OVERVIEW

This lesson has two primary cognitive goals: to provide students with a situated learning experience to think like an Internet security expert, and to impart practical knowledge about browsing the web securely. This assessment procedure intends to both reinforce and extend learning of both objectives and provide an indication to the instructor of the level of mastery.

Two activities will be assessed. First, students will undergo a summative team design challenge in which they pretend to be designing a trustworthy certificate policy for a Certificate Authority. They will give a ten minute presentation of their recommendations to the entire class, and this presentation's content and justification will be the basis of assessment. Second, students will individually complete a take-home exercise in which they use Firefox or another modern browser to evaluate an unknown digital certificate, list major assumptions involved in accepting the certificate, and demonstrate that they can use the browser settings to decide whether to trust or deny its authority. Each will submit a screencast of their process (at most 5 minutes in length) for evaluation.

PROCEDURE

1) *Team Design Challenge: Policies for a Trustworthy Certificate Authority*

Form teams of four to six students each. Each team is given the prompt and a series of questions they must answer. They are encouraged to talk to other teams and draw/sketch out flowcharts for several processes. They are given 20 minutes to come up with creative, consistent answers to all questions. After 20 minutes, teams must stop their ideation and focus on presentation planning. After 10 minutes of preparation, groups must give a presentation to the group lasting no more than 10 minutes. They are encouraged to identity one primary advantage and one disadvantage of their scheme as part of the goal of the presentation.

2) *Individual Take-Home Screencast: Trusting Certificates with Modern Browsing Technology*

Each student is given a prompt and a series of questions. They must open up a browsing session, navigate to a provided URL, and then think through each question out loud while manipulating the certificate or authority policies of the browser. They are encouraged to rehearse their process a few times before recording a five minute screencast (a video of their on-screen actions with audio narrative). The narrative should both answer the questions and outline things they still wonder about.

MATERIALS

Design Challenge Instructions (attached)

Practical Browsing Instructions (attached)

Design Challenge Evaluation Sheet (attached)

Practical Browsing in an Insecure World Evaluation Sheet (attached)

RATIONALE

1) Team Design Challenge

This exercise is highly situated and contributes to students "thinking like security professionals". They must develop creative answers to open-questions such as "how will you revoke certificates?" or "how do you verify a company's identity before you give them a certificate?". The presentation of a carefully justified proposal is similar to the kind of self-verification that might exist at a real corporate authority like VeriSign, Inc. The required questions will both revisit concepts built up in previous lessons (e.g. key size as indicator of time until breaking) and extend new ones (e.g. revocation), thereby fulfilling the learning goals of the assessment process.

2) Take-Home Exercise

This exercise fulfills the practical usage goals of the lesson. Students should be able to interact with a modern browser to diagnose a digital certificate for a real-world website and adjust security policies to taste. The screencast format encourages metacognition (e.g. "think out loud about your process and justify it") and provides the instructor with both visual and auditory information about what the student can do in a practical context. Successful completion of the exercise should be a summative presentation of what the individual knows about certificates and reinforce concepts learned throughout the unit (e.g. key size is related to expiration date, browsers have an internally maintained list of trusted third parties, etc). Students are also encouraged to use provide at least two things they still wonder about in their narrative (e.g. "where does the browser's list come from?"), which may encourage learning via reflection.

Trustworthy CA Policy Design Challenge 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 Authority (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?*

Take-Home Exercise Instructions

This exercise intends to evaluate your understanding of certificates and trust as it relates to practical browsing. Please download screencast software (google: "Jing") and make a video of at most 5 minutes in length in which you navigate to a bank of your choice within Firefox or similar browser and narrate the process by which you can trust that site.

Specifically, you should do the following:

1) Explain certificate's primary function. Identify and justify the key fields within the provided digital certificate

2) Explain how the browser translates the fields in a certificate into trustworthy knowledge.

    a. how does the browser verify the issuer did in fact issue the certificate?
    b. what is each public key for?

3) Identify the trusted authority and explain why the browser showed implicit trust in that authority without human confirmation.
    a. How does the browser know the authority's public key is correct?

4) Demonstrate that you can override browser settings to reject this certificate

Design Challenge Presentation Evaluation Sheet

Comment on the team's provided answers to the prompt questions:

7) *Did the team demonstrate efforts for verifying subject identity in non-digital context? Did they articulate disadvantages clearly? Did they prove both domain name ownership and identity?*

8) *Are necessary certificate fields (name, signature, public key, expiration date) present? Did the team articulate clear requirements (e.g. key size) and rationale (e.g. hacking time) for each?*

9) *Did the team's publication policy demonstrate concern for finding a trustworthy distribution channel?*

10) *Did the team demonstrate awareness that human knowledge of private keys is dangerous? Did they take appropriate safeguards that are both practically plausible and good for trust?*

11) *Was the revocation policy clear? Did they acknowledge disadvantages?*

Overall comments:

Practical Browsing Take-Home Exercise Evaluation Sheet

Did the individual complete the following tasks successfully?

1) Explain certificate's primary function. Diagnose key fields within the provided digital certificate.

- ☐ Says something like "A certificate's primary function is to bind an entity to a public key"
- ☐ Can correctly identify subject's public key field and evaluate key size
- ☐ Can correctly identify subject's expiration date and explain how this value is derived.

Comments

2) Explain how the browser translates the fields in a certificate into trustworthy knowledge

- ☐ Explains the certificate signature verifies the authority did in fact issue the certificate
- ☐ Explains that the subject public key is used to initiate encryption

Comments

3) Identify the trusted authority and explain why the browser showed implicit trust in that authority without human confirmation.

- ☐ Explains the browser has internal cache of trusted authorities
- ☐ Explains where this internal cache comes from (ships with browser)

Comments

4) Demonstrate ability to override this trust within the browser.

- ☐ Accesses browser's trusted authorities list and toggles enabled switch on the one in question

Comments