Case Study II: A Web Server

Prof. Daniel A. Menascé
Department of Computer Science
George Mason University
www.cs.gmu.edu/faculty/menasce.html

Copyright Notice

- Most of the figures in this set of slides come from the book "Performance by Design: computer capacity planning by example," by Menascé, Almeida, and Dowdy, Prentice Hall, 2004. It is strictly forbidden to copy, post on a Web site, or distribute electronically, in part or entirely, any of the slides in this file.

The Web Server

- A large company uses an internal Web server to allow its programmers, testers, and documentation personnel to download two types of files:
  - PDF files containing documents and manuals
  - ZIP files containing software files.
- The server has one CPU and 4 identical disks.
- PDF files are stored on disks 1 and 2 (with evenly distributed access)
- ZIP files are stored in disks 3 and 4 (with evenly distributed access)

Capacity Planning Questions

- How many PDF and ZIP file downloads can be sustained concurrently with given response times?
- What is the impact of using Secure Sockets Layer (SSL) for secure downloads?

From the Web Log

File Type	Size (KB)	Elapsed Time (sec)
PDF	303	1.43
ZIP	1233	5.81
ZIP	1077	5.08
PDF	315	1.48
ZIP	1240	5.84
PDF	413	1.95
ZIP	1139	5.37
ZIP	1198	5.64
PDF	323	1.52
ZIP	1188	5.60
. . . . .		

5

PDF File Size Statistics (in KB)	
Mean	377.6
Median	375.5
Standard Deviation	43.1
Sample Variance	1859.5
Range	149.2
Minimum	300.4
Maximum	449.6
Sum	155,183
Count	411
1/2 95% Confidence Interval	4.17

Cpdf = 43.1 KB / 377.6 KB = 0.114

6

Confidence Interval Estimation of the Mean

- Known population standard deviation.
- Unknown population standard deviation:
  - Large samples: sample standard deviation is a good estimate for population standard deviation. OK to use normal distribution.
  - Small samples and original variable is normally distributed: use *t* distribution with *n-1* degrees of freedom.

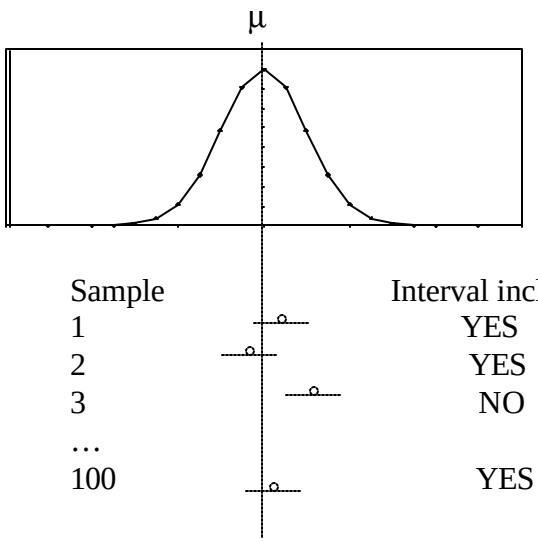
7

Confidence Interval Estimation of the Mean

$$\Pr[c_1 \leq m \leq c_2] = 1 - a$$

(c_1,c_2): confidence interval
α: significance level (e.g., 0.05)
1-α: confidence coefficient (e.g., 0.95)
100(1-α): confidence level (e.g., 95%)

8



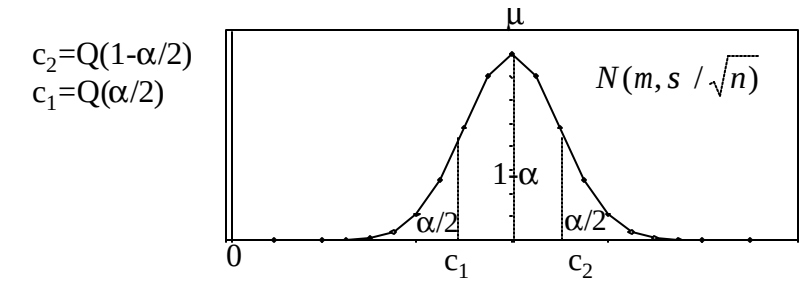
100 (1 – α) of the 100 samples include the population mean μ.

Central Limit Theorem

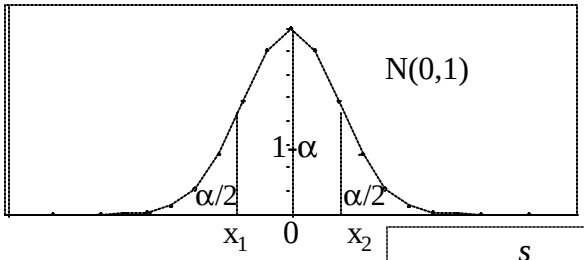
- If the observations in a sample are independent and come from the same population that has mean μ and standard deviation σ then the sample mean for **large** samples has a normal distribution with mean μ and standard deviation $\sigma/\sqrt{n}$.

$$\overline{x} \sim N(m, s/\sqrt{n})$$

- The standard deviation of the sample mean is called the *standard error.*



c_2=Q(1-α/2)
c_1=Q(α/2)



$x_2 = z_{1-\alpha/2}$

$x_1 = z_{\alpha/2} = -z_{1-\alpha/2}$

$$c_2 = m + \frac{s}{\sqrt{n}} z_{1-a/2}$$

$$c_1 = m + \frac{s}{\sqrt{n}} z_{a/2} = m - \frac{s}{\sqrt{n}} z_{1-a/2}$$

11

Confidence Interval (large (n>30) samples)

- 100 (1-α)% confidence interval for the population mean:

$$\left(\bar{x} - z_{1-a/2}\frac{s}{\sqrt{n}}, \bar{x} + z_{1-a/2}\frac{s}{\sqrt{n}}\right)$$

$\bar{x}$: sample mean
s: sample standard deviation
n: sample size
$z_{1-a/2}$: (1-α/2)-quantile of a unit normal variate (N(0,1)).

12

Confidence Interval (small samples, normally distributed population)

- 100 (1-α)% confidence interval for the population mean:

$$(\bar{x} - t_{[1-a/2;n-1]} \frac{s}{\sqrt{n}}, \bar{x} + t_{[1-a/2;n-1]} \frac{s}{\sqrt{n}})$$

$\bar{x}$: sample mean
s: sample standard deviation
n: sample size
$t_{[1-a/2;n-1]}$: critical value of the *t* distribution with *n-1* degrees of freedom for an area of α/2 for the upper tail.

13

Computing Important Quantiles in Excel

$z_{1-a/2}$ = (1-α/2)-quantile of a unit normal variate (N(0,1)):
= NORMINV (1-α/2,0,1) = NORMSINV(1- α/2)
Half-interval = CONFIDENCE (α,σ,n)

$t_{[1-a/2;n-1]}$ = (1-α/2)-quantile of *t*-variate with *n-1* degrees of freedom = TINV(α,n-1)

14

ZIP File Size Statistics (in KB)	
Mean	1155.6
Median	1157.9
Standard Deviation	85.7
Sample Variance	7350.0
Range	299.8
Minimum	1000.1
Maximum	1299.9
Sum	680,650
Count	589.0
1/2 95% Confidence Interval	6.92

Czip = 85.7 KB / 1155.6 KB = 0.074

15

Building the Performance Model

- Computing concurrency levels:

$$\overline{N}_{pdf} = \frac{\sum_{i=1}^{411} e_{i,pdf}}{\text{interval duration}} = \frac{731.5}{200} = 3.7$$

$$\overline{N}_{zip} = \frac{\sum_{i=1}^{589} e_{i,zip}}{\text{interval duration}} = \frac{3207.7}{200} = 16.1$$

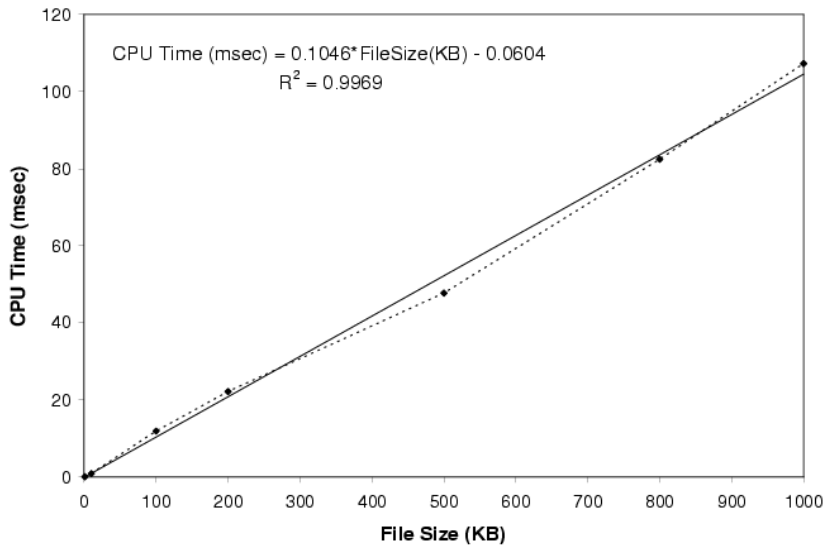
- Will use a ratio of 1:4 for PDF to ZIP file downloads.

16

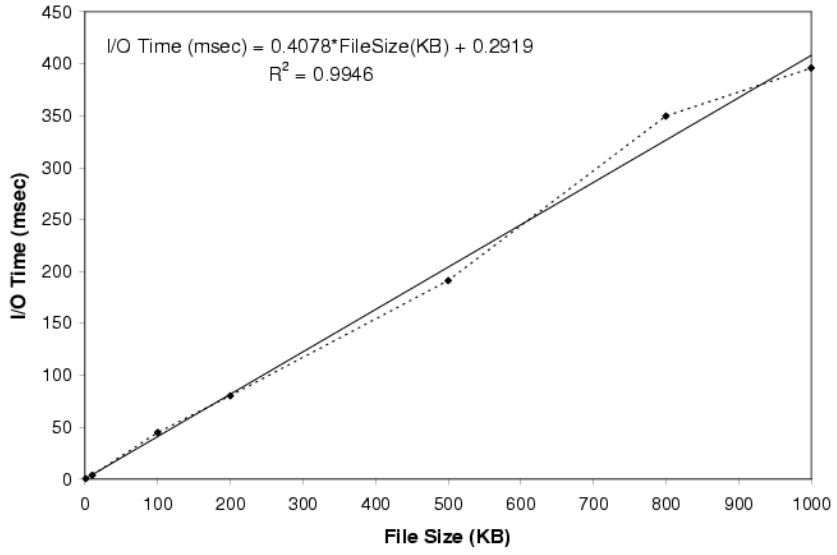
Building the Performance Model

- Computing Service Demands
  - Experiments conducted on a similar machine.
  - A set of *n* dummy files with files sizes of 10 KB, 100 KB, 200 KB, 500 KB, 800 KB, and 1000 KB are used.
  - For each file size, the *n* files are downloaded while measuring the CPU and disk utilization of the test server.
  - Service demand = utilization/(*n* / interval)

17



18



19

Service Demands

$$D_{CPU,pdf} = 0.1046 \times 377.6 - 0.0604 = 39.4\text{msec}$$

$$D_{disk1,pdf} = D_{disk2,pdf} = 0.5 \times (0.4078 \times 377.6 + 0.2919) = 77.1\text{msec}$$

$$D_{disk3,pdf} = D_{disk4,pdf} = 0$$

$$D_{CPU,zip} = 0.1046 \times 1155.6 - 0.0604 = 120.8\text{msec}$$

$$D_{disk3,zip} = D_{disk4,zip} = 0.5 \times (0.4078 \times 1155.6 + 0.2919) = 235.8\text{msec}$$

$$D_{disk1,zip} = D_{disk2,zip} = 0$$

20

Original Layout QN Model

	Service Demands (sec)	
CPU	0.0394	0.1208
Disk 1 (PDF)	0.0771	0.0000
Disk 2 (PDF)	0.0771	0.0000
Disk 3 (ZIP)	0.0000	0.2358
Disk 4 (ZIP)	0.0000	0.2358

Closed QN:

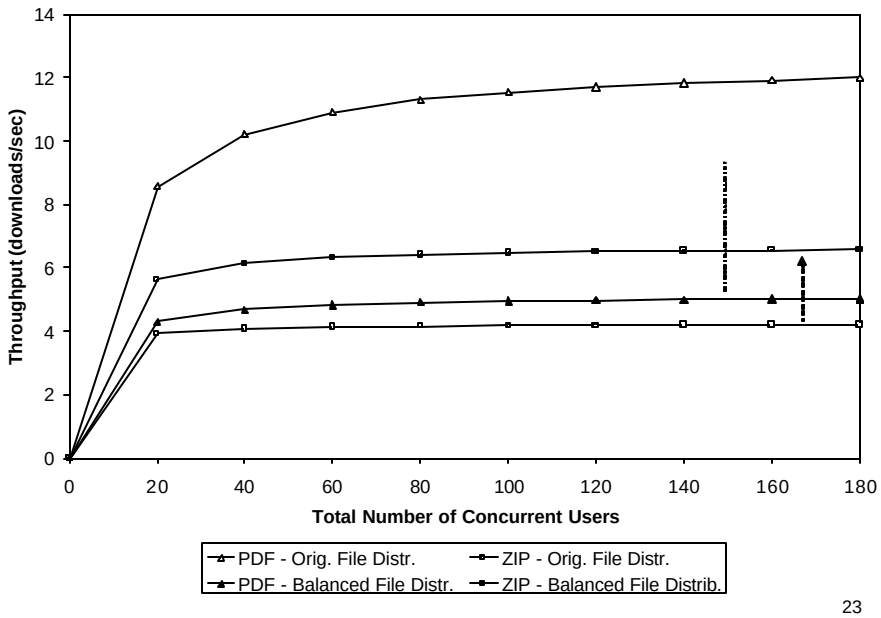
- two classes: PDF and ZIP.
- customer population ratio: 1:4

21

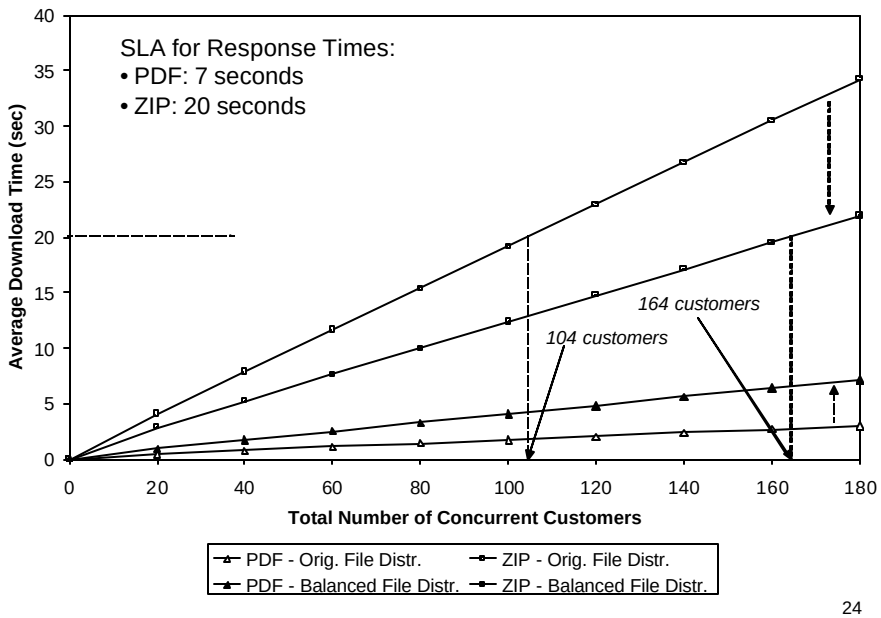
Balanced Configuration

	Service Demands (sec)	
CPU	0.0394	0.1208
Disk 1 (PDF)	0.0386	0.1179
Disk 2 (PDF)	0.0386	0.1179
Disk 3 (ZIP)	0.0386	0.1179
Disk 4 (ZIP)	0.0386	0.1179

22



23



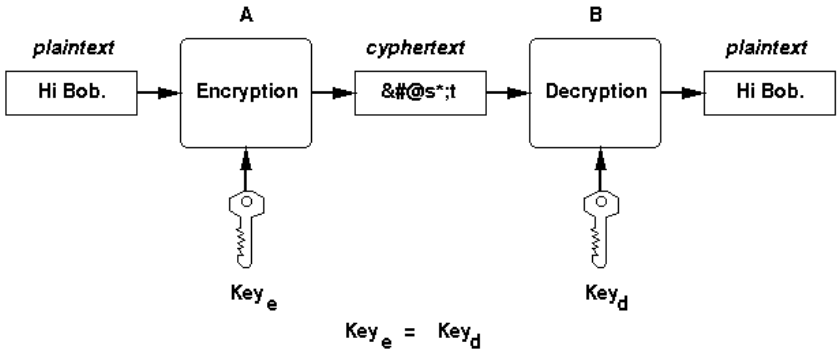
24

Secure Download Scenarios

- Use of Secure Sockets Layer (SSL) for authentication and data integrity and confidentiality.
- SSL has a handshake phase during which public key encryption is used to exchange secrets used to generate a symmetric key.

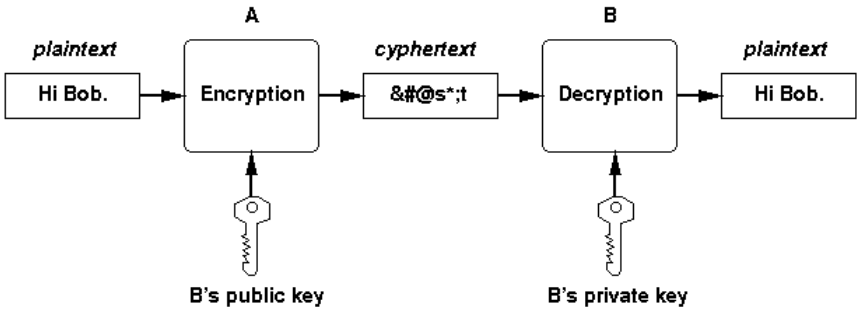
25

Symmetric Encryption and Decryption



26

Public Key Encryption and Decryption



27

Performance Considerations

- Public Key (PK) cryptography is order of magnitudes slower than symmetric key cryptography.
  - encrypting a 128-byte block using a public key of 512 bits takes 3.5 msec on a Pentium-II 266 MHz while symmetric key encryption using AES would take less than one microsecond on the same machine.

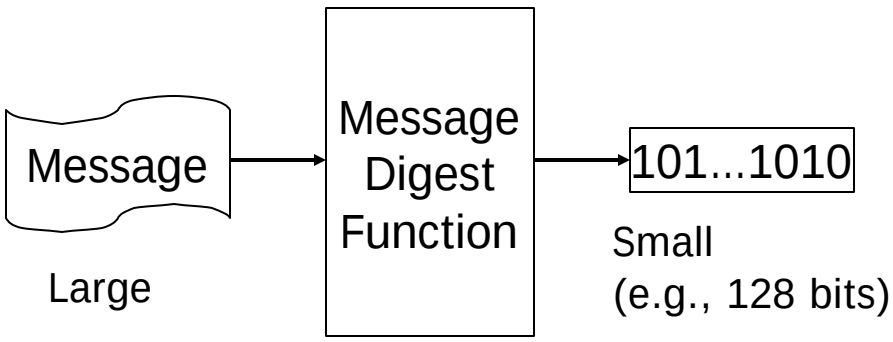
28

Performance Considerations

- Symmetric key cryptography is not scalable to a large number of users: they are required to share a secret key.
- It is faster to encrypt with a public key than to decrypt with a secret key.

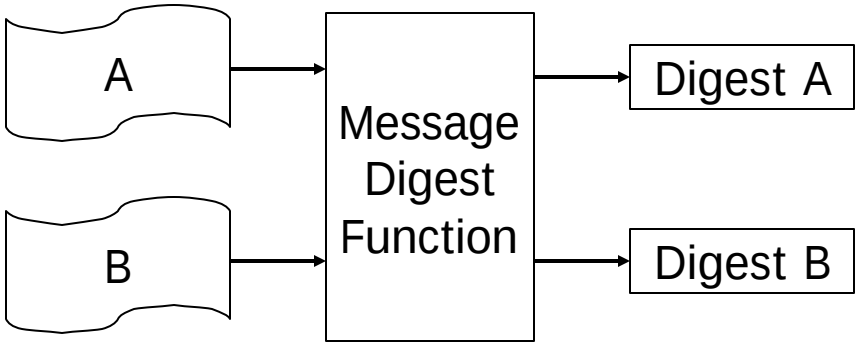
29

Message Digest



30

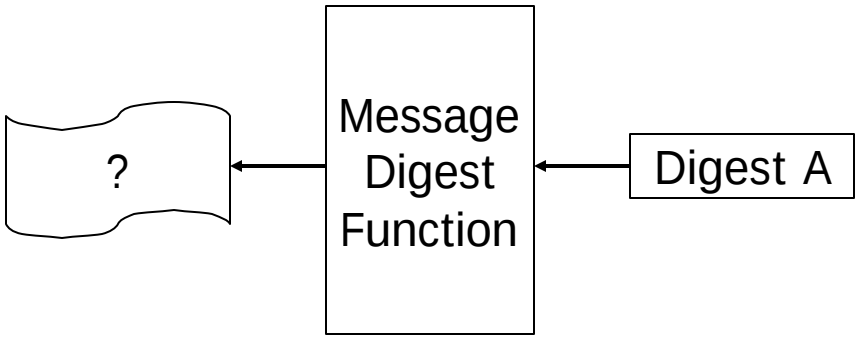
Message Digest



If A ≠B => Digest A ≠ Digest B

31

Message Digest



Extremely hard to get A from Digest A!

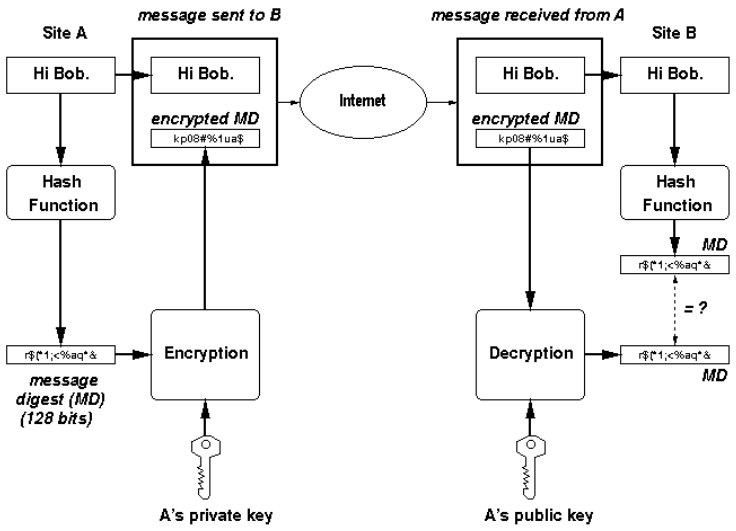
32

Performance of Message Digest Functions

- Message digest generation is a fast operation. For example, the hash generation rate of SHA-1 is 13 clock cycles per byte on a Pentium machine. So, a digest of a 1-Mbyte file would be generated in approximately 13 msec on a 1 GHz Pentium machine.

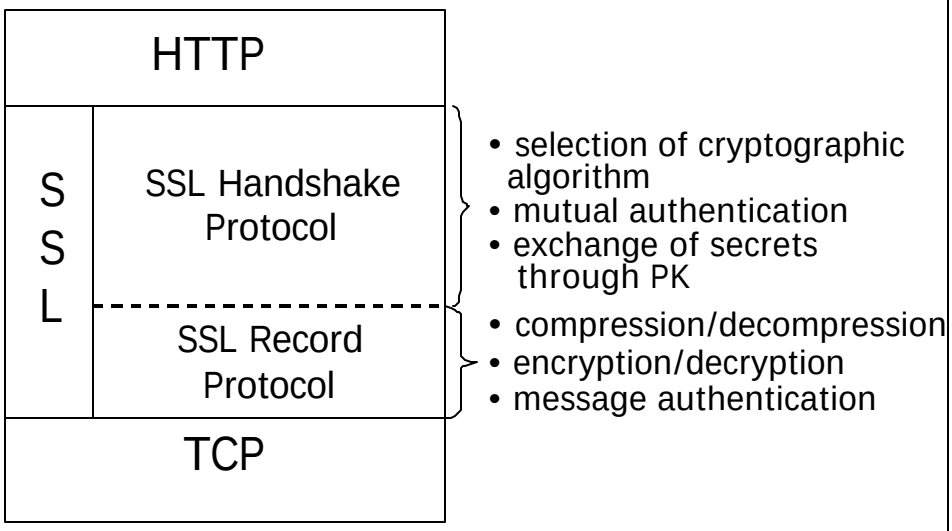
33

Digital Signature



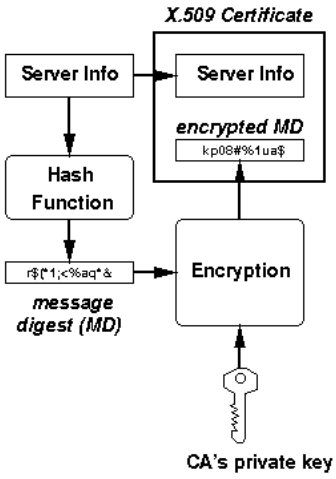
34

SSL Protocol Overview



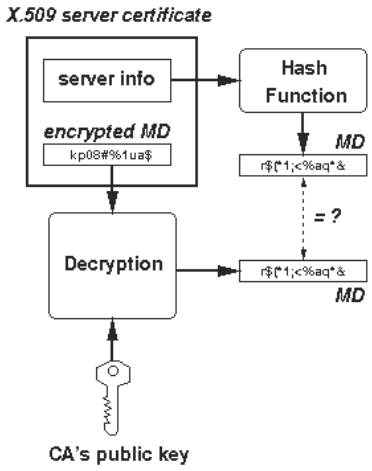
35

Generation of a Server Certificate



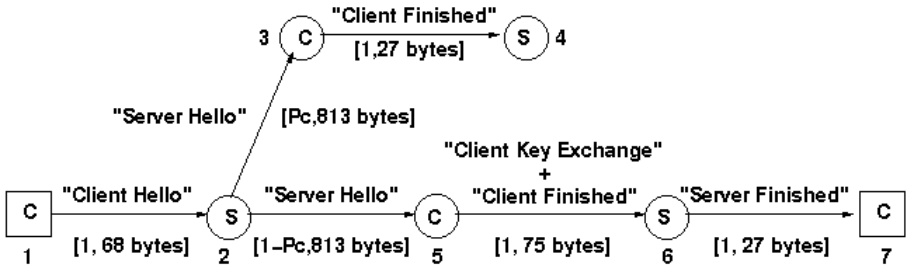
36

Verification of a Server Certificate



37

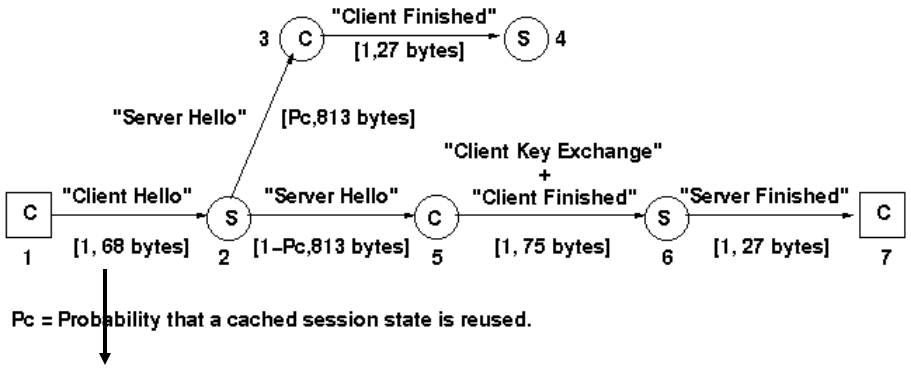
SSL Connection Establishment



Pc = Probability that a cached session state is reused.

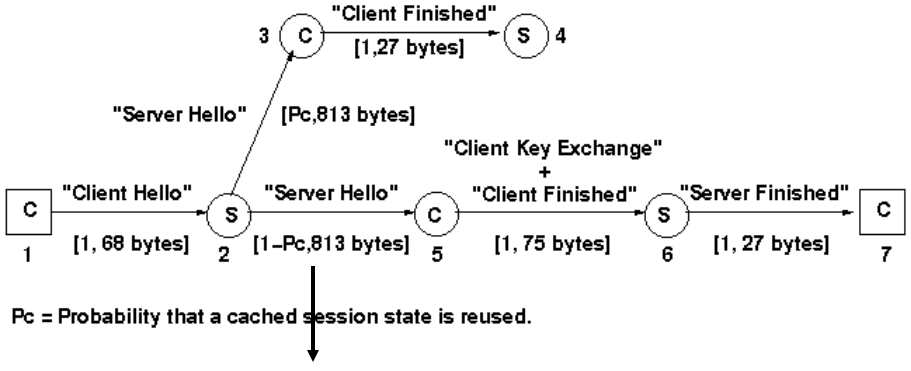
38

SSL Connection Establishment



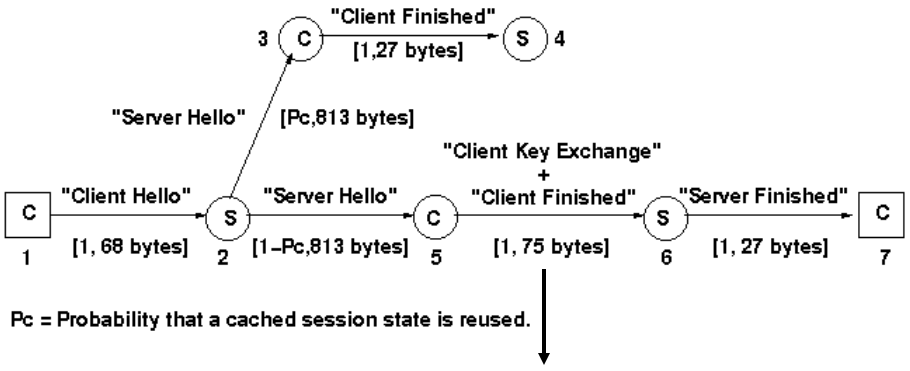
(Client random number, session id, cypher suites)

SSL Connection Establishment



(X.509 Certificate, server random number, server session ID, cypher suites)

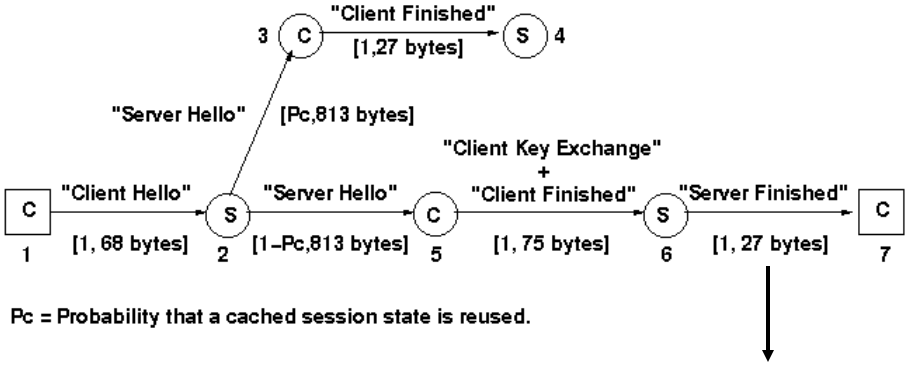
SSL Connection Establishment



(master secret key encrypted with server's public key)

41

SSL Connection Establishment



(digest of all messages sent by client encrypted with bulk encryption key)

42

CPU Times for Various Security Options

	Handshake Time (msec)	CPU Processing Time per KB (msec)
Low Security	10.2	0.104
Medium Security	23.8	0.268
High Security	48.0	0.609

Levels of security depend on key lengths and on the strength of the security algorithms used.

Additional Service Demands (sec) for Secure Download

	PDF	ZIP
Low Security	0.0495	0.1304
Medium Security	0.1250	0.3333
High Security	0.2781	0.7519

43

Results for Secure Downloads

No. Concurrent Downloads	X_PDF (files/sec)	X_ZIP (files/sec)	R_PDF sec	R_ZIP sec
Low Security				
20	2.25	3.15	1.78	5.09
40	2.26	3.17	3.55	10.08
60	2.25	3.18	5.32	15.10
80	2.25	3.18	7.10	20.12
Medium Security				
20	1.22	1.75	3.28	9.13
40	1.22	1.76	6.56	18.19
60	1.22	1.76	9.85	27.27
High Security				
20	0.63	0.91	6.34	17.49
40	0.63	0.92	12.69	34.93

44

Experimental Comparison of Two Servers

- Factors that affect performance: processor speed, number of processors, and main memory.
- Levels: values of a factor.

Factor	Levels
Processor Speed (GHz)	2.0, 2.4, 2.8, 3.1
No. processors	1, 2, 4, 8
Main memory (GB)	1, 2, 4

45

Using Confidence Intervals to Compare the Two Servers

- Select a representative workload and apply it to the two servers and measure the download times in each case.
- Compute the difference between the download times.

Type	Size (KB)	Elapsed Time (sec) Original Server	Elapsed Time (sec) New Server	New-Original
PDF	300	1.42	1.39	-0.03
PDF	301	1.42	1.38	-0.04
PDF	301	1.42	1.38	-0.03
PDF	301	1.42	1.38	-0.04
PDF	302	1.42	1.41	-0.01
PDF	302	1.42	1.42	0.00
PDF	302	1.42	1.38	-0.04
		. . . . .		
ZIP	1000	4.71	4.71	-0.01
ZIP	1001	4.72	4.58	-0.14
ZIP	1002	4.72	4.59	-0.13
ZIP	1004	4.73	4.60	-0.13
ZIP	1005	4.73	4.55	-0.18
ZIP	1005	4.73	4.71	-0.02
ZIP	1005	4.74	4.62	-0.12
ZIP	1005	4.74	4.58	-0.15
ZIP	1006	4.74	4.58	-0.16
ZIP	1007	4.75	4.62	-0.13

46

Using Confidence Intervals to Compare the Two Servers

- Compute the 95% confidence interval for the average difference between the download times.
- If the 95% confidence interval for the average difference contains zero, then the two servers are statistically identical at the 95% confidence level.

Difference (new-orig) for PDF Files:	
Mean	-0.0357
Standard Deviation	0.0235
Lower bound 95% CI Difference	-0.0380
Upper bound 95% CI Difference	-0.0334

Difference (new-orig) for ZIP Files:	
Mean	-0.1109
Standard Deviation	0.0631
Lower bound 95% CI Difference	-0.1160
Upper bound 95% CI Difference	-0.1058

The new server outperforms the original server for both PDF and ZIP files at the 95% confidence level.

47