INFRASTRUCTURE DESIGN AND MANAGEMENT

2110684 Information System Architecture

Natawut Nupairoj Ph.D.

Department of Computer Engineering, Chulalongkorn University

Agenda

- Capacity Planning
- System Availability and Monitoring
- Security

CAPACITY PLANNING

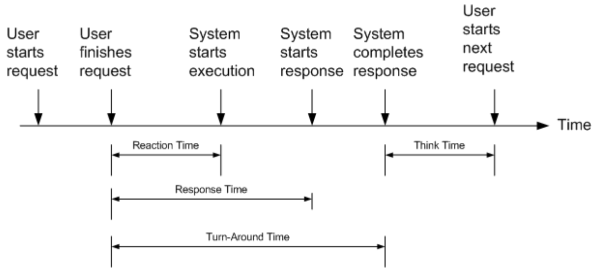
Capacity Planning

- Determining the production capacity needed by an organization to meet changing demands for its products
- Infrastructure Sizing
  - Servers, Network, Storage
  - Depends on to-be-deployed applications and hardware
  - Vendor can provide more accurate sizing
  - Can refer to standard benchmark for rough estimation
    - SPEC
    - TPC

Popular Metrics

- Time - Execution Time
- Rate - Throughput and Processing Speed
- Resource – Utilization
- Ratio - Cost Effectiveness
- Reliability – Error Rate
- Availability – Mean Time To Failure (MTTF)

Definition of Time



Throughput

- Number of jobs that can be processed in a unit time.
- Aka. Bandwidth (in communication).
- The more, the better.
- High throughput does not necessary mean low execution time.
  - Pipeline.
  - Multiple execution units.

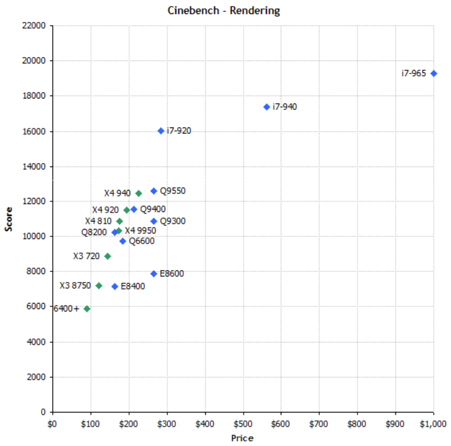
Utilization

- The percentage of resources being used
- Ratio of
  - busy time vs. total time
- The more the better?
  - True for manager
  - But may be not for user/customer
- Resource with highest utilization is the "bottleneck"

Cost Effectiveness

- Peak performance/cost ratio
- Price/performance ratio

Price/Performance Ratio



From Tom's Hardware Guide: CPU Chart 2009

SPEC

- By Standard Performance Evaluation Corporation
- Using real applications
- http://www.spec.org
- SPEC CPU2006
  - Measure CPU performance
    - Raw speed of completing a single task
    - Rates of processing many tasks
  - CINT2006 - Integer performance
  - CFP2006 - Floating-point performance

CINT2006

400.perlbench	C	PERL Programming Language
401.bzip2	C	Compression
403.gcc	C	C Compiler
429.mcf	C	Combinatorial Optimization
445.gobmk	C	Artificial Intelligence: go
456.hmmer	C	Search Gene Sequence
458.sjeng	C	Artificial Intelligence: chess
462.libquantum	C	Physics: Quantum Computing
464.h264ref	C	Video Compression
471.omnetpp	C++	Discrete Event Simulation
473.astar	C++	Path-finding Algorithms
483.xalancbmk	C++	XML Processing

CFP2006

410.bwaves	Fortran	Fluid Dynamics
416.gamess	Fortran	Quantum Chemistry
433.milc	C	Physics: Quantum Chromodynamics
434.zeusmp	Fortran	Physics / CFD
435.gromacs	C/Fortran	Biochemistry/Molecular Dynamics
436.cactusADM	C/Fortran	Physics / General Relativity
437.leslie3d	Fortran	Fluid Dynamics
444.namd	C++	Biology / Molecular Dynamics
447.dealII	C++	Finite Element Analysis
450.soplex	C++	Linear Programming, Optimization
453.povray	C++	Image Ray-tracing
454.calculix	C/Fortran	Structural Mechanics
459.GemsFDTD	Fortran	Computational Electromagnetics
465.tonto	Fortran	Quantum Chemistry
470.lbm	C	Fluid Dynamics
481.wrf	C/Fortran	Weather Prediction
482.sphinx3	C	Speech recognition

Top 10 CINT2006 Speed (as of 29 July 2009)

System	Result	# Cores	# Chips	Cores/Chip	Processor
Sun Blade X6275 (Intel Xeon X5570 2.93GHz)	37.4	8	2	4	Intel Xeon X5570
ASUS TS700-E6 (Z8PE-D12X) server system (Intel Xeon W5580)	37.3	8	2	4	Intel Xeon W5580
CELSIUS R670, Intel Xeon W5580	37.2	8	2	4	Intel Xeon W5580
Sun Blade X6270 (Intel Xeon X5570 2.93GHz)	36.9	8	2	4	Intel Xeon X5570
Sun Ultra 27 (Intel Xeon W3570 3.2GHz)	36.8	4	1	4	Intel Xeon W3570
Sun Fire X4170 (Intel Xeon X5570 2.93GHz)	36.8	8	2	4	Intel Xeon X5570
Sun Blade X6270 (Intel Xeon X5570 2.93GHz)	36.8	8	2	4	Intel Xeon X5570
Sun Blade X6275 (Intel Xeon X5570 2.93GHz)	36.7	8	2	4	Intel Xeon X5570
Dell Precision T7500 (Intel Xeon W5580, 3.20 GHz)	36.7	8	2	4	Intel Xeon W5580
CELSIUS M470, Intel Xeon W5580	36.6	4	1	4	Intel Xeon W5580

Other Interesting SPECs

- SPEC jAppServer2004
  - Measure the performance of J2EE 1.3 application servers
- SPEC Web2009
  - Emulates users sending browser requests over broadband Internet connections to a web server
- SPECpower_ssj2008
  - Evaluates the power and performance characteristics of volume server class computers

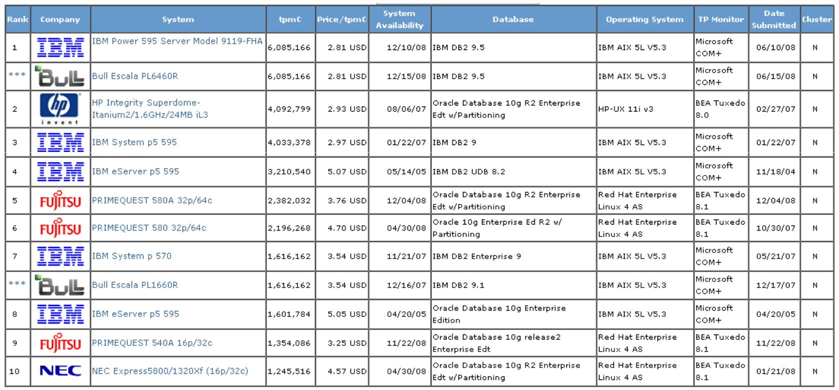
TPC

- Transaction Processing Performance Council
- http://www.tpc.org
- TPC-C: performance of Online Transaction Processing (OLTP) system
  - tpmC: transactions per minute.
  - $/tpmC: price/performance.
- Simulate the wholesale company environment
  - N warehouses, 10 sales districts each.
  - Each district serves 3,000 customers with one terminal in each district.

TPC Transactions

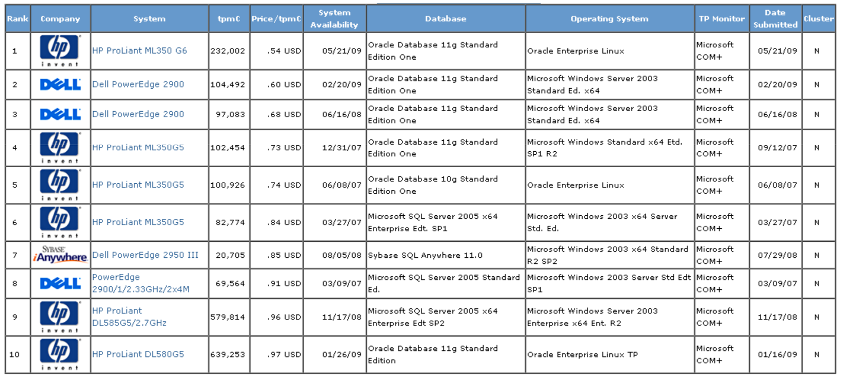
- An operator can perform one of the five transactions
  - Create a new order.
  - Make a payment.
  - Check the order's status.
  - Deliver an order.
  - Examine the current stock level.
- Measure from the throughput of New-Order.
- Top 10 (Performance, Price/Performance).

Top 10 TPC-C Performance (as of 29 July 2009)



Rank	Company	System	tpmC	Price/tpmC	System Availability	Database	Operating System	TP Monitor	Date Submitted	Cluster
1	IBM	IBM Power 595 Server Model 9119-FHA	6,085,166	2.81 USD	12/10/08	IBM DB2 9.5	IBM AIX 5L V5.3	Microsoft COM+	06/10/08	N
***	Bull	Bull Escala PL6460R	6,085,166	2.81 USD	12/15/08	IBM DB2 9.5	IBM AIX 5L V5.3	Microsoft COM+	06/15/08	N
2	hp invent	HP Integrity Superdome-Itanium2/1.6GHz/24MB iL3	4,092,799	2.93 USD	08/06/07	Oracle Database 10g R2 Enterprise Edt w/Partitioning	HP-UX 11i v3	BEA Tuxedo 8.0	02/27/07	N
3	IBM	IBM System p5 595	4,033,378	2.97 USD	01/22/07	IBM DB2 9	IBM AIX 5L V5.3	Microsoft COM+	01/22/07	N
4	IBM	IBM eServer p5 595	3,210,540	5.07 USD	05/14/05	IBM DB2 UDB 8.2	IBM AIX 5L V5.3	Microsoft COM+	11/18/04	N
5	FUJITSU	PRIMEQUEST 580A 32p/64c	2,382,032	3.76 USD	12/04/08	Oracle Database 10g R2 Enterprise Edt w/Partitioning	Red Hat Enterprise Linux 4 AS	BEA Tuxedo 8.1	12/04/08	N
6	FUJITSU	PRIMEQUEST 580 32p/64c	2,196,268	4.70 USD	04/30/08	Oracle 10g Enterprise Ed R2 w/ Partitioning	Red Hat Enterprise Linux 4 AS	BEA Tuxedo 8.1	10/30/07	N
7	IBM	IBM System p 570	1,616,162	3.54 USD	11/21/07	IBM DB2 Enterprise 9	IBM AIX 5L V5.3	Microsoft COM+	05/21/07	N
***	Bull	Bull Escala PL1660R	1,616,162	3.54 USD	12/16/07	IBM DB2 9.1	IBM AIX 5L V5.3	Microsoft COM+	12/17/07	N
8	IBM	IBM eServer p5 595	1,601,784	5.05 USD	04/20/05	Oracle Database 10g Enterprise Edition	IBM AIX 5L V5.3	Microsoft COM+	04/20/05	N
9	FUJITSU	PRIMEQUEST 540A 16p/32c	1,354,086	3.25 USD	11/22/08	Oracle Database 10g release2 Enterprise Edt	Red Hat Enterprise Linux 4 AS	BEA Tuxedo 8.1	11/22/08	N
10	NEC	NEC Express5800/1320Xf (16p/32c)	1,245,516	4.57 USD	04/30/08	Oracle Database 10g R2 Enterprise Edt w/Partitioning	Red Hat Enterprise Linux 4 AS	BEA Tuxedo 8.1	01/21/08	N

Top 10 TPC-C Price/Performance (as of 29 July 2009)



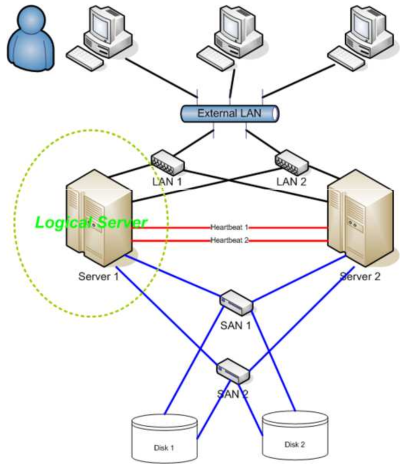
Rank	Company	System	tpmC	Price/tpmC	System Availability	Database	Operating System	TP Monitor	Date Submitted	Cluster
1	hp invent	HP ProLiant ML350 G6	232,002	.54 USD	05/21/09	Oracle Database 11g Standard Edition One	Oracle Enterprise Linux	Microsoft COM+	05/21/09	N
2	DELL	Dell PowerEdge 2900	104,492	.60 USD	02/20/09	Oracle Database 11g Standard Edition One	Microsoft Windows Server 2003 Standard Ed. x64	Microsoft COM+	02/20/09	N
3	DELL	Dell PowerEdge 2900	97,083	.68 USD	06/16/08	Oracle Database 11g Standard Edition One	Microsoft Windows Server 2003 Standard Ed. x64	Microsoft COM+	06/16/08	N
4	hp invent	HP ProLiant ML350G5	102,454	.73 USD	12/31/07	Oracle Database 11g Standard Edition One	Microsoft Windows Standard x64 Etd. SP1 R2	Microsoft COM+	09/12/07	N
5	hp invent	HP ProLiant ML350G5	100,926	.74 USD	06/08/07	Oracle Database 10g Standard Edition One	Oracle Enterprise Linux	Microsoft COM+	06/08/07	N
6	hp invent	HP ProLiant ML350G5	82,774	.84 USD	03/27/07	Microsoft SQL Server 2005 x64 Enterprise Edt. SP1	Microsoft Windows 2003 x64 Server Std. Ed.	Microsoft COM+	03/27/07	N
7	SYBASE iAnywhere	Dell PowerEdge 2950 III	20,705	.85 USD	08/05/08	Sybase SQL Anywhere 11.0	Microsoft Windows 2003 x64 Standard R2 SP2	Microsoft COM+	07/29/08	N
8	DELL	PowerEdge 2900/1/2.33GHz/2x4M	69,564	.91 USD	03/09/07	Microsoft SQL Server 2005 Standard Ed.	Microsoft Windows 2003 Server Std Edt SP1	Microsoft COM+	03/09/07	N
9	hp invent	HP ProLiant DL585G5/2.7GHz	579,814	.96 USD	11/17/08	Microsoft SQL Server 2005 x64 Enterprise Edt SP2	Microsoft Windows Server 2003 Enterprise x64 Ent. R2	Microsoft COM+	11/17/08	N
10	hp invent	HP ProLiant DL580G5	639,253	.97 USD	01/26/09	Oracle Database 11g Standard Edition	Oracle Enterprise Linux TP	Microsoft COM+	01/16/09	N

SYSTEM AVAILABILITY AND MONITORING

System Availability

- How to ensures a certain absolute degree of operational continuity during a given measurement period
- Availability includes ability of the user community to access the system, whether to submit new work, update or alter existing work, or collect the results of previous work
- Model of Availability
  - Active-Standby: HA Cluster or Failover Cluster
  - Active-Active: Server Load Balancing

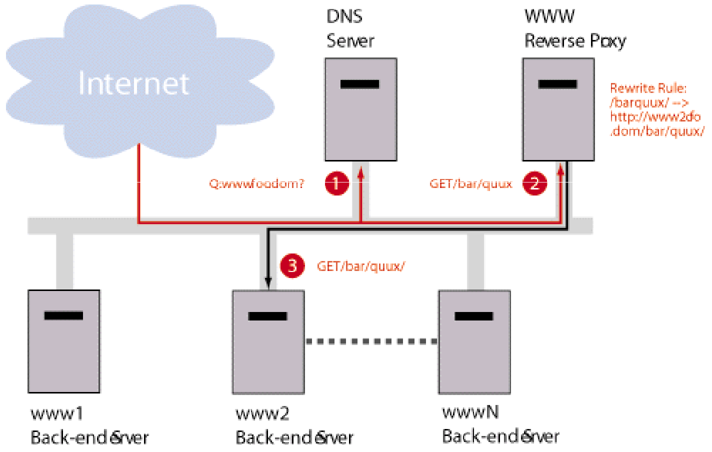
HA Cluster



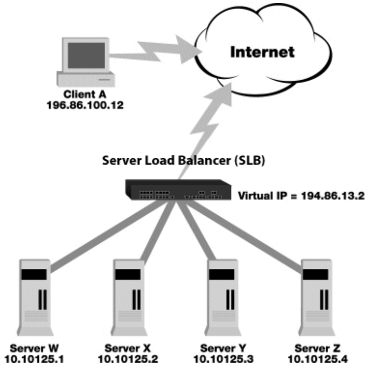
Server Load Balancing

- Spread work between two or more computers, network links, CPUs, hard drives, or other resources, in order to get optimal resource utilization, throughput, or response time
- Approaches
  - The DNS Approach
  - The Reverse Proxy Approach
  - Load balancer Approach

Reverse Proxy Approach

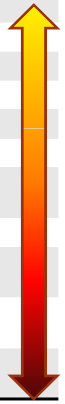


Server Load Balancing



Downtime Table

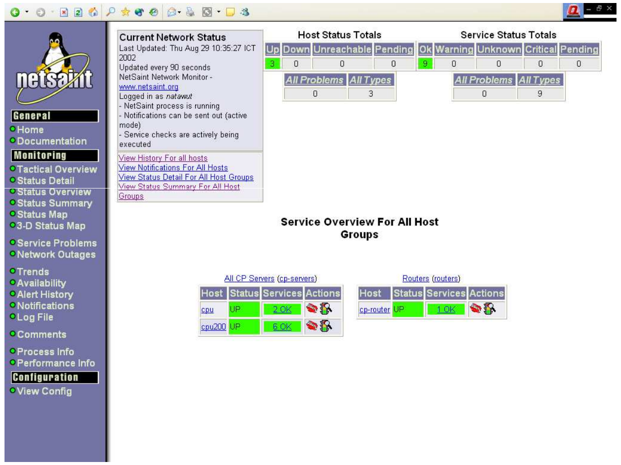
Availability %	Downtime per year	Downtime per month*	Downtime per week
90%	36.5 days	72 hours	16.8 hours
95%	18.25 days	36 hours	8.4 hours
98%	7.30 days	14.4 hours	3.36 hours
99%	3.65 days	7.20 hours	1.68 hours
99.5%	1.83 days	3.60 hours	50.4 min
99.8%	17.52 hours	86.23 min	20.16 min
99.9% ("three nines")	8.76 hours	43.2 min	10.1 min
99.95%	4.38 hours	21.56 min	5.04 min
99.99% ("four nines")	52.6 min	4.32 min	1.01 min
99.999% ("five nines")	5.26 min	25.9 s	6.05 s
99.9999% ("six nines")	31.5 s	2.59 s	0.605 s



Budget

Sample Network Monitoring Applications

- There are several network management applications
  - OS Tools
    - Ping, tracerout, netstat, etc.
  - Freewares
    - Netsaint, MRTG, snort, etc.
  - Commercial
    - CA Unicenter, HP Openview, IBM Trivoli, CiscoWorks.



Current Network Status
Last Updated: Thu Aug 29 10:35:27 ICT 2002
Updated every 90 seconds
NetSaint Network Monitor - www.netsaint.org
Logged in as *natawut*
- NetSaint process is running
- Notifications can be sent out (active mode)
- Service checks are actively being executed

View History For all hosts
View Notifications For All Hosts
View Status Detail For All Host Groups
View Status Summary For All Host Groups

Host Status Totals

Up	Down	Unreachable	Pending
3	0	0	0

All Problems	All Types
0	3

Service Status Totals

Ok	Warning	Unknown	Critical	Pending
9	0	0	0	0

All Problems	All Types
0	9

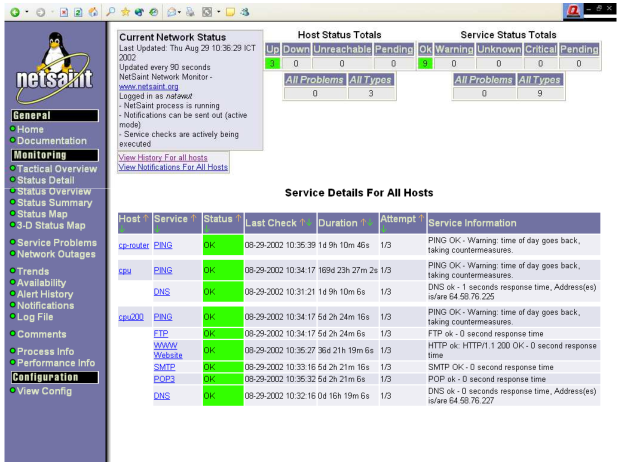
Service Overview For All Host Groups

All CP Servers (cp-servers)

Host	Status	Services	Actions
cpu	UP	2 OK	
cpu200	UP	6 OK	

Routers (routers)

Host	Status	Services	Actions
cp-router	UP	1 OK	



Current Network Status
Last Updated: Thu Aug 29 10:36:29 ICT 2002
Updated every 90 seconds
NetSaint Network Monitor - www.netsaint.org
Logged in as *natawut*
- NetSaint process is running
- Notifications can be sent out (active mode)
- Service checks are actively being executed

View History For all hosts
View Notifications For All Hosts

Host Status Totals

Up	Down	Unreachable	Pending
3	0	0	0

All Problems	All Types
0	3

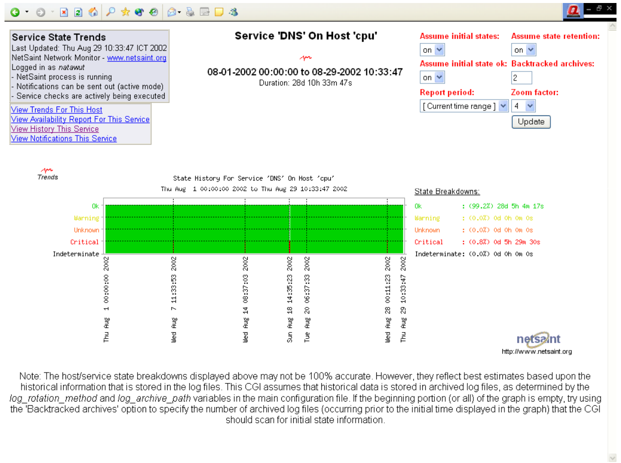
Service Status Totals

Ok	Warning	Unknown	Critical	Pending
9	0	0	0	0

All Problems	All Types
0	9

Service Details For All Hosts

Host	Service	Status	Last Check	Duration	Attempt	Service Information
cp-router	PING	OK	08-29-2002 10:35:39	1d 9h 10m 46s	1/3	PING OK - Warning: time of day goes back, taking countermeasures.
cpu	PING	OK	08-29-2002 10:34:17	169d 23h 27m 2s	1/3	PING OK - Warning: time of day goes back, taking countermeasures.
	DNS	OK	08-29-2002 10:31:21	1d 9h 10m 6s	1/3	DNS ok - 1 seconds response time, Address(es) is/are 64.58.76.225
cpu200	PING	OK	08-29-2002 10:34:17	5d 2h 24m 16s	1/3	PING OK - Warning: time of day goes back, taking countermeasures.
	FTP	OK	08-29-2002 10:34:17	5d 2h 24m 6s	1/3	FTP ok - 0 second response time
	WWW Website	OK	08-29-2002 10:35:27	36d 21h 19m 6s	1/3	HTTP ok: HTTP/1.1 200 OK - 0 second response time
	SMTP	OK	08-29-2002 10:33:16	5d 2h 21m 16s	1/3	SMTP OK - 0 second response time
	POP3	OK	08-29-2002 10:35:32	5d 2h 21m 6s	1/3	POP ok - 0 second response time
	DNS	OK	08-29-2002 10:32:16	0d 16h 19m 6s	1/3	DNS ok - 0 seconds response time, Address(es) is/are 64.58.76.227



Service State Trends
Last Updated: Thu Aug 29 10:33:47 ICT 2002
NetSaint Network Monitor - www.netsaint.org
Logged in as *natawut*
- NetSaint process is running
- Notifications can be sent out (active mode)
- Service checks are actively being executed

View Trends For This Host
View Availability Report For This Service
View History This Service
View Notifications This Service

Service 'DNS' On Host 'cpu'

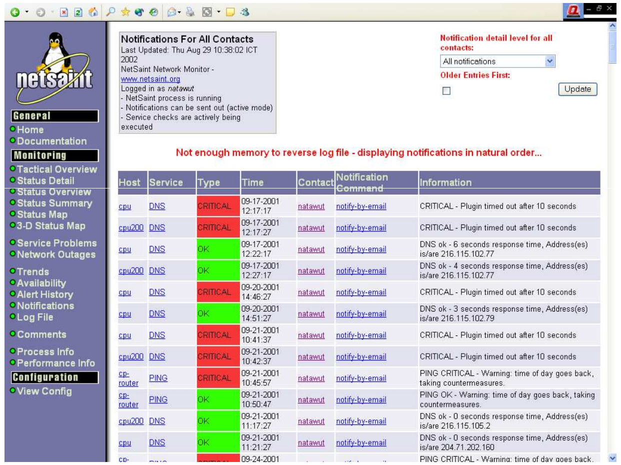
08-01-2002 00:00:00 to 08-29-2002 10:33:47
Duration: 28d 10h 33m 47s

Assume initial states: on
Assume state retention: on
Assume initial state ok: on
Backtracked archives: 2
Report period: [Current time range]
Zoom factor: 4
Update

State Breakdowns:

```
Ok           : (99.2%) 28d 5h 4m 17s
Warning      : (0.0%) 0d 0h 0m 0s
Unknown      : (0.0%) 0d 0h 0m 0s
Critical     : (0.8%) 0d 5h 29m 30s
Indeterminate: (0.0%) 0d 0h 0m 0s
```

Note: The host/service state breakdowns displayed above may not be 100% accurate. However, they reflect best estimates based upon the historical information that is stored in the log files. This CGI assumes that historical data is stored in archived log files, as determined by the *log_rotation_method* and *log_archive_path* variables in the main configuration file. If the beginning portion (or all) of the graph is empty, try using the 'Backtracked archives' option to specify the number of archived log files (occurring prior to the initial time displayed in the graph) that the CGI should scan for initial state information.



Notifications For All Contacts
Last Updated: Thu Aug 29 10:38:02 ICT 2002
NetSaint Network Monitor - www.netsaint.org
Logged in as *natawut*
- NetSaint process is running
- Notifications can be sent out (active mode)
- Service checks are actively being executed

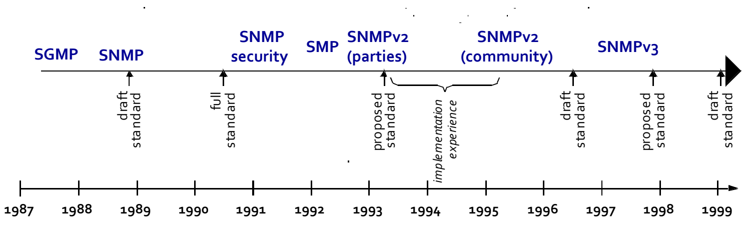
Notification detail level for all contacts: All notifications
Older Entries First: □
Update

Not enough memory to reverse log file - displaying notifications in natural order...

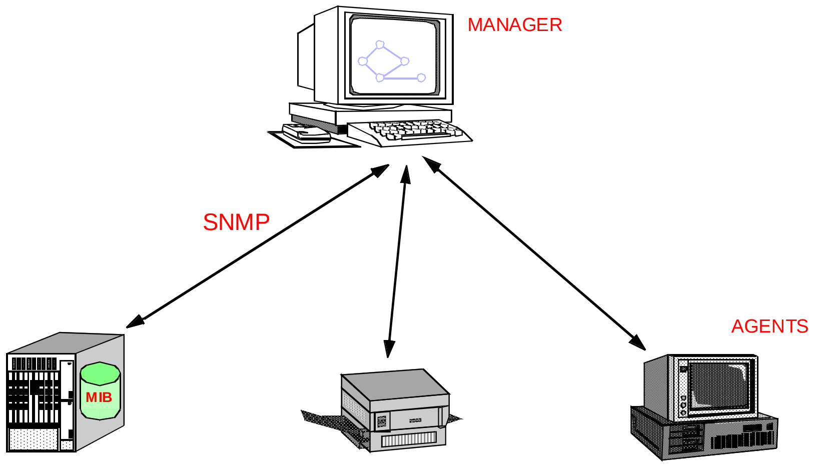
Host	Service	Type	Time	Contact	Notification Command	Information
cpu	DNS	CRITICAL	09-17-2001 12:17:17	natawut	notify-by-email	CRITICAL - Plugin timed out after 10 seconds
cpu200	DNS	CRITICAL	09-17-2001 12:17:27	natawut	notify-by-email	CRITICAL - Plugin timed out after 10 seconds
cpu	DNS	OK	09-17-2001 12:22:17	natawut	notify-by-email	DNS ok - 6 seconds response time, Address(es) is/are 216.115.102.77
cpu200	DNS	OK	09-17-2001 12:27:17	natawut	notify-by-email	DNS ok - 4 seconds response time, Address(es) is/are 216.115.102.77
cpu	DNS	CRITICAL	09-20-2001 14:46:27	natawut	notify-by-email	CRITICAL - Plugin timed out after 10 seconds
cpu	DNS	OK	09-20-2001 14:51:27	natawut	notify-by-email	DNS ok - 3 seconds response time, Address(es) is/are 216.115.102.79
cpu	DNS	CRITICAL	09-21-2001 10:41:37	natawut	notify-by-email	CRITICAL - Plugin timed out after 10 seconds
cpu200	DNS	CRITICAL	09-21-2001 10:42:37	natawut	notify-by-email	CRITICAL - Plugin timed out after 10 seconds
cp-router	PING	CRITICAL	09-21-2001 10:45:57	natawut	notify-by-email	PING CRITICAL - Warning: time of day goes back, taking countermeasures.
cp-router	PING	OK	09-21-2001 10:50:47	natawut	notify-by-email	PING OK - Warning: time of day goes back, taking countermeasures.
cpu200	DNS	OK	09-21-2001 11:17:27	natawut	notify-by-email	DNS ok - 0 seconds response time, Address(es) is/are 216.115.105.2
cpu	DNS	OK	09-21-2001 11:21:27	natawut	notify-by-email	DNS ok - 0 seconds response time, Address(es) is/are 204.71.202.160
cp-			09-24-2001			PING CRITICAL - Warning: time of day goes back,

SNMP

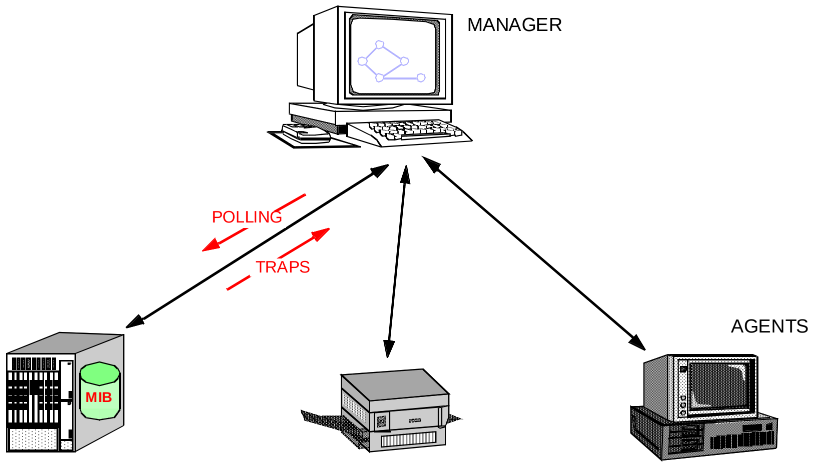
- Simple Network Management Protocol.



Basic SNMP Concepts

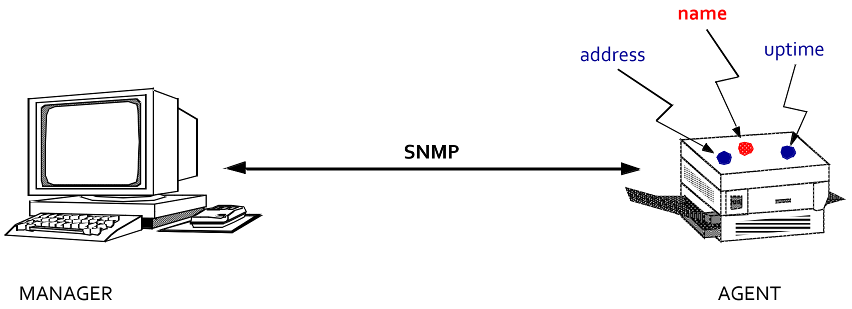


Operational Modes



SNMP Frameworks – MIB

- Management Information Base
  - MIB Objects
    - Variables that represent the resources of the system.
    - Can have several types of values.



SECURITY

Security Management

- Security must be considered both at infrastructure level and application level
- Infrastructure level
  - Control physical access
  - Operating system level = "hardening"
  - Secure coding
    - Avoid certain coding patterns to remove vulnerbilities
  - Network security

Security Equipment

- Firewall
- IDS / IPS
- Anti-Virus
- Spam Filter
- Authentication

Two-Factor Authentication

- Something you know
  - Password
- Something you have
  - ID Card, Credit Card, Mobile Phone
- Something you are
  - Biometric: retina, voice, fingerprint, etc.

Authentication Devices

What is Network Security?

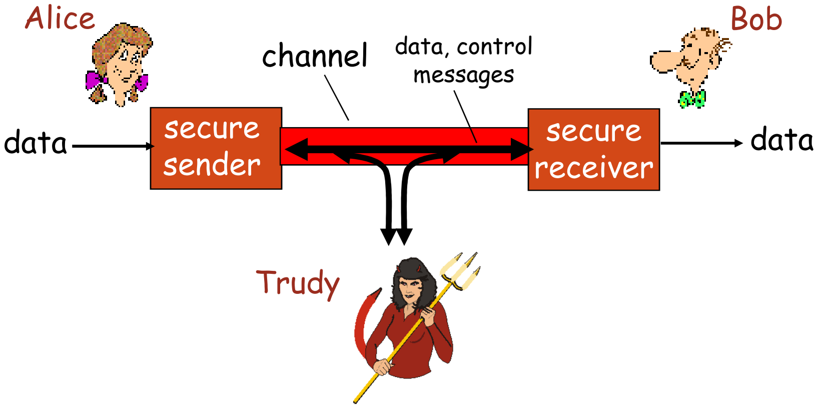
- Confidentiality: only sender, intended receiver should "understand" message contents.
- Authentication: confirm identity of each other.
- Message Integrity: ensure message not altered (in transit, or afterwards) without detection.

Frank and Ernest

THAT'S THE GREAT THING ABOUT THE INTERNET - ANONYMITY.
E-Mail: FandE@thecomics.com. www.frankandernest.com
11/12
THAVES

Copyright (c) 1998 by Thaves. Distributed from www.thecomics.com.

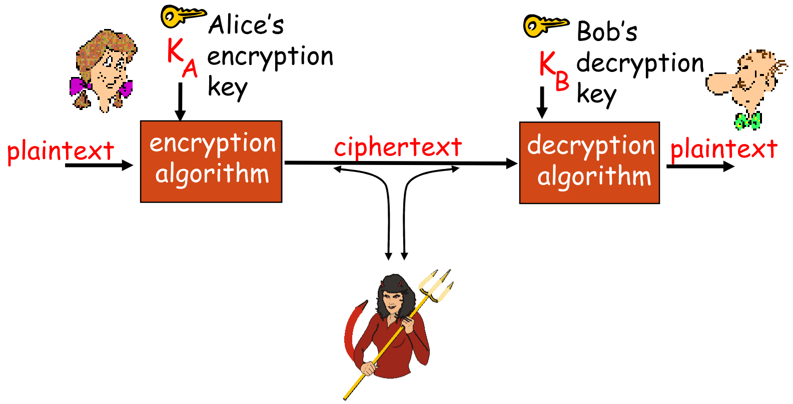
Friends and Enemies: Alice, Bob, Trudy



Who might Bob, Alice be?

- ☐… well, *real-life* Bobs and Alices!
- ☐Web browser/server for electronic transactions (e.g., on-line purchases)
- ☐on-line banking client/server
- ☐DNS servers
- ☐routers exchanging routing table updates
- ☐other examples?

The language of cryptography



symmetric key crypto: sender, receiver keys *identical*

public-key crypto: encryption key *public*, decryption key *secret* (private)

Symmetric key cryptography

substitution cipher: substituting one thing for another

- monoalphabetic cipher: substitute one letter for another

```
 plaintext:  abcdefghijklmnopqrstuvwxyz

ciphertext:  mnbvcxzasdfghjklpoiuytrewq
```

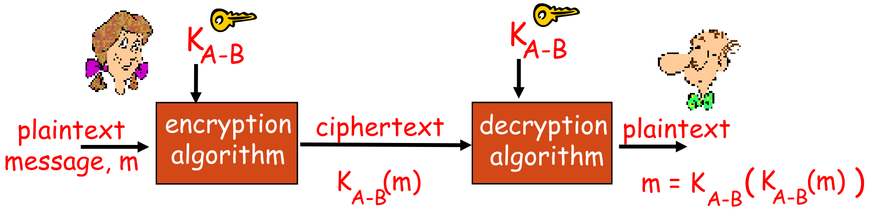
E.g.:
```
 Plaintext: bob. i love you. alice
ciphertext: nkn. s gktc wky. mgsbc
```

Q: How hard to break this simple cipher?:

❑ brute force (how hard?)

❑ other?

Symmetric key cryptography



symmetric key crypto:

Bob and Alice share same (symmetric) key: K_{A-B}

- e.g., key is knowing substitution pattern in mono alphabetic substitution cipher
- Q: how do Bob and Alice agree on key value?

Symmetric key crypto: DES

DES: Data Encryption Standard

☐ US encryption standard [NIST 1993]

☐ 56-bit symmetric key, 64-bit plaintext input

☐ How secure is DES?

- DES Challenge: 56-bit-key-encrypted phrase ("Strong cryptography makes the world a safer place") decrypted (brute force) in 4 months
- no known "backdoor" decryption approach

☐ making DES more secure:

- use three keys sequentially (3-DES) on each datum
- use cipher-block chaining

Public Key Cryptography

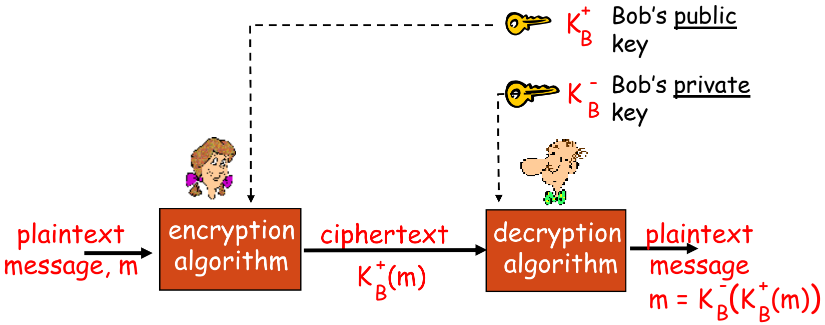
symmetric key crypto

- Sender and receiver know shared secret key
- Q: how to agree on key in first place (particularly if never "met")?

public key cryptography

- radically different approach [Diffie-Hellman76, RSA78]
- sender, receiver do *not* share secret key
- *public* encryption key known to *all*
- *private* decryption key known only to receiver

Public key cryptography



K_B^+ Bob's public key

K_B^- Bob's private key

plaintext message, m

encryption algorithm

ciphertext $K_B^+(m)$

decryption algorithm

plaintext message $m = K_B^-(K_B^+(m))$

Digital Signatures

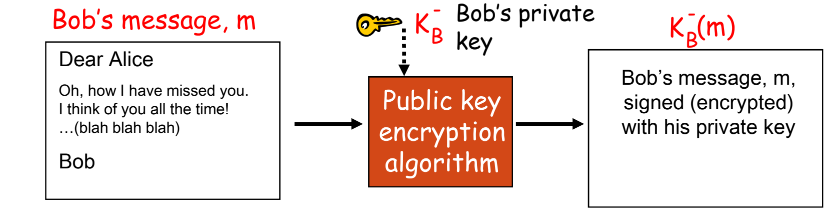
Cryptographic technique analogous to hand-written signatures.

- sender (Bob) digitally signs document
  - establishing he is document owner/creator.
- verifiable, nonforgeable:
  - recipient (Alice) can prove to someone that Bob, and no one else (including Alice), must have signed document

Digital Signatures

Simple digital signature for message m:

- Bob signs m by encrypting with his private key K_B^-, creating "signed" message, $K_B(m)$



Bob's message, m

Dear Alice

Oh, how I have missed you.
I think of you all the time!
…(blah blah blah)

Bob

K_B^- Bob's private key

Public key encryption algorithm

$K_B^-(m)$

Bob's message, m, signed (encrypted) with his private key

Digital Signatures (more)

- Suppose Alice receives msg m, digital signature $K_B^-(m)$
- Alice verifies m signed by Bob by applying Bob's public key K_B^+ to $K_B^-(m)$ then checks $K_B^+(K_B^-(m)) = m$.
- If $K_B^+(K_B^-(m)) = m$, whoever signed m must have used Bob's private key.

Alice thus verifies that:

Bob signed m.

No one else signed m.

Bob signed m and not m'.

Non-repudiation:

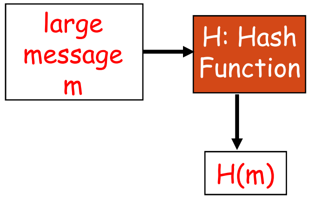
✓ Alice can take m, and signature $K_B^-(m)$ to court and prove that Bob signed m.

Message Digests

Computationally expensive to public-key-encrypt long messages

Goal: fixed-length, easy- to-compute digital "fingerprint"

- apply hash function H to *m*, get fixed size message digest, *H(m).*



large message m

H: Hash Function

H(m)

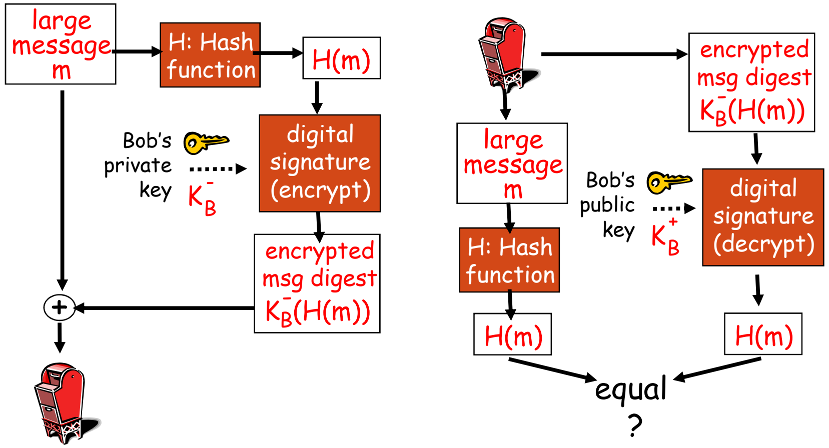
Hash function properties:

- many-to-1
- produces fixed-size msg digest (fingerprint)
- given message digest x, computationally infeasible to find m such that x = H(m)

Digital signature = signed message digest

Bob sends digitally signed message:

Alice verifies signature and integrity of digitally signed message:



large message m

H: Hash function

H(m)

Bob's private key K_B^-

digital signature (encrypt)

encrypted msg digest $K_B^-(H(m))$

+

encrypted msg digest $K_B^-(H(m))$

large message m

H: Hash function

H(m)

Bob's public key K_B^+

digital signature (decrypt)

H(m)

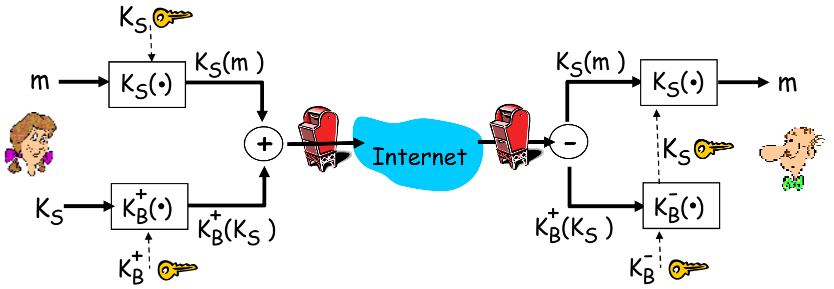
equal ?

Hash Function Algorithms

- MD5 hash function widely used (RFC 1321)
  - computes 128-bit message digest in 4-step process.
  - arbitrary 128-bit string x, appears difficult to construct msg m whose MD5 hash is equal to x.
- SHA-1 is also used.
  - US standard [NIST, FIPS PUB 180-1]
  - 160-bit message digest

Sample Application Secure e-mail

- Alice wants to send confidential e-mail, m, to Bob.

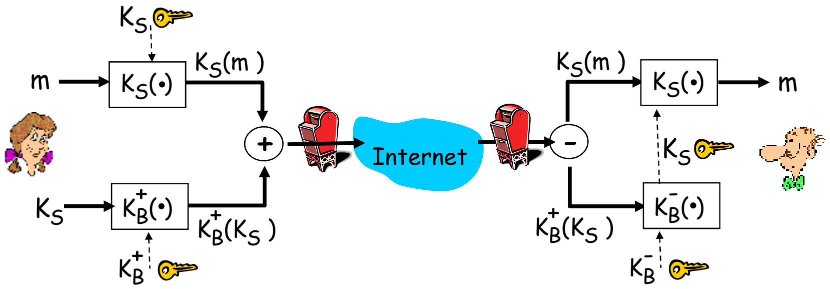


Alice:

- generates random *symmetric* private key, K_S.
- encrypts message with K_S (for efficiency)
- also encrypts K_S with Bob's public key.
- sends both $K_S(m)$ and $K_B(K_S)$ to Bob.

Secure e-mail

- Alice wants to send confidential e-mail, m, to Bob.

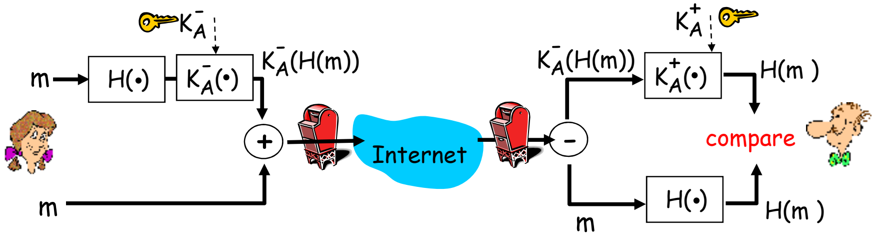


Bob:

- uses his private key to decrypt and recover K_S
- uses K_S to decrypt $K_S(m)$ to recover m

Secure e-mail (continued)

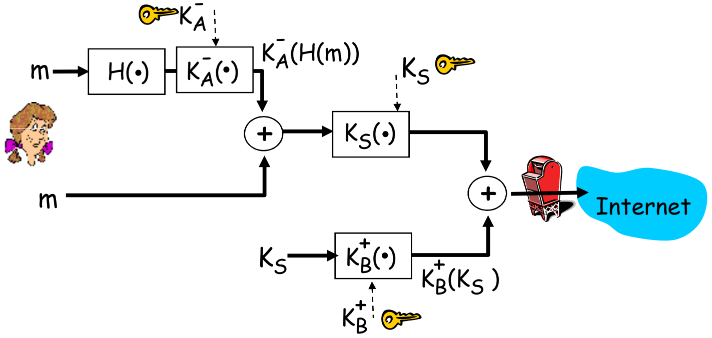
- Alice wants to provide sender authentication message integrity.



- Alice digitally signs message.
- sends both message (in the clear) and digital signature.

Secure e-mail (continued)

- Alice wants to provide secrecy, sender authentication, message integrity.



Alice uses three keys: her private key, Bob's public key, newly created symmetric key

Trusted Intermediaries

Public key problem:

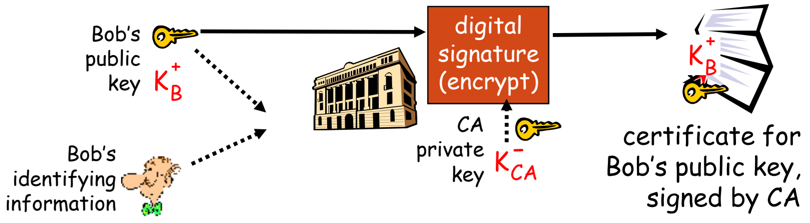
- When Alice obtains Bob's public key (from web site, e-mail, diskette), how does she know it is Bob's public key, not Trudy's?

Solution:

- trusted certification authority (CA)

Certification Authorities

- Certification authority (CA): binds public key to particular entity, E.
- E (person, router) registers its public key with CA.
  - E provides "proof of identity" to CA.
  - CA creates certificate binding E to its public key.
  - certificate containing E's public key digitally signed by CA – CA says "this is E's public key"



Bob's public key K_B^+

Bob's identifying information

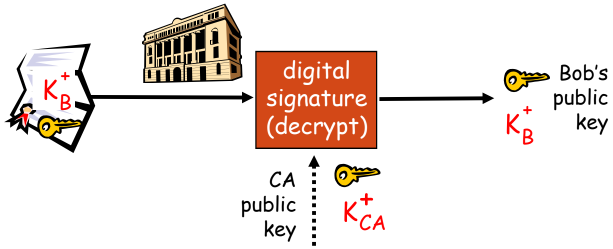
digital signature (encrypt)

CA private key K_{CA}^-

certificate for Bob's public key, signed by CA

Certification Authorities

- When Alice wants Bob's public key:
  - gets Bob's certificate (Bob or elsewhere).
  - apply CA's public key to Bob's certificate, get Bob's public key



digital signature (decrypt)

CA public key K_{CA}^+

Bob's public key K_B^+

Smart Card

- Pocket-size card with circuit to process information
  - Retrieve / store information
  - Digital signing

References

- J. Kurose and K. Ross, *Computer Networking: A Top-Down Approach Featuring the Internet*, 2nd Edition, Addison Wesley, 2002.
- P. Sokol, *From EDI to Electronic Commerce: A Business Initiative*, McGraw-Hill, 1995.
- M. Johnson, “XML for the absolute beginner ”, *Javaworld*, April 1999, http://www.javaworld.com/javaworld/jw-04-1999/jw-04-xml.html.
- W3C, “XML Tutorial”, http://www.w3schools.com/xml/default.asp.
- M. Hall and L. Brown, “Introduction to XML”, 2001, http://www.corewebprogramming.com.

References

- J. Kurose and K. Ross, *Computer Networking: A Top-Down Approach Featuring the Internet*, Addison Wesley, 2001.
- Netsaint, http://www.netsaint.org.
- The SimpleWeb Tutorials, http://www.simpleweb.org/tutorials/.
- Electronic and telecommunication Institute, *Lessons about SNMP*, http://www.et.put.poznan.pl/snmp/main/mainmenu.html.
- Yoram Cohen, *SNMP – Simple Network Management Protocol*, http://www.rad.com/networks/1995/snmp/snmp.htm.