CIT 424
Computer System Security

02/16/15
Spring 2015

Digital Signature

Digital Signature Algorithms

- In some cases, secrecy isn’t required
- But authentication is
- The data must be guaranteed to be that which was originally sent
- Especially important for data that is long-lived

Encryption and Digital Signatures

- Digital signature methods are based on encryption
- The basic act of having performed encryption can be used as a signature
    - If only I know *K*, then $C=E(P,K)$ is a signature by me
    - But how to check it?

Signatures With Shared Key Encryption

- Requires a trusted third party
- Signer encrypts document with secret key shared with third party
- Receiver checks validity of signature by consulting with trusted third party
- Third party required so receiver can’t forge the signature

For Example,

K_S

When in
the Course
of human
events it
becomes
necessary
for one

Elas7pa
10’gw0mega
30’sswp.
1f43’-s 4
32.doas3
Dsp5.a#l
^o,a 02

K_S

When in
the Course
of human
events it
becomes
necessary
for one

Signatures With Public Key Cryptography

- Signer encrypts document with his private key
- Receiver checks validity by decrypting with signer's public key
- Only signer has the private key
  - So no trusted third party required
- But receiver must be certain that he has the right public key

For Example,

K_d

When in the Course of human events it becomes necessary for one

Elas7pa 10'gwomega 30'sswp. 1f43'-s 4 32.doas3 Dsp5.a#l ^o,a 02

When in the Course of human events it becomes necessary for one

K_e

Alice's public key

Problems With Simple Encryption Approach

- Computationally expensive
    - Especially with public key approach
- Document is encrypted
    - Must be decrypted for use
    - If in regular use, must store encrypted and decrypted versions

Digital Certificates

Digital Certificate Contents

- Name of holder
- Public key of holder
- Name of trusted third party (certificate authority)
- DIGITAL SIGNATURE OF CERTIFICATE AUTHORITY
- Data on which hash and public-key algorithms have been used
- Other business or personal information

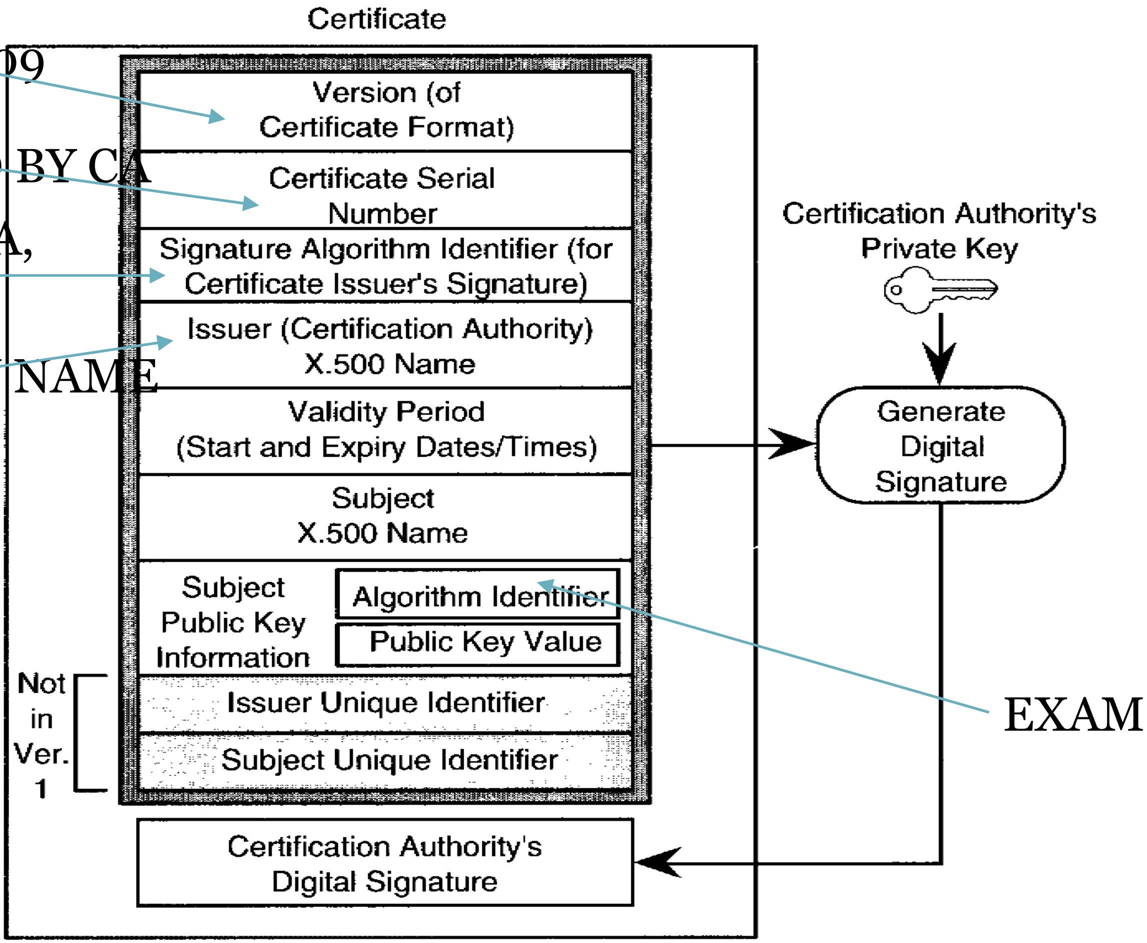
X.509 Version 2 Certificate

VERSION # OF X.509

UNIQUE # ASSIGNED BY CA

EXAMPLES: MD5RSA, sha1RSA

USUALLY A DOMAIN NAME



Certificate

Version (of Certificate Format)

Certificate Serial Number

Signature Algorithm Identifier (for Certificate Issuer's Signature)

Issuer (Certification Authority) X.500 Name

Validity Period (Start and Expiry Dates/Times)

Subject X.500 Name

Subject Public Key Information

Algorithm Identifier

Public Key Value

Issuer Unique Identifier

Subject Unique Identifier

Not in Ver. 1

Certification Authority's Digital Signature

Certification Authority's Private Key

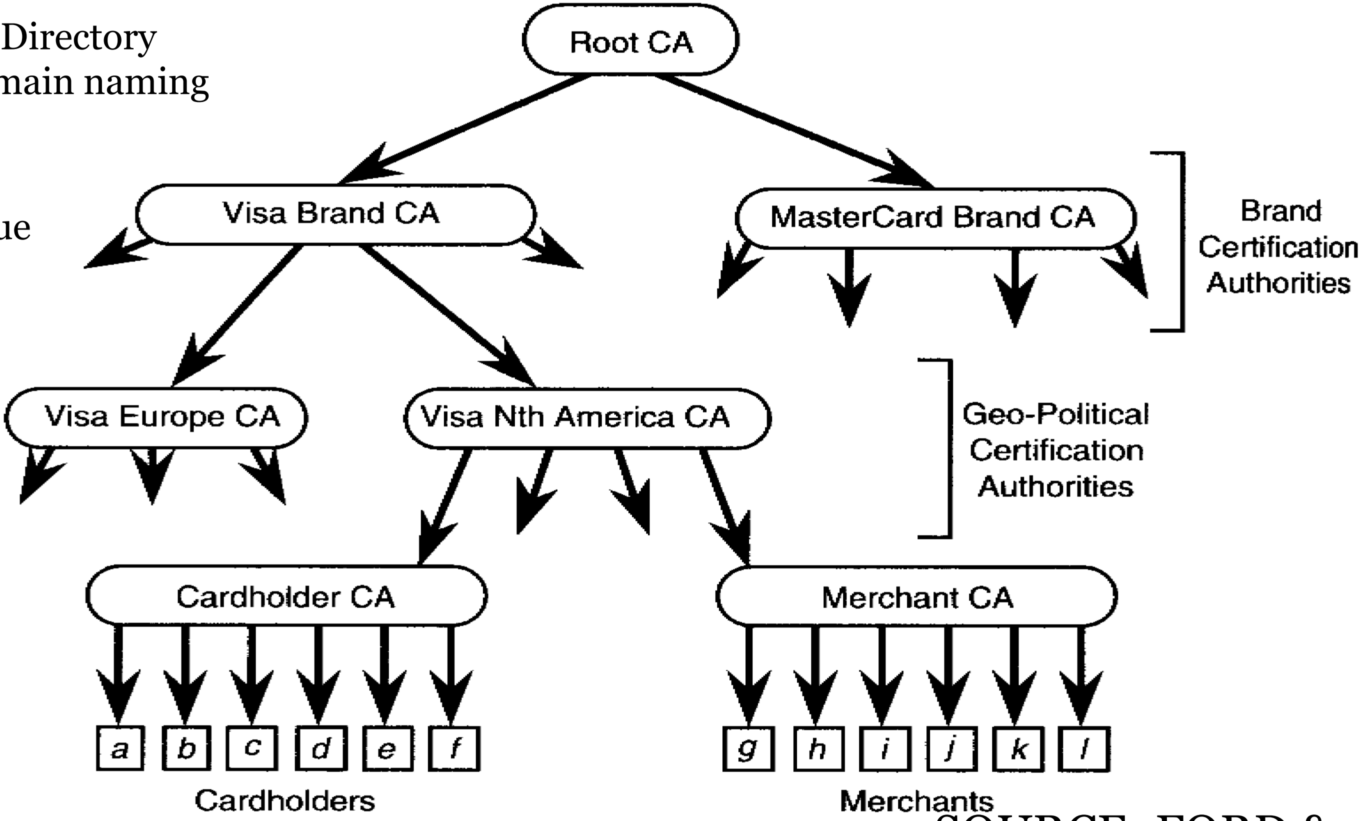
Generate Digital Signature

EXAMPLES: R

Certification Chains

X.500 Name Directory
similar to domain naming

Children have unique
relative names

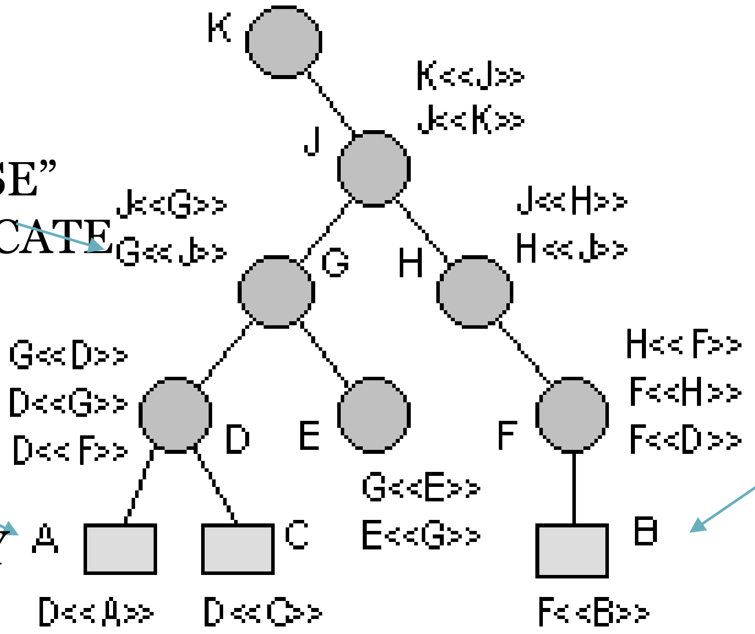


SOURCE: FORD &
BAUM,
*SECURE ELECTRONIC
COMMERCE*

Certification Paths

○ = CERTIFICATION AUTHORITY

□ = END USER



"REVERSE" CERTIFICATE

ALICE CERTIFICATE ISSUED BY D D<<A>>

ALICE WILL TRUST ANY PARTY TRUSTED BY D

BOB CERTIFICATE ISSUED BY F F<<B>>

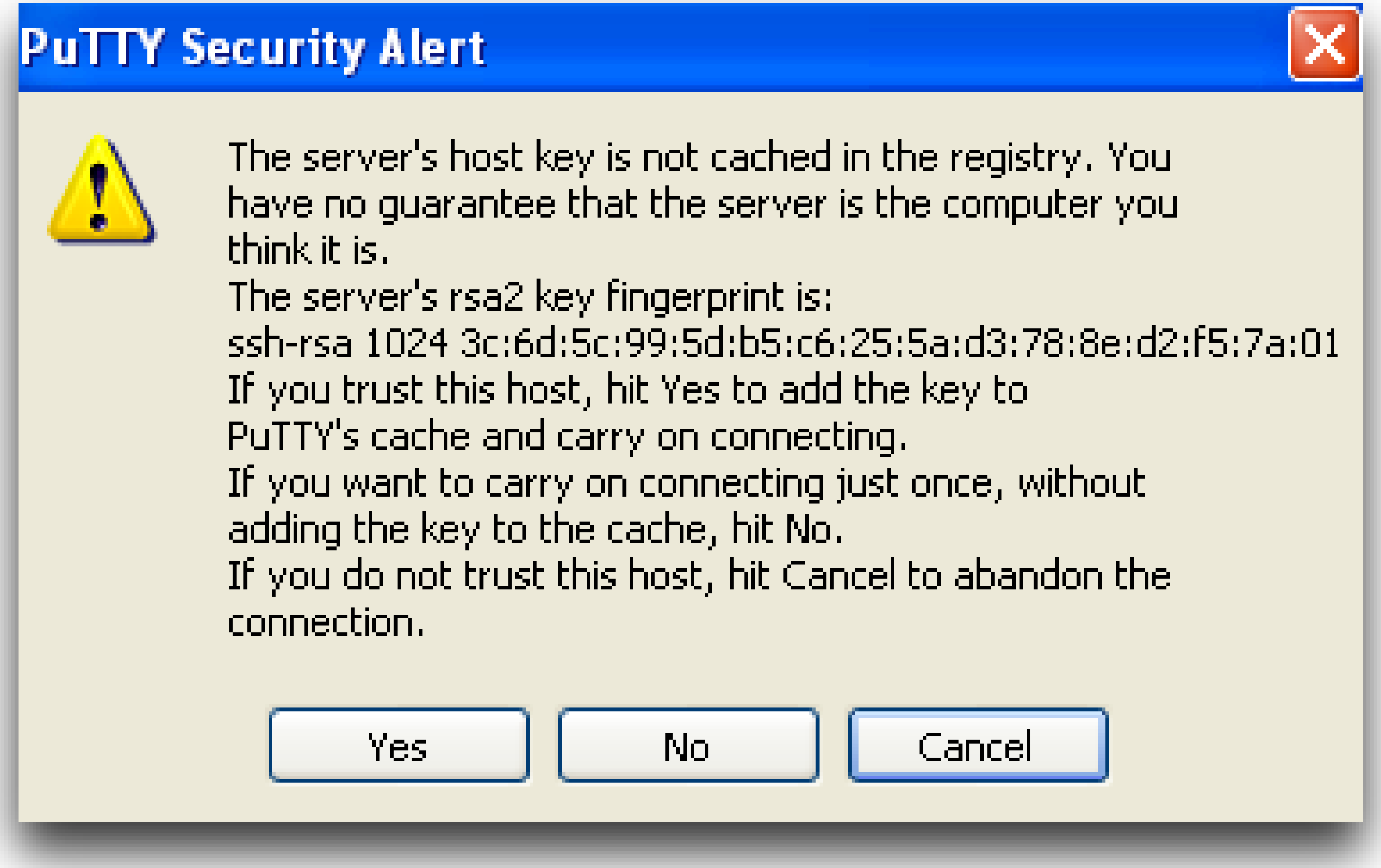
CERTIFICATION PATH:	D<<G>>,	G<<J>>,	J<<H>>,	H<<F>>,	F<<B>>

D TRUSTS G G TRUSTS J J TRUSTS H H TRUSTS F F TRUSTS B

ALICE NOW HAS (AND TRUSTS) BOB'S CERTIFICATE

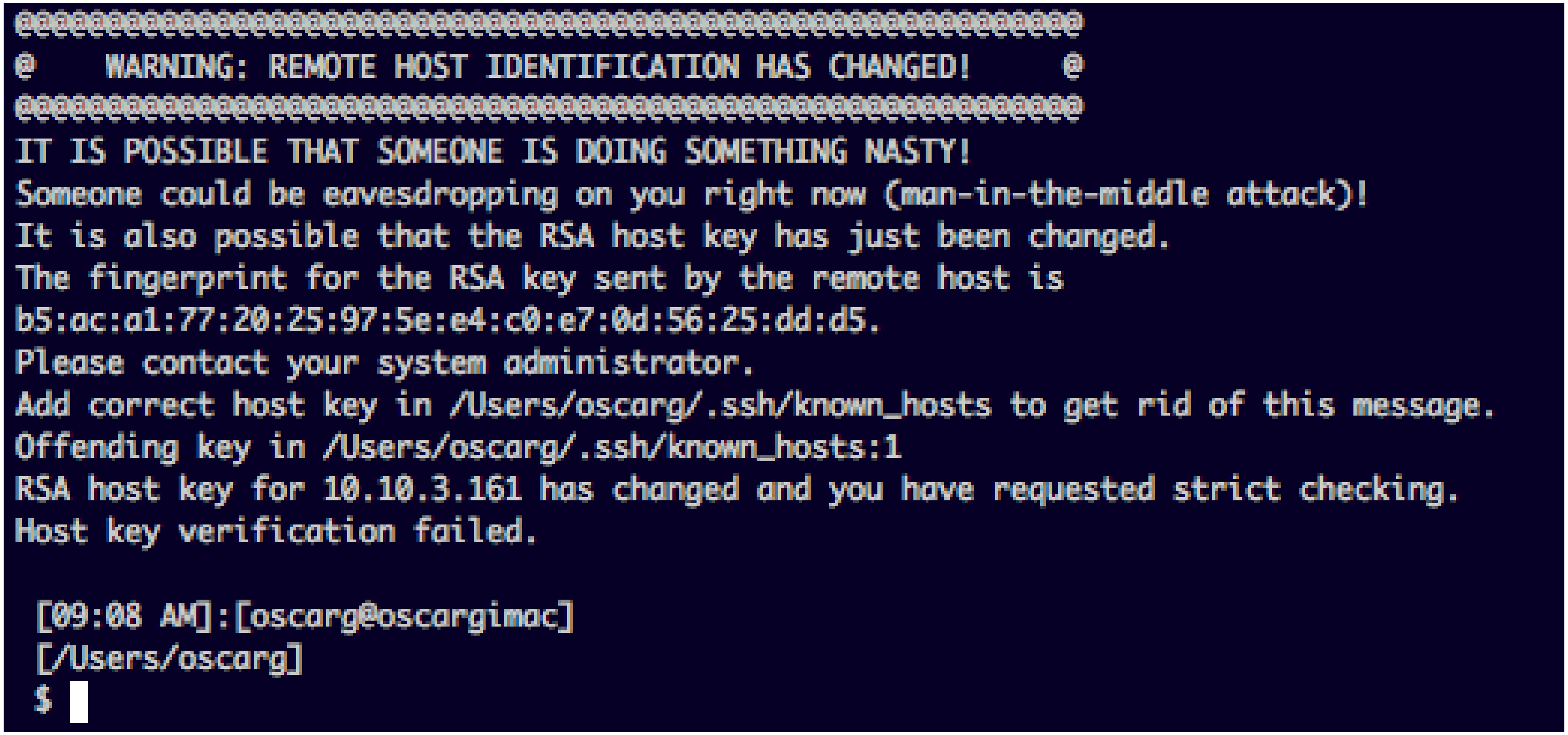
Leap of Faith

SSH: First Time Connection



The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.
The server's rsa2 key fingerprint is:
ssh-rsa 1024 3c:6d:5c:99:5d:b5:c6:25:5a:d3:78:8e:d2:f5:7a:01
If you trust this host, hit Yes to add the key to PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without adding the key to the cache, hit No.
If you do not trust this host, hit Cancel to abandon the connection.

SSH: When the Key is Changed



```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
b5:ac:a1:77:20:25:97:5e:e4:c0:e7:0d:56:25:dd:d5.
Please contact your system administrator.
Add correct host key in /Users/oscarg/.ssh/known_hosts to get rid of this message.
Offending key in /Users/oscarg/.ssh/known_hosts:1
RSA host key for 10.10.3.161 has changed and you have requested strict checking.
Host key verification failed.

 [09:08 AM]:[oscarg@oscargimac]
 [/Users/oscarg]
 $ 
```