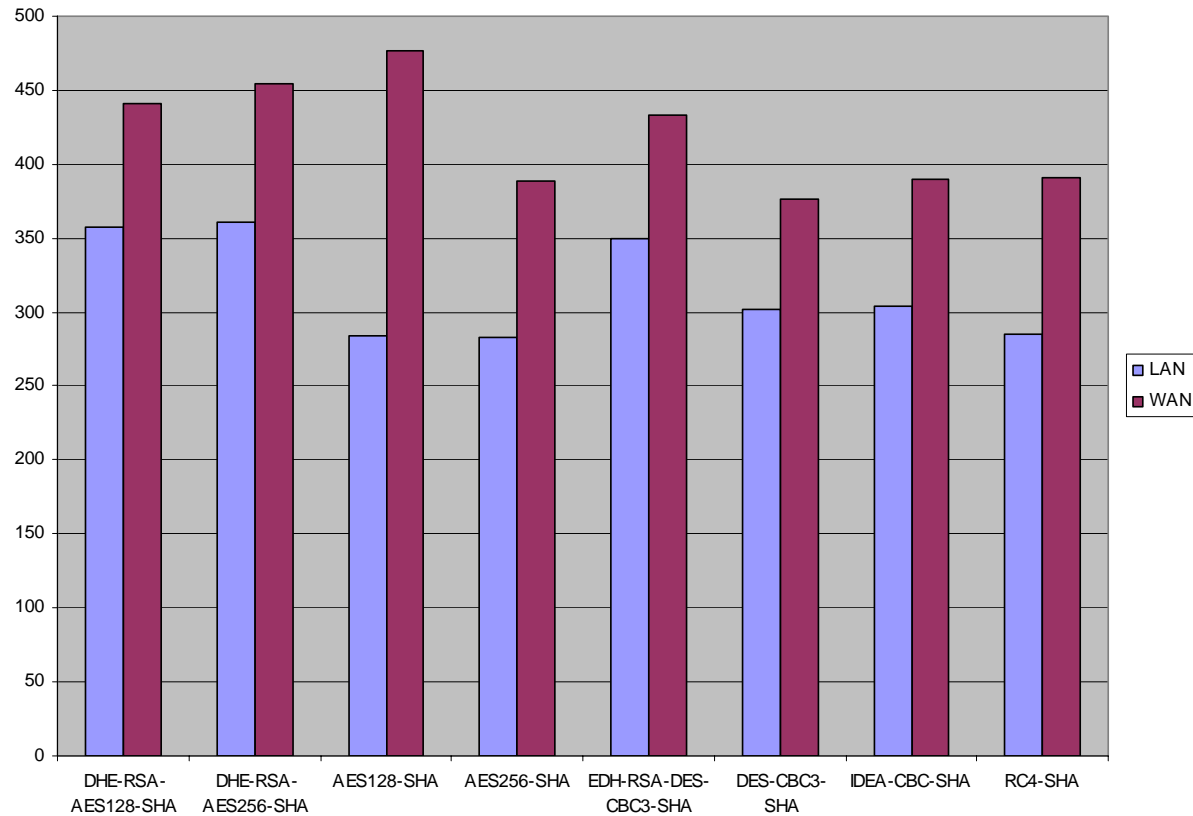
Performance metrics (5): Network Speed

Connection Delay for LAN/WAN Networks (ms) for RSA 1024 certificate



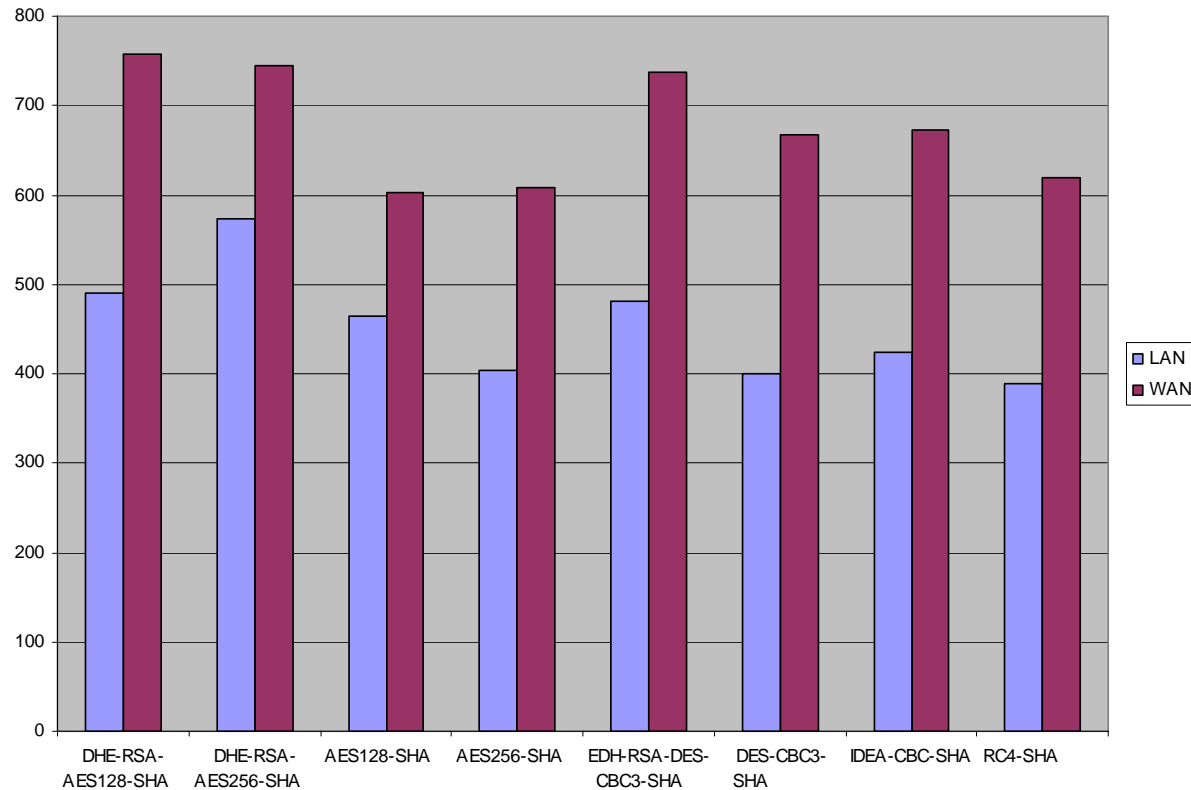
Performance metrics (5): Network Speed

Authentication Delay for LAN/WAN network for RSA 1024 Certificate



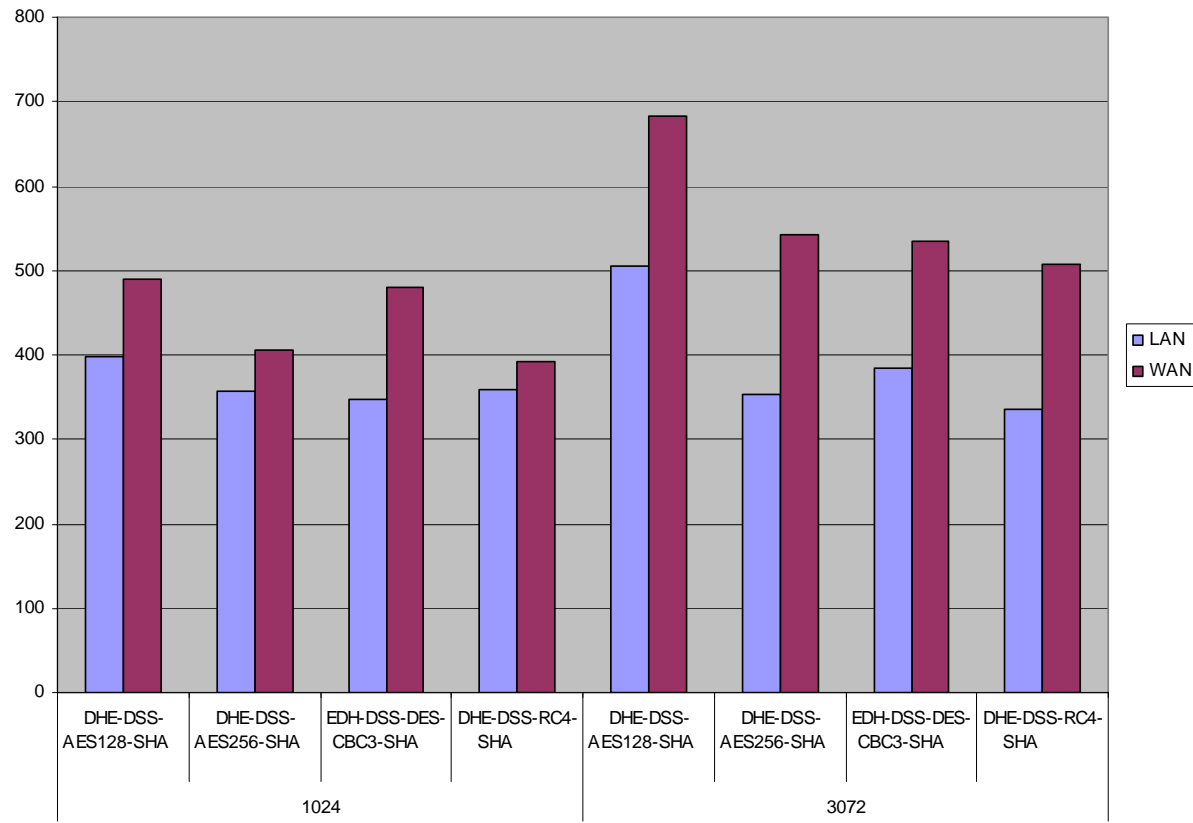
Performance metrics (5): Network Speed

Authentication Delay for LAN/WAN Network for RSA 3072 certificate (ms)



Performance metrics (5): Network Speed

Authentication Delay for LAN/WAN network for DSA 1024/3072 certificate



Contributions

- Implemented a real-time secure teleconference software over SSL connections
 - Created a private CA and sign certificates for server and clients
- Produced a comparative study of the connection, authentication and key exchange delay for
 - Different combination ciphers provided by OpenSSL
 - Different certificate key length
 - Different hardware platform and operation systems
 - Different network speed
- Analyzed the throughput of several strong symmetric ciphers in the voice stream encryption context, and compare the results with OpenSSL benchmark
- Studied the throughput of the SPEEX codec, and its effect on the total transmission delay
- Studied the effect of an 1-bit transmission error on the voice stream for
 - Several symmetric ciphers and operation modes
 - With/without Speex compression

Conclusions

- OpenSSL, although optimized for web applications, provides a good enough support for secure teleconference
- The certificate checking and key exchange delay grows larger as we move to larger RSA and DSA key length, however a more important factor in the total delay is the network speed.
- Using a voice codec reduces the allocated bandwidth about 10 times at the expense of increased transmission delay. Using of faster computer platforms (and therefore more expensive) helps in reducing both compression delay and authentication/key exchange/encryption/decryption delay.