Day One Warm-up:

Why do we need internet security?

Part A: Motivation

Set-up

Arrange to have a projector or large screen. Students gathered together in big group.

Instructions

Display the following email message to students

---------- Forwarded message ----------
From: **Wells Fargo Customer Service** <customerservice@wellsfargo.com>
Date: Thu, Feb 25, 2010 at 4:43 PM
Subject: Should I trust this message?
To: master@michaelchughes.com

Dear Wells Fargo customer,

We have noticed that you experienced trouble logging into Wells Fargo Online Banking. After three unsuccessful attempts to access your account, your Wells Fargo Online Profile has been locked. This has been done to secure your accounts and to protect your private information. Wells Fargo is committed to making sure that your online transactions are secure.

To unlock your account, and verify your identity please sign in at wellsfargo.com

Sincerely,
Wells Fargo
Online Customer Service

Explain that you are an active WellsFargo customer and you're a little worried. Ask "*can I trust this message?*"

Elicit ideas about ways you could confirm the message is valid. Try to come up with at least three as a class. For example, call Wells Fargo and ask, google the message, etc.

Ask what could happen if you click the provided link. Make sure answers are justified.

Click the link and explain that the page looks like this

Ask “this looks okay, right? can I log in?”

Elicit ideas about the risks/dangers of logging into this site.

Try to come up with alternatives to make sure this site is valid (e.g. type in the address yourself, google it, etc.)

Explain that this email is a clever forgery: the link was to vvellsfargo.com (note the double “v”)

Explain that an owner of vvellsfargo.com could easily fake the wellsfargo homepage and steal passwords. Make sure students understand consequences.

*At the end of **Motivation,** instructor should*

Emphasize lesson goals of acquiring security expert ways of thinking and practical knowledge

Explain that this requires thinking in creative and unconventional ways

Encourage kids to ask questions throughout the lesson

Day One Background

Part A: The Internet delivery system and its security risks

Set-Up

Need projector or large screen. Keep students in big group.

Instructions

Show short youtube video to expose inner workings of the internet.

http://www.youtube.com/watch?v=qv0XCaUkfNk

Engage class in discussion with questions like the following,

1) How does a message get from sender to receiver? Does anyone else have access to it?

2) Who owns a website like www.wellsfargo.com? How can we be sure?

3) What could happen if someone could eavesdrop on your internet communications?

4) What could happen if someone could intercept and replace your internet communications?

5) What major security risks exist in using the internet?

*At the end of **Part A**, instructor should*

*Explain and define the goals of **privacy** and **authentication***

Emphasize that both concerns are at play every time you use the internet

Emphasize other goals of trustworthy communication NOT covered in this lesson… e.g. guaranteeing receiver gets message, denial of service, etc.

Part B: Easy demonstration of encryption

Set-up

Keep large screen/projector and class in big group. Run the EasyRSA applet suite on the projector and demonstrate the basics of public key cryptography.

Instructions

Explain to students that encryption is the process of using mathematical functions to produce unrecognizable garbage from plain text. Emphasize that it is *deterministic* (e.g. will always produce the same output from the same input).

Demonstrate the Encryption Applet with a sample message and preloaded key.

Explain decryption is a twin mathematical process that allows a user to transform the unrecognizable garbage back into the original text message. This is also deterministic.

Demonstrate the Decryption Applet with a sample message and preloaded key.

Define a **key** as a special input to the encryption/decryption process that governs how the message is jumbled up. Explain that encryption and decryption procedures must have related keys in order to successfully unlock a coded message.

Explain that the cryptosystem behind online banking is called a public key system. This means that two keys are involved in the process: one for encryption and one for decryption.

The encrypting key is called the **private key**. The decrypting key is called the **public key**.

Explain that these keys are mathematically related.

Demonstrate the Key Generation Applet.

Show how these keys can then be used to encrypt and decrypt a message.

Show that a small change to either the key or the message will render the decryption process garbage.

Answer student questions.

*At the end of **Part B**, instructor should*

*Recap **public key** and **private key** definitions, explain these are alive behind any secure site they visit.*

Explain that students will use these applets to progressively build up a trustworthy communication system similar to what is behind the internet.

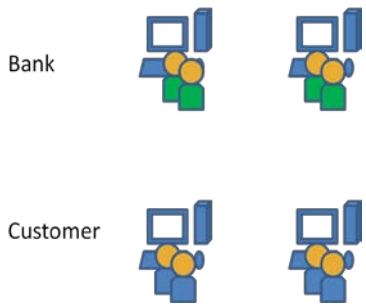
Challenge A:

Encrypted communication between two familiar parties

Pre-requisite

Students should complete the Demo-based Introduction to Public Key Cryptography lesson

Set-up



Divide students into pairs that represent either Banks or Customers, as shown to the right

Assign each to a pair of corresponding computer terminals, each with operational cryptographic applets and email clients for exchanging information. Each pair receives a stack of post-it notes and a few pens.

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

Explain the following task narrative.

"Each pair represents either a Bank and a Customer who want to communicate safely over the internet. Specifically, each collaborative Bank/Customer team will design a procedure for sending a link to the Bank's log-in page to the Customer using public key encryption. The Customer may visit the Bank to devise a plan for at most 3 minutes, then must separate to remote terminals and act out the plan. 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 log-in message and link is also provided.

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. Please raise your hand when you've done so. You have at most 2 additional meetings in case your original plan does not succeed.

*At the end of **Part A(i)**, instructor should*

Verify the exchange of *public keys* in each pair's face-to-face meeting.

Verify a successful encryption-decryption sequence for each pair.

Recap as a big group

- define **key exchange** as process where individuals share public keys
- recap why this must happen before encrypted communication

Challenge B:

Intruder-proof Encrypted Communication

Set-up

Same as A(i) above.

Instructions

Explain the following task narrative.

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.

As the process unfolds, instructor should wander around and make sure teams are on track / not stuck. Encourage teams that "get it" to push the limit on the expected time before the key is "hacked", e.g. hint at multiple levels of encryption. Additionally, try to acquire a key from each group so you can start hacking it.

*At the end of **Part A(i)**, instructor should*

Verify each pair discovered that longer keys are more difficult to break.

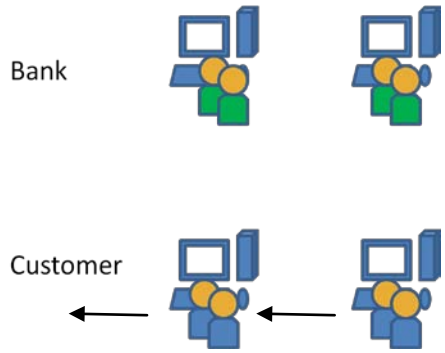
Verify a successful encryption-decryption sequence for each pair.

For entire class:

- recap why awareness of key breakability is important
- discuss additional ways to foil attacker
    - hide public keys from view
    - use multiple layers of encryption e.g. encrypt(encrypt(x))

Part A(iii)

Set-up



Arrange pairs as above in A(ii), shown to the left.

Ask each Bank-Customer group to meet for 3 minutes and generate a fresh encryption protocol based on the lessons learned about intruders.

Then have groups separate into respective pairs. After returning to terminals, instruct customers to shift one station over (arrows).

Instructions

Customers, you have become unsatisfied with your accounts financial reasons and now need to log-in to a new bank. However, you do not have time to meet in person and must figure out a way to do key exchange without talking to the Banks directly.

Can you figure out a way as a Customer to decode the Bank's log-in instructions without knowing its public key at first? HINT: look around you. Just because you can't talk to the Bank doesn't mean you can't talk at all…"

Allow 5 minutes for Customer-Customer and Bank-Bank conversation.

Then ring the bell and have banks email message through instructor terminal to the customer.

*At the end of **Part B (i),** instructor should*

Verify that Customers exchanged public keys used in previous interactions from fellow customers.

Verify a successful encryption-decryption sequence for each pair.

For entire class:

- motivate that most online transactions cannot be prefaced by face-to-face key exchange, so another mechanism is necessary
- define **trusted third party** as crucial way to verify entity's key
- ask why customers were able to trust the customers next to them

Day Two Warm-up: What is a Digital Certificate?

Pre-requisite

Successful completion of Challenge A

Part A(i): Case Study on Identity Documentation

Set-up

Students work in pairs on this exercise. Seat them at desks with writing utensils.

Instructions

During Day One, we discovered that encrypted communication can be difficult to establish when a key exchange must occur without a trustworthy face-to-face meeting. One way to solve this problem is to have a trusted-third party provide documentation about the bank's digital identity. If you trust the party, you can use this documentation to figure out who owns a website and what public key the owner uses.

The documentation is called a Digital Certificate. It functions in many ways like a digital driver's license or passport. A driver's license is a state-issued document that attests that the named individual belongs to a particular photograph and a particular address. Similarly, a digital certificate is documentation that the named company/individual owns a particular web address and has a particular public key.

In order to understand the assumptions and reasoning for trusting a digital certificate, as a pair complete a case study in which you will both be employees of a multi-national bank Secure Bank and Trust. Your job is to examine the identity documentation provided by prospective customers and determine if it is sufficient to open an account.

*At the end of **Part A (i),** instructor should*

Verify teams identified hidden assumptions for trust (state issuing the license isn't compromised, person still resides in that state/ at that address, etc.)

Review methods of verifying license is legitimate (scan barcode, look-up in published book, call state and confirm number)

Review discrepancies in the analogy between driver's license and digital certificate

- license provides multimodal info, certificate is just text
- license provides photograph, address; certificate provides public key

Part A ii: Practical exploration of digital certificates in Firefox

Set-up

Students work in pairs on this exercise. Station them at computers with internet connections.

Instructions

Students will use Firefox to navigate to a banking website like www.bankofamerica.com or www.wellsfargo.com and view its certificate(s). Detailed instructions provided in the Student Handout Packet.

They will complete a list of questions about the certificate(s) and why this documentation provides confidence that the website is legitimate.

*At the end of **Part A (ii),** instructor should*

Make sure each pair could view the certificate and understand basic ideas

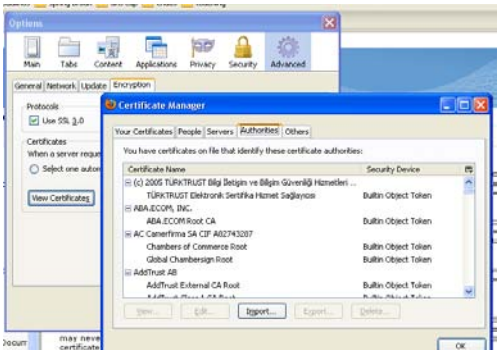
Define "subject", "issuer", "algorithm", and other terms common to certificates

Review assumptions for trusting the certificate

- issuer assumptions
  - long-enough public key to prevent hacking
  - keeps private key secret
  - expiration dates managed well
  - vetted subject's ownership of domain
  - …
- subject assumptions
  - long-enough public key to prevent hacking
  - keeps private key secret
  - continues to own the domain
  - …

Recap how we are able to know the Issuer's public key

- Ships with Firefox (show Firefox's list of trusted authorities... Tools>Options>…)



Day Two Challenge:

Encrypted communication between unfamiliar parties

Pre-requisite

Successful completion of Challenge A and the "What is a Digital Certificate?" warm-up.

Part B(i) Digital Certificate Communication

Set-up

Same as Day One. Students in Pairs as either Banks or Customers.

Instructions

"We now understand that trusted third parties are a crucial way to conduct transactions with entities we have never used before. A digital certificate is a trusted third party's documentation that a named entity owns to a particular URL and a particular public key.

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 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.

*At the end of **Part B (i),** instructor should*

Verify teams add Bank public key to certificate template.

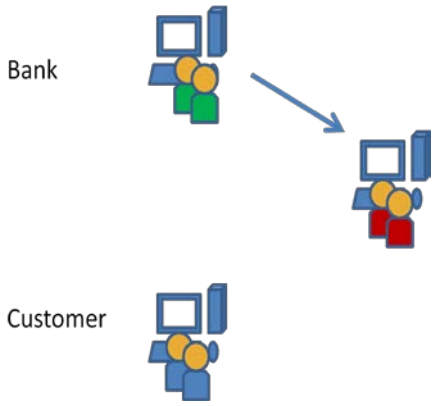
Verify a successful encryption-decryption sequence for each pair.

For entire class:

- Recap what banks sign and what TTP signs, and why
- Discuss what needs to passed as plain text and why it needs to be accompanied by signature (and who should sign that signature)

Part B(ii) Encrypted Certificate Communication with Intruders

Set-up



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

The chain of message passing is now Bank -> Attacker -> Customer.

Instructions

Bankers and Customers, your communications are now threatened by an intruder. You can assume the intruder knows many things, including at bare minimum your public key and the TTP's public key. Your new challenge is to design a process that will allow the Customers to trust communications from the Bank at least 3 minutes after the message was sent, all without knowing the Bank's public key to begin with. The Instructor will serve as the TTP. I will provide any encryption services you might need, just ask.

Attackers, you will have the opportunity to intercept the message and try your best to hack it. Once the message is sent, you will have 3 minutes to decrypt the message, insert a counterfeit one, and send it along. There are many weaknesses for you to exploit. Be sure to think creatively and plan ahead. Feel free to listen in on what the Bankers/Customers are scheming.

As the Lesson Unfolds

As trusted third party, generate unique private key at beginning of lesson. Leave private key visible for everybody. Encourage Attacker team to "steal it".

Look out for requests to upgrade length of the TTP public key. Comply with them via regenerating key. Make sure all students know of this change.

Look out for requests to sign documents. Sign them with private key and pass back to the requesting Bank. Comply with any signing requests, even from the attackers.

Help students identify known weaknesses with provided system, such as,

1) Expiration date should be added (so the certificate can be trusted only within validity period)
2) Subject's Public Key is vulnerable to hacking
3) Trusted Third Party's public key is vulnerable to hacking

This exercise may be repeated several times to allow ideas to sink in and allow all participants to try role of “attacker”.

*At the end of **Part B (ii),** instructor should*

Verify that Banker teams designed reasonable certificate procedures that recognized weaknesses and took measures to overcome them.

Verify Attackers identified several possibilities to exploit (e.g. Issuer public key hacking OR forging own certificate authority).

For entire class:

- Make list of known weaknesses, highlight any that weren’t identified
- Go over process of certificate signing by TTP. What hidden assumptions are made about TTP’s key handling?

Day Three:

Assessment: Designing certificate issuer policy

Set-up

Stick with teams of five/six from part B(ii). Now everyone plays the role of the Trusted Third Party.

Instructions

"In previous lessons, you've identified several crucial design features for Digital Certificate-based exchanges. Now, you'll all act as managers of a Certificate Issuer (aka TTP) to design policy for how you will issue certificates and manage verification requests. This challenge will summarize and extend the knowledge we've been building throughout the past few days. Your presentation at the end of this exercise will be evaluated to assess your understanding of key issues related to certificates.

Encourage the group to get online and look at real certificates and TTP policies.

You have 25 minutes as a group to plan a 10 minute presentation that answers these questions. Your presentation should also highlight overall strengths and weaknesses of your overall TTP policy.

1) *What will your certificates look like? What fields and values will be required?*
2) *What key size will be required? How will you determine this? What disadvantages might exist for keys that are "too long"?*
3) *How will you publish your public keys? What happens after the expiration date?*
4) *How will you determine whether a company is legitimate and warrants trust? What safeguards will you adhere when verifying identity and key ownership?*
5) *What policies will you require subjects to adhere to? How should they create/store private keys? Who should have access to them?*
6) *What happens when a subject does not adhere to these policies? Will you revoke a certificate? How will you let customers know?*

*At the end of **Part C,** instructor should*

Comment on strengths/weaknesses of each proposal.

After all proposals are presented, for entire class:

- Emphasize revocation as lasting issue of PKI infrastructures
- Emphasize risks present remain challenges today for VeriSign, etc.