Chapter 13

by

David G. Messerschmitt

Some objectives

• High availability
  – Expanding expectations, approaching 24x7
  – Redundancy/replication, security, human factors
• Protect confidential information
• Limit services to legitimate users or customers
• Conduct secure commercial transactions

Availability costs!

• On-line upgrade and maintenance
• More application testing, more rapid bug reports and fixes
• Equipment or application redundancy
• Data replication
• Operational vigilance

Question

• What availability would you like to see in:
  – Consumer stock trading system?
  – Currency trading system?
  – Train control system?
  – Bank ATM?
  – Social application like email?
  – Telephone system?
Different security environments

- Intranet and extranet
  - All users may be trusted
- Organization-to-organization
  - Users in other organizations are less trusted, have less access
- Citizenry
  - Determined adversaries must be assumed

Access control

- First line of defense is to limit information and services to authorized users
- Requires:
  - Authorization policies
  - Databases with authorizations
  - Confidentiality of information and communication
  - Authentication of users who do gain access

Non-repudiation

- The second line of defense is to maintain a provable audit of commitments
  - Requires non-repudiation: neither sender nor recipient can deny message
  - Non-repudiation requires message integrity

Core technology

- Encryption
  - Depends on the existence of hard (not impossible) problems that are thought to be uncomputable by the fastest computers in reasonable time
  - “Size” of problem can be adjusted to future and anticipated computing technology
  - Symmetric and asymmetric versions

Virus

- Normal executable
- Infected executable
- Alice writes message on paper in permanent ink
- Alice adds her signature
- Alice seals message in envelope
- Bob verifies Alice’s signature
- Post office physical security
- Alice requests return acknowledgement from Bob
- Only Bob breaks seal and opens envelope
- Alice adds her signature
- Post office physical security
Encryption

- Transform “plaintext” data to “ciphertext” data in a way that
  - plaintext cannot be recovered without knowledge of a key
  - at least not without extraordinary computing resources

Confidentiality

Bob must possess a secret not available to anyone else

Confidentiality (con’t)

Bob must possess a secret not available to anyone else
Confidentiality (con’t)

Alice (sender)  Bob (recipient)

Alice must be able to transform the message so that only the person possessing that secret can read it.

Bob must possess a secret not available to anyone else.

Authentication

Goal:

• Before Bob can trust a message received from Alice, he needs to verify that Alice is who she claims she is.
• Alice may want to verify Bob’s identity before sending him a message.

Authentication (con’t)

Alice (sender)  Bob (recipient)

Alice must possess a secret not available to anyone else (alternatively, physical characteristics like a finger print might be used).

Bob must be able to verify that Alice possesses that secret without Alice revealing it on the network (and possibly not to Bob).

Authentication (con’t)

Alice (sender)  Bob (recipient)

Alice must possess a secret not available to anyone else (alternatively, physical characteristics might be used).

Bob must be able to verify that Alice possesses that secret without Alice revealing it on the network (and possibly not to Bob).

Challenge-response protocol

Alice (being authenticated)

Bob

Public key

APK

Secret key

ASK

Decryption

Encryption

k

l

k+1

Compare

Response

Encryption

Decryption

Challenge

Response

Public key

APK

Encryption

Decryption

k
Question

• How does Bob obtain Alice’s public key?
• How does Bob authenticate that public key?
• Answer: Key must come from a trusted authority

Authentication (con’t)

Alice (sender)  
Bob (recipient)  

Alice must possess a secret not available to anyone else (alternatively, physical characteristics might be used)

Digital certificate

Bob also must have confirmation from a trusted authority of Alice’s public key

Non-repudiation

Alice (sender)  
Bob (recipient)  

Alice can transform the message using a secret only she possesses

Digital signature

(Alice) sender  
Bob (recipient)  

Secret key ASK  
Public key APK

Plaintext  
Signature  
Compare

Non-repudiation

Alice (sender)  
Bob (recipient)  

Alice must sign the message using a secret not revealed to anybody else

Digital certificate

Bob must be able to verify the signature using public information confirmed by a trusted authority

Summary

• A message can be sent from Alice to Bob, such that:
  – It is confidential
  – Alice’s identity is authenticated
  – Provably the message was not modified after Alice generated it, and she cannot repudiate it
• All this requires a system for distribution and certification of secrets
Distribution of secrets

• Users choose their own secrets and inform sites (password)
• In a closed administrative environment, secrets can be distributed by administrative fiat
  – Authentication servers avoid the “n^2 secret problem”
• For the citizenry, infrastructure required

Chain of trust

Certificate authority
\[\text{Bank’s certificate issued by CA} \]
\[\text{Authority’s known public key} \]  
\[\text{Verify signature}\]

Bank’s public key

Merchant’s certificate issued by bank

Merchant’s public key

Verify signature

Consumer electronic commerce

Customer (client)

Seller (server)

Trusting CA public key, client can obtain authenticated public key of a seller

Client can generate a random, secret “session key” and send confidentially to server

Client can authenticate server using challenge response protocol

Client and server can communicate confidentially
Certificate infrastructure

- Certificate authorities
- Individual and corporate certificates
- Benefits:
  - Authentication of sellers and buyers
    - Avoid sales to minors etc.
  - Non-repudiation of transactions

Privacy concerns

- On-line transactions can be tracked
- Traditional opposition to “identity card” for this reason
- Safeguards are possible
  - Example: Secure Electronic Transactions (SET)

Encryption obscures data representation

<table>
<thead>
<tr>
<th>Information</th>
<th>Data</th>
<th>Cipherertext</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information</td>
<td>Data</td>
<td>Information</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Block substitution table</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plaintext (n bits)</td>
</tr>
<tr>
<td>---------------------</td>
</tr>
<tr>
<td>0000000000000000</td>
</tr>
<tr>
<td>0000000000000001</td>
</tr>
<tr>
<td>000000000000010</td>
</tr>
<tr>
<td>...</td>
</tr>
<tr>
<td>1111111111111111</td>
</tr>
</tbody>
</table>

Understanding Networked Applications: A First Course
Block substitution table

<table>
<thead>
<tr>
<th>Plaintext (n bits)</th>
<th>Ciphertext (n bits)</th>
</tr>
</thead>
</table>
| For each of the $2^n$ possible plaintext blocks, the substitute ciphertext block of n bits is used. The table has $n \cdot 2^n$ bits total.

Confidentiality based on the block substitution cipher

- This is a symmetric encryption/decryption algorithm.
- The key is the table, which has $n \cdot 2^n$ bits.

Practicality

- For small block size $n$, statistical techniques can easily infer the table.
- For large block size $n$, the table is too large to be practical.
  - e.g. $n=64$, $64 \cdot 2^{64} = 10^{21}$, far greater than the total storage in a computer.

Practicality (con’t)

- Keys need not be as large for an exhaustive key trial attack.
  - e.g. $10^9$ trials/sec, 10 years = $3 \times 10^8$ sec
  - $3 \times 10^{17}$ trials in 10 years
  - $2^{59} = 6 \times 10^{17}$
  - 59 bit key will do it!
- Conclusion: need an encryption algorithm!
  - Key with 64 or 128 bits may be enough.

RSA asymmetric algorithm

- $C = P^s \mod n$
- $P = C^t \mod n$
- $t$ cannot be computed from $(n,s)$ in reasonable time.
Notice the asymmetry

The two keys can be applied in either order, and we still return to where we started.

Kerberos

Authentication server

B

\[ E_{skx}[k, ABSK, ID_A] \]
\[ E_{skd}[k, ID_A] \]
\[ E_{skd}[k+1] \]

A

\[ E_{skd}[k, ID_A] \]
\[ E_{skd}[k, ABSK, ID_B] \]
\[ ID_A, ID_B \]

49

50