AT&T

AT&T
Labs

Performance Implications of Security Protocols

Varsha Mainkar

Technical Staff Member

Network Design & Performance Analysis

Advanced Technologies, AT&T Labs

Joint Work with Paul Reeser

5th INFORMS Telecom Conference

Boca Raton, 7 March 2000

Outline of Talk

- Overview of Secure Sockets Layer v3.0
  - **SSL Handshake Protocol**
  - **SSL Record Protocol**
- Factors Affecting Performance
  - **Handshake Layer:**
    - **socket setup, key generation, session caching**
  - **Record Layer:**
    - **encryption/decryption, hardware accelerators**
- Performance Results & Observations
  - **LDAP over SSL over Ethernet**
  - **HTTP over SSL over Internet**
    - **response time, network traffic**

Overview of Secure Sockets Layer

Secure Sockets Layer (SSL) protocol

- Sandwiched in between L4 application protocol (eg, HTTP) and reliable L3 transport protocol (TCP)
  - **eg, HTTPS (port 443) ~ HTTP / SSL / TCP/IP / Ethernet**

Two cryptography layers within SSL

- SSL Handshake (aka Message) layer
  - **RSA certificate/public-key exchange for authentication**
  - **cryptographic parameters (session key) establishment**
- SSL Record layer
  - **encapsulation of higher level protocols (including Handshake)**
  - **RC4 compression + bulk encryption of data using session key**
  - **MD5 message authentication code (MAC) for data integrity**

Performance Implications of Security Protocols:

SSL Handshake Layer

AT&T Labs

Client		Server
TCP SYN	→	
	←	TCP SYN-ACK
rand x SSL Client Hello [Session ID, if cached] ClientHelloDone	x →	SSL Server Hello [Digital Certificate], [ServerKeyExchange], [CertificateRequest] ServerHelloDone rand y public key P
	← y,P	
rand z P(z) K=f(x,y,z) K(fin) [Digital Certificate], [ClientKeyExchange], [CertificateVerify] ChangeCipherSpec Finished (encrypted)	P(z),K(fin) →	
	← K(fin)	[CertificateVerify] ChangeCipherSpec Finished (encrypted) $z=P^{-1}P(z)$ K=f(x,y,z) K(fin)
Application Request (eg, HTTP POST)	→	
	←	Response

Performance Implications of Security Protocols: SSL Record Layer

- *Compresses* 16KB units of higher layer application data
- Computes message auth code (MAC) on compressed data
- Encrypts compressed data using 40- or 128-bit session key
- Sends headers + encrypted compressed data + MAC

Message Type (handshake, data, alert, ...) : 1B
Protocol Version : 2B
Fragment Length : 2B
Sequence Number : 8B
Compressed, encrypted data + MAC: up to 16KB If stream cipher: encrypted size = compressed size If block cipher: padded to make it into 8B blocks

Factors Affecting Performance I

Secure SSL socket setup (handshake)

- Network latency :
  - **adds ~ 2 RTTs to delay for first segment of application response (4 RTTs for secure SSL socket vs 2 RTTs for clear TCP socket)**
    - **eg, @ 200ms Internet RTT, adds ~ 400ms to response time**
- Network bandwidth :
  - **adds ~ 2KBs to total application traffic on network**
    - **eg, @ 26.4Kbps modem throughput, adds ~ 650ms to latency**
    - **significant for small transactions (eg, HEAD, POST login)**
- CPU consumption :
  - **costs ~ O(300ms) of additional server CPU consumption**
    - **session-key generation + 1024-bit RSA decryption operation**
  - **adds ~ 300/(1–ρ) ms to application response time, where ρ = server CPU utilization**

Factors Affecting Performance II

Session state management (ID caching)

- Client can request to resume previously established session
  - **client includes Session ID in Client Hello message**
  - **allows multiple HTTP transactions w/in single SSL session**
- Beneficial for “sessional” applications (eg, secure WebMail)
  - **avoids session key generation & server decrypt operation**
  - **avoids 1 out of 2 extra RTTs & some extra data exchange**
- But, could be detrimental for secure “transactional” apps, where SSL session = 1 tx (eg, secure login + insecure WM)
  - **may have significant overhead due to session ID mgmt (inefficient if client performs only one secure transaction)**

Factors Affecting Performance III

Hardware accelerator cards

- PCI adapter board with RSA public-key math co-processor
  - **CryptoSwift (Rainbow Technologies)**
  - **nFast (nCipher Corporation Ltd)**
- Supports most security protocols & cryptography methods
  - **SSL, SET, SSH, IPSec, …**
  - **RSA, PGP (Diffie-Hellman), DSA, ...**
- Vendors' claims for single accelerator board:
  - **10-fold reduction in CPU consumption for SSL setup**
  - **20-fold increase in SSL transaction throughput**
  - **50% reduction in SSL transaction response time**
  - **but, only modest acceleration of RC4 bulk encryption**

Factors Affecting Performance IV

RC4 bulk encryption (symmetric key)

- 40-bit (export) vs 128-bit (domestic) RC4 session cipher-key
  - **we found little or no impact on response time**
  - **re CPU consumption: accelerator vendors claim that**

    "RC4 only consumes a few percent of your processor"
  - **our results suggest otherwise**

Performance Implications of Security Protocols:
Results for LDAP / SSL / Ethernet

AT&T Labs

- Retrieve personal address book from LDAP directory server

# Entries in PAB	Client LDAP Server (over LAN)	
	SSL Enabled	Without SSL
0*	9	5
10	14	9
20	21	13
30	28	17
40	35	21
50	42	26
Average	**~ 9s + 7s/10 entries**	**~ 5s + 4s/10 entries**

*** empty PAB = SSL connection (key exch, authentication, handshake, etc)**

- Results
  - **handshake ~ 1.8x impact**
  - **encryption ~ 1.75x impact**

Performance Implications of Security Protocols: Results for HTTP / SSL / Internet

AT&T Labs

Test Configuration

- Server : SGI Challenge L (4 194Mhz CPUs), Irix 6.5, SSL 3.0 (128-bit), Netscape Enterprise 3.6
- Clients : NT workstation + NT server, Silk Performer 2.5
- Network : 56Kbps modem (connecting @ 26.4Kbps)

"WebMail" Transaction Workload

- Login (https POST user name + password)
  - **no SSL, SSL – handshake (ID cached), SSL + handshake**
- Downloads (20KB, 100KB, 200KB, 500KB, 1MB ascii files)
  - **no SSL, and SSL – handshake (ID cached)**

Performance Metrics

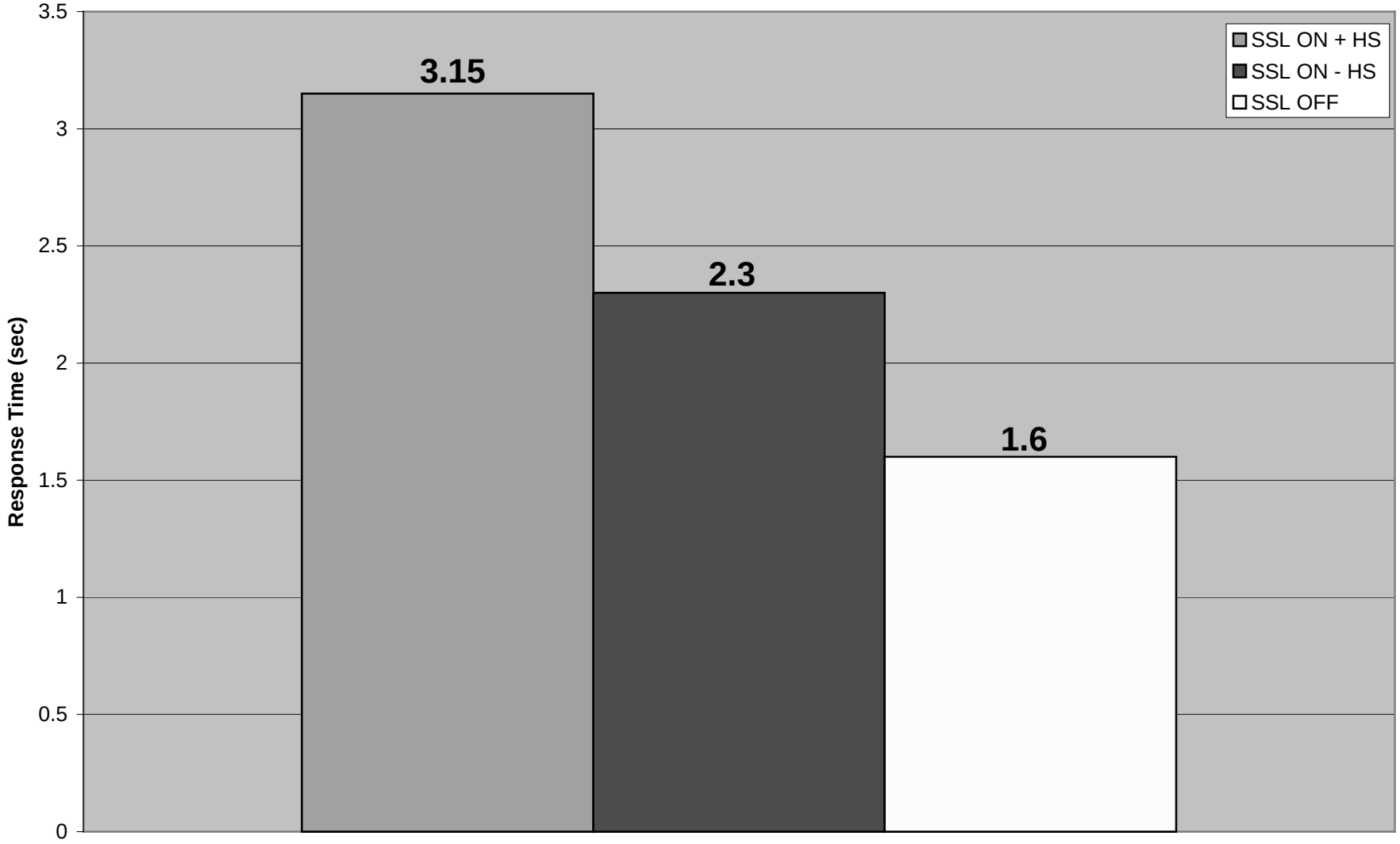
- client response time, server CPU time, network traffic

Performance Implications of Security Protocols:

WebMail Login Response Time

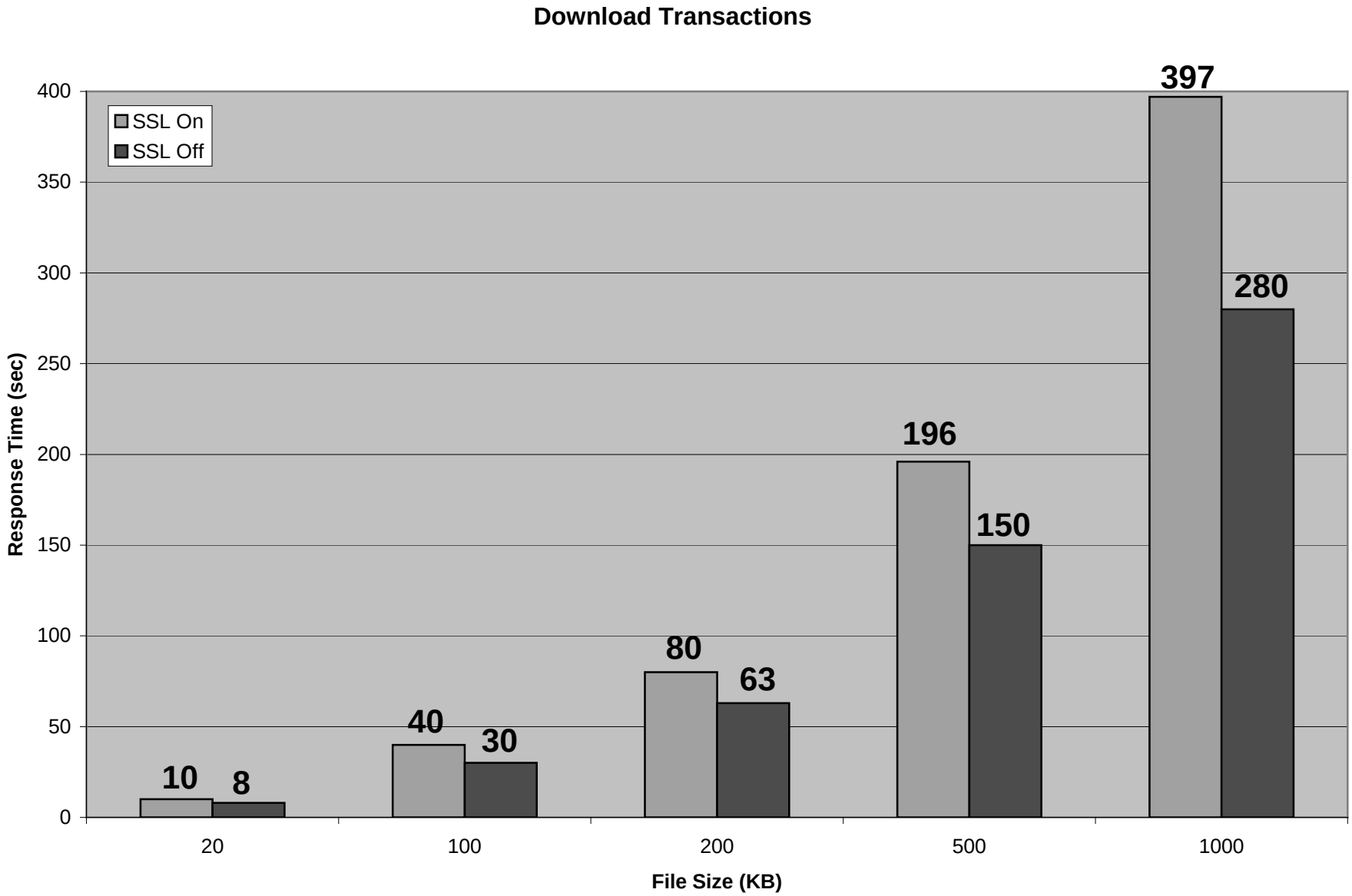
AT&T Labs

Login Transaction



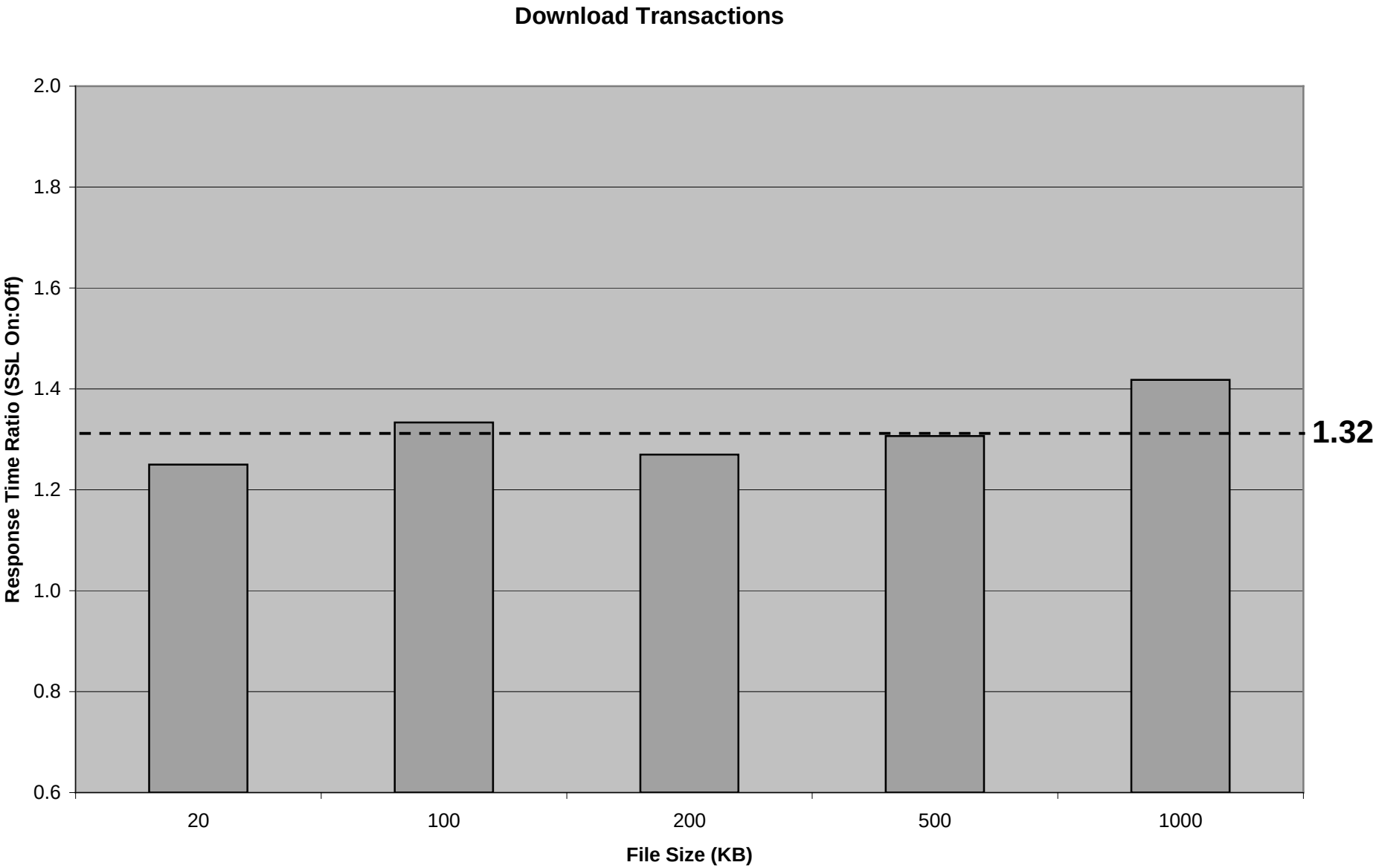
Performance Implications of Security Protocols:
WebMail Download Response Time

AT&T Labs



Performance Implications of Security Protocols:
WM Download Response Time Ratio

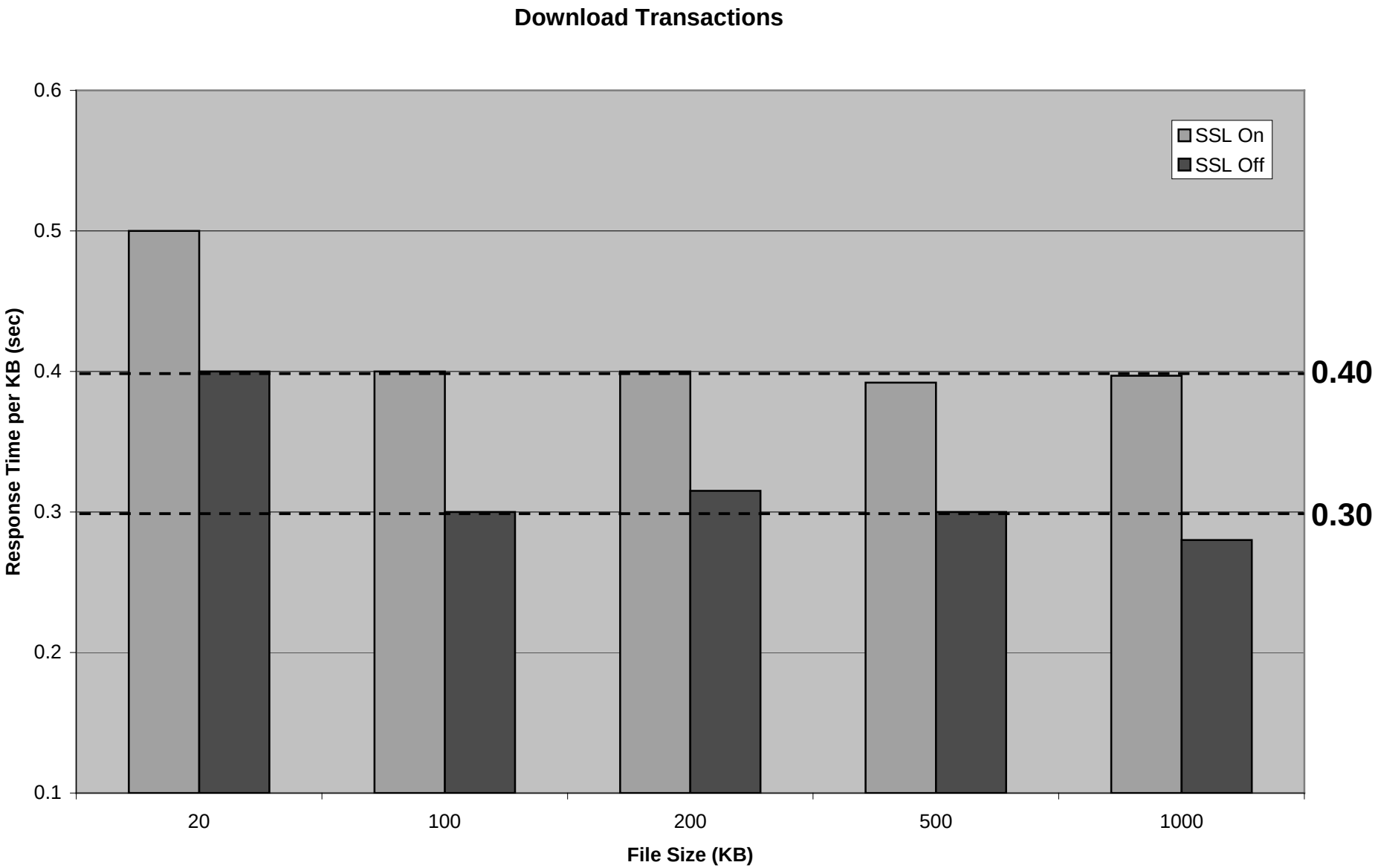
AT&T Labs



Performance Implications of Security Protocols:

WM Download Response Time/KB

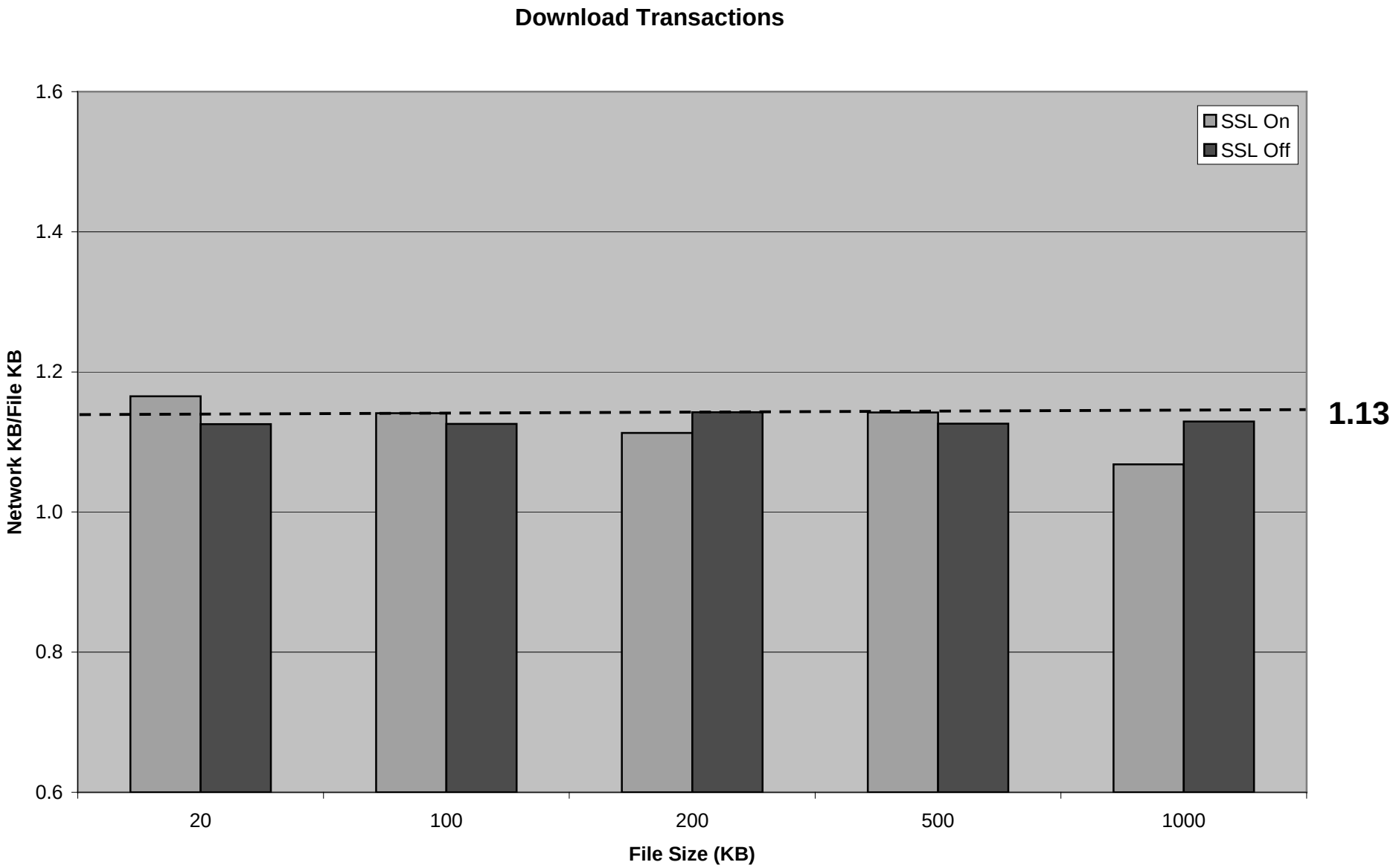
AT&T Labs



Performance Implications of Security Protocols:

WM Download Network KB/File KB

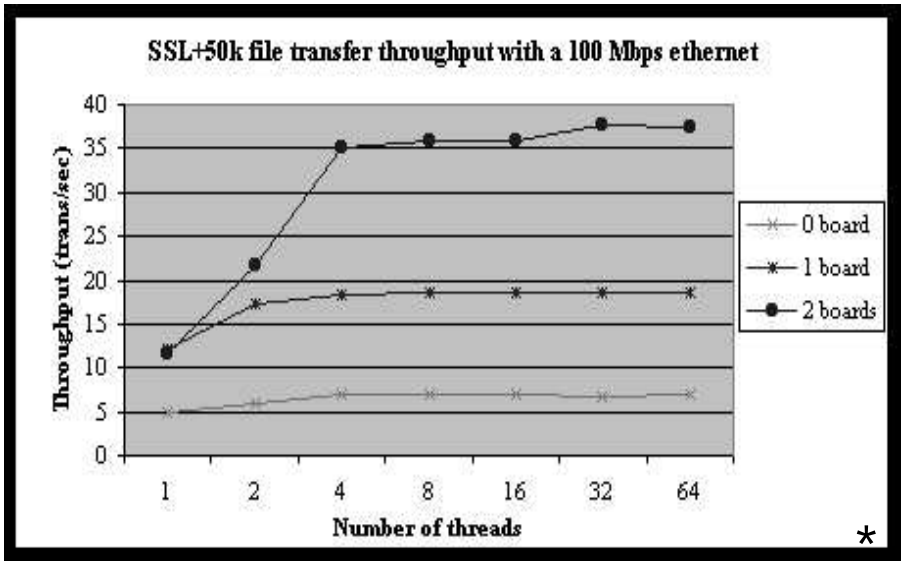
AT&T Labs

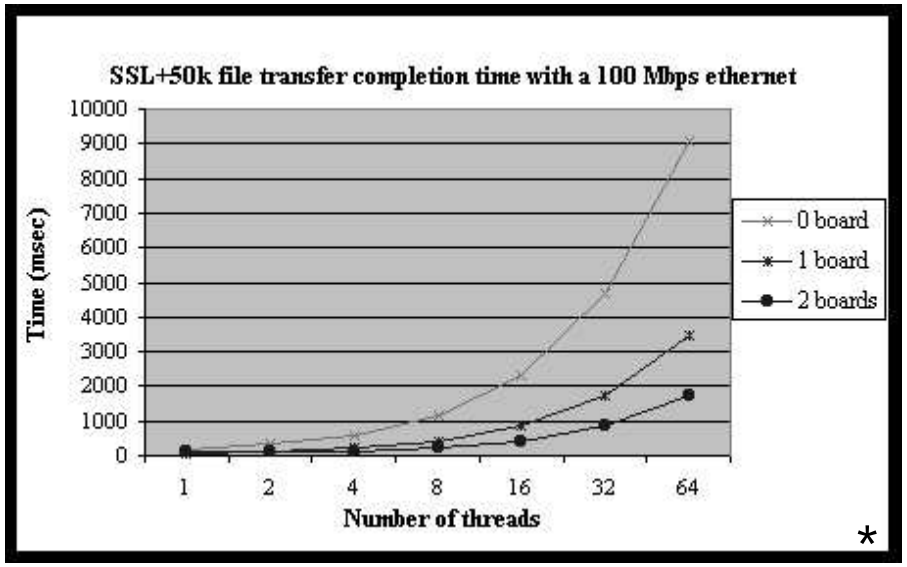


Performance Implications of Security Protocols: Hardware Accelerators

AT&T Labs

- PCI adapter board with RSA public-key math co-processor
  - **CryptoSwift (Rainbow Technologies), nFast (nCipher Corp)**
- Vendors' claims for single accelerator board:
  - **10-fold reduction in CPU consumption for SSL setup**
  - **20-fold increase in SSL transaction throughput**
  - **50% reduction in SSL transaction response time**





* "CryptoSwift Performance under SSL with File Transfer" Keung (1997)

Performance Implications of Security Protocols:
Conclusions of Study

AT&T Labs

- Handshake adds 2 RTTs, 2KB traffic, O(300ms) CPU time
  - **Login latency (via modem, low server load) ~ 2.0x increase**
- Session ID caching can recoup ~ 1/2 of added overhead, provided application workload is “sessional” not “transactional”
  - **Login latency (via modem, low server load) ~ 1.4x increase**
- Download latency (via modem, low server load) ~ 1.3x impact
- Net effect on server CPU (via modem, low server load) :
  huge CPU penalty to download in SSL (up to 250x increase!)
  - **either RC4 bulk encryption <u>is</u> costly, or SSL file download over low-speed connection is <u>extremely</u> inefficient (TBD...)**
- Little/no effect on network traffic (compression not apparent)
- Crypto accelerators may offer promise in some scenarios
  - **little help for bulk encryption, but promising for handshake**