PUBLIC KEY INFRASTRUCTURE

Presented By: Mamtha

Alice

Private Key

Public Key
1. PUBLIC ANNOUNCEMENT

- The owner broadcasts her public key. For example, by publishing it in web-site.

But is that a good idea?

- Not a standardized idea, no systematic way to find/verify the public key when needed
- Some form of trust is required. For previous example, the website has to be trusted

https://www.schneier.com/blog/about/contact.html
2. PUBLICLY AVAILABLE DIRECTORY

• If Bob wants to find the public key associated with the name alice@yahoo.com.sg, he can search the public directory by querying a server.

<table>
<thead>
<tr>
<th>Name</th>
<th>Public Key</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:alice@yahoo.com.sg">alice@yahoo.com.sg</a></td>
<td>x1s34adf39</td>
</tr>
<tr>
<td><a href="mailto:alice@gmail.com">alice@gmail.com</a></td>
<td>asd3123411</td>
</tr>
<tr>
<td><a href="mailto:john@nus.edu">john@nus.edu</a></td>
<td>2s3dasdf233</td>
</tr>
<tr>
<td><a href="mailto:jane@msn.com">jane@msn.com</a></td>
<td>a323fasdfas</td>
</tr>
</tbody>
</table>

Alice: Email is "signed" using my private key.

Bob: What is the public key of alice@yahoo.com.sg?

The public key of alice@yahoo.com.sg is x1s34adf39
2. PUBLICLY AVAILABLE DIRECTORY

But is this a good idea?

Public Key Directory

<table>
<thead>
<tr>
<th>Name</th>
<th>Public Key</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="mailto:alice@yahoo.com.sg">alice@yahoo.com.sg</a></td>
<td>x1s34adf39</td>
</tr>
<tr>
<td><a href="mailto:alice@gmail.com">alice@gmail.com</a></td>
<td>asd3123411</td>
</tr>
<tr>
<td><a href="mailto:john@nus.edu">john@nus.edu</a></td>
<td>2s3dasdf233</td>
</tr>
<tr>
<td><a href="mailto:jane@msn.com">jane@msn.com</a></td>
<td>a323fasdfas</td>
</tr>
</tbody>
</table>

3. PUBLIC KEY INFRASTRUCTURE

- Certificate Authority (CA)
- Registration authority (RA)
- Central directory
- Certificate management system
- Certificate policy
CERTIFICATE

Certificate
• Public Key
• Information about the identity of its owner (ie. subject)
• Digital signature of an entity that has verified the certificate's contents (ie. CA)
• Time window that this certificate is valid (eg. For temporary certificate and single sign-on)
• Purpose of the public key

CA: The public key of alice@yahoo.com.sg is x1s34adf39 and it is valid until 1 Sep 2021

Name          Public Key
alice@yahoo.com.sg  x1s34adf39
alice@gmail.com    asd3123411
john@nus.edu       2s3dasdf233
jane@msn.com       a323fasdfas

Alice: Email is "signed" using my private key. Also, my signature
Bob: What is the public key of alice@yahoo.com.sg?
HTTPS://INTERNET-BANKING.DBS.COM.SG/IB/WELCOME

Certificate Viewer: "internet-banking.dbs.com.sg"

General Details

This certificate has been verified for the following uses:
SSL Client Certificate
SSL Server Certificate

Issued To

Name: Internet-banking.dbs.com.sg
Organization: DBS Bank Ltd
Organizational Unit: Citrus Technology And Operations
Serial Number: 6862/594707:38:A7:A4E8E691/05A39068F8

Issued By

Name: Symantec Class 3 Extended Validation SHA256 SSL CA
Organization: Symantec Corporation
Organizational Unit: Symantec Trust Network

Period of Validity

Begin: Thursday, 1 December 2016
End: Friday, 12 January 2018

Fingerprints


From: alice@yahoo.com.sg
Subject: Hello Bob
Meeting 3pm at the usual place today.
signature: xsdewsdesd

CERTIFICATE CHAIN

name: CA#1
public key: x3141342
Valid until: 1 Sep 2020
note: CA#1 can issue certificate
signature of the Root CA

Alice Email

name: alice@yahoo.com.sg
public key: x1s34adfs39
Valid until: 1 Sep 2019
signature of the CA#1

CA#1 Certificate

Alice Certificate
HIERARCHY OF TRUST

RESPONSIBILITY OF CA

• Has to make sure that the information is indeed correct. Is it really www.nus.edu.sg? - registration authority (RA)
ATTACKS ON PKI

- Some browsers ignore substrings in the “name” field after the null characters when displaying it in the address bar, but include them when verifying the certificate.
- (a) Name appeared in the certificate which is used in verifying the certificate:
  “www.comp.nus.edu.sg\0hacker.com”
- (b) The browser displays it as
  “www.comp.nus.edu.sg”

ABUSE BY CA

- There are so many CA’s. One of them could be malicious. A rogue CA can forge any certificate.

LENOVO’S SUPERFISH SCANDAL

• Self-signed root certificate
• Vs Web Of Trust

http://www.slate.com/articles/technology/bitwise/2015/02/lenovo_superfish_scandal_why_it_s_one_of_the_worst_consumer_computing_screw.html

TYPO SQUATTING

ivle.nvs.edu.sg
vs
ivle.nus.edu.sg
TYPOSQUATTING

ivle.nvs.edu.sg vs ivle.nus.edu.sg