Challenge A: remote encrypted communication between two familiar people

Part A(i): Key Exchange, Encryption and Decryption Challenge

Instructions

Each pair represents a Bank and a Customer who want to communicate safely over the internet.

Your task is to design a secure procedure for sending a link to the Bank's log-in page to the Customer.

You are given the EasyRSA public key encryption applets demonstrated previously.

The process will go like this:

1) The Customer may visit the Bank to devise a plan for at most 3 minutes
2) Customer and Bank teams separate to remote terminals and act out the plan.
3) Bank receives a link of the form `http://www.bit.ly/abcdefg` `from the instructor`
4) The bank will then encrypt a message with the appropriate link and send it to the instructor
5) Instructor will relay this message to the Customer (simulating routed traffic of the internet)
6) The customer will then decrypt the message and access the provided link.

You are provided all the applets for encryption and key generation shown in the demo, as well as pens and paper. Additionally, the Bank's message is also provided via email at the start. Make sure to insert the link provided by the instructor after the planning meeting is over.

You are encouraged to sketch out your process as a flow chart. Each time you hit ENTER or click a button on an applet should probably be documented.

The goal of this exercise is for the Customer to successfully decrypt the log-in prompt message and access the link pointing to the YES! page. Please raise your hand when you've done so. You can have at most 2 additional meetings in case your original plan does not succeed.

Message Text

```
Dear Valued Customer,

Thanks for opening an account at Secure Bank and Trust.

Please log-in to your account online: http://www.bit.ly/abcdefg

Thanks! - Your banking team
```

Flowchart Work Space

Part A(ii): Encryption and Decryption with Intruder Challenge

Instructions

Your seamless communication line is about to be threatened. It turns out that because a public key and private key are mathematically related, given enough time I can compute the private key that corresponds to a given public key. I can do this using this KeyHacker applet, which you all have access to as part of the EasyRSA programs.

Your challenge is to devise a communication process that will allow you to pass messages from Bank to Customer successfully at least two minutes after the key exchange, knowing there is an intruder in the middle who can hack into your communication and provide a fake link.

The process will go like this:

1) The Customer may visit the Bank to devise a plan for at most 3 minutes
2) Customer and Bank separate to remote terminals and act out the plan.
3) Bank receives a link of the form `http://www.bit.ly/abcdefg` from the instructor.
4) The bank will then encrypt the message with the appropriate link and send it to the instructor
5) Instructor will attempt to hack the provided message for two minutes. If successful, he will insert a false link that looks similar in form to the Bank's.
6) After two minutes he will pass on to the Customer either the hacked message or the original at his discretion.
7) The customer will then determine whether she trusts the message. If she does, she will decrypt the message and access the provided link.

Note that as the All-Knowing Attacker, I am free to wander around and eavesdrop on any conversation to aid my malicious plans. So be careful. I suggest you pay close attention to your key generation process. Good luck.

Message Text

```
Dear Valued Customer,

Thanks for opening an account at Secure Bank and Trust.

Please log-in to your account online: http://www.bit.ly/abcdefg

Thanks! - Your banking team
```

Workspace

Part A(iii): Remote key exchange challenge

Set-up

Each customer-bank pair should meet to agree on a revised scheme using the lessons about key vulnerability discussed just before this. At most 3 minutes are available.

Next, after Bank-Customer separation all Customers need to rotate one station to the over. Customers have shifted accounts for financial reasons and now need to log-in to their new bank. However, they do not have time to meet in person and must figure out a way to do key exchange without talking to the Banks in person.

Instructions

Now that you've mastered understanding of public key cryptography, you have a new challenge: successful communication without a face-to-face meeting Bank and Customer meeting to exchange keys.

The process will go like this:

1) Customer and Bank teams separate to remote terminals.
2) Each bank receives a link of the form `http://www.bit.ly/abcdefg` from the instructor.
3) For a 3 minute planning period, customer teams can talk to each other, as can banks. However, no intermingling is allowed.
4) The bank will then encrypt the message with the appropriate link and send it to the instructor
5) Instructor will relay the message to the appropriate customer
6) The customer will then determine whether she trusts the message. If she does, she will decrypt the message and access the provided link.

Message Text

```
Dear Valued Customer,

Thanks for opening an account at Secure Bank and Trust.

Please log-in to your account online: http://www.bit.ly/abcdefg

Thanks! - Your banking team
```

Workspace

Day Two: Warm Up

"What is a Digital Certificate?"

Part A(i) Case Study in Identity Documentation

Instructions

Customers of Secure Bank and Trust are allowed to open accounts via mail. Your job is to examine the identification documents provided by prospective customers and decide whether to stamp the documents as trustworthy or not.

To assist your efforts, a list of questions have been provided that you should probably think through.

A) Application #1

1. Who issued this document? How do you know?

2. Do you trust this issuer? Why?

3. What assumptions do you make about the issuer if you trust the information documented here?

4. What assumptions do you make about the document's owner if you trust the information here?

5. If you were uncertain about trusting this document, how could you confirm its validity?

B) Application #2

1. Who issued this document? How do you know?

2. Do you trust this issuer? Why?

3. What assumptions do you make about the issuer if you trust the information documented here?

4. What assumptions do you make about the document's owner if you trust the information here?

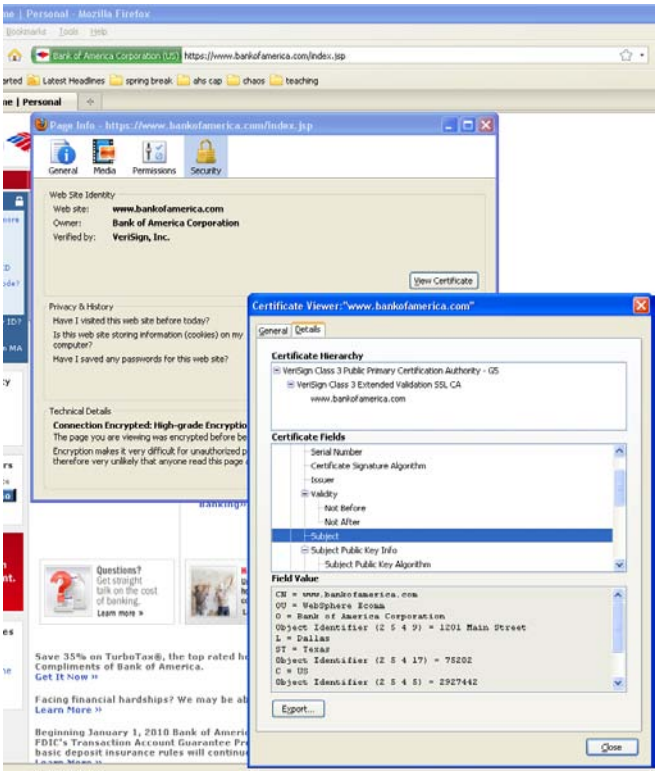
5. If you were uncertain about trusting this document, how could you confirm its validity? Think of at least three different ways.

6. Why does this document expire? Think of at least two potential reasons.

Part A(ii) : Practical Digital Certificates in Firefox

Instructions

In Firefox, navigate to your favorite banking website, or choose one of www.bankofamerica.com or www.wellsfargo.com. Click on the green bar in the URL entry line to access its digital certificate, which is shown below.



Using the information found in the digital certificate viewer, try to answer the following questions in pairs. It may be the case that much of the available information doesn't make much sense, but try your best to use the concepts and exercises we've completed so far to untangle what's going on.

Questions (not Evaluated)

1) Who issued this certificate? How do you know?

2) Give several reasons you can trust (or not trust) this company to provide certificates?

3) Who is the "subject" of the certificate? Can you find the subject's public key?

4) Why do you think a Not Valid After date is provided?

5) What assumptions do you make about the issuing organization if you trust this document?

6) What assumptions do you make about the website owner if you trust this document?

7) What is the "signature" section of the certificate for? Who signs this certificate?

8) How is this documentation different than a driver's license or passport? Think of at least 3 different ways.

Day Two Challenge:

Encrypted communication between unfamiliar parties

Prerequisite

Successful completion of the Day Two Warm-up exercise: "What is a digital certificate?"

Part B(i) Digital certificate mediated communication

Set-up

Bank-customer teams of students.

Instructions

Bankers and Customers, your new challenge is to design a process that will allow the Customers to trust and use communications from the Bank without ever knowing the Bank's public key. I, the Instructor, will serve as the TTP. My public key is _____ <insert key there>. I will provide any encryption services you might need, just ask.

Each Bank has a certificate template in their email inbox. However, several items are missing from this template. Your task is to first meet with your customers to agree on an overall certificate format and encryption/decryption protocol. You should plan out exactly what the Bank needs to encrypt and what the instructor needs to encrypt.

Next, you will separate to respective stations. Banks will generate a fresh key pair, add it to the appropriate spot on the template, then pass the template to the instructor, who will encrypt the message and pass it back to the bank. Finally, the bank will send along the appropriate message to the customer, who must unlock it using only knowledge of the TTP public key and the certificate

Process

1) Customer and Bank plan together for 5 minutes about certificate format and protocol
2) Customer and Bank teams separate to remote terminals.
3) Each bank generates a fresh key pair, inserts it into certificate, and sends to TTP for certification
4) TTP sends back a "signed" copy of the certificate to the bank
5) Instructor sends bank a link of the form `http://www.bit.ly/abcdefg`
6) The bank will then encrypt the message with the appropriate link and send it to the instructor
7) Instructor will relay the message to the appropriate customer
8) The customer will then determine whether she trusts the message. If she does, she will decrypt the message and access the provided link.

Certificate Template

```
------------  PLAIN TEXT IDENTITY INFORMATION ------------------
======= OWNER INFO ==============================================
Name:  Bank 01
Public Key:  < insert here >


======= TRUSTED AUTHORITY INFO ==================================
Name: Hughes Security Enterprises, Inc.


------------   ENCRYPTED SIGNATURE  -----------------------------
<< insert here >>
```

Workspace

Part B(ii) Certified Communication with Intruders

Set-up

Combine pairs into groups of six. Two Bankers, two Customers, and two Attackers.

Banker/Customer Instructions

1) Meet together for 5 minutes to plan protocol, revise if necessary from previous challenge
2) Banks and Customers separate
3) Customer obtains instructor public key.
4) Banks generate their own brand new public/private key pair.
5) Bank send certificate form with provided public key to Instructor
6) Instructor sends certificate back to Bank with appropriate signatures
7) Instructor sends bank a link of the form `http://www.bit.ly/abcdefg`
8) The bank will then encrypt a message with the appropriate link and send it to the instructor
9) Instructor will then pass on this message to the Attackers who have 3 minutes to hack it
10) After 3 minutes instructor receives attacker message
11) Instructor then passes one or both of attacker and banker messages to Customer
12) The customer will then determine whether she trusts the message. If she does, she will decrypt the message and access the provided link.

Attacker Instructions

1) Meet together for 5 minutes
    a. Actively snoop around …
        i. EVERYTHING IS FAIR GAME FOR YOU TO LOOK AT/HEAR
    b. Devise plan of attack… how will you generate a certificate that a customer might accidentally trust?
2) While banks are generating certificates…
    a. Keep snooping around, devising plan
    b. Maybe use KeyHacker at this point
    c. Maybe generate own public key and submit request for certificate from bank
3) Instructor sends attacker a link of the form `http://www.bit.ly/abcdxyz`
4) After bank's submit message, instructor will pass on a copy to Attacker team
5) Attackers have 3 minutes to unlock this message and replace it with their own
6) After 3 minutes attackers send message to instructor
7) Instructor then passes one or both of attacker and banker messages to Customer
8) The customer will then determine whether she trusts the message. If she does, she will decrypt the message and access the provided link.

Repeat this exercise as necessary.

Work Space

Challenge C: Designing certificate issuer policy: creation and revocation

Instructions

"You've identified several crucial design features for Digital Certificate-based exchanges. Now, you'll all act as managers of a Certificate Issuer to design policy for how you'll be a trusted third party.

You have 10 minutes as a group. Come up with answers to these questions:

1) *How will you determine what entities you issue certificates to? What is the verification process to be sure you know who these entities are? Will this happen online?*

2) *What will your certificates look like? What fields and values will be required?*

3) *How will you publish your public keys? What happens after the expiration date?*

4) *What policies will you require subjects to adhere to? How should they create/store private keys? Who should have access to them?*

5) *What happens when a subject does not adhere to these policies? Will you revoke a certificate? How will you let customers know?*