Security Protocols and Application — Final Exam Part 2/2

Philippe Oechslin and Serge Vaudenay

19.6.2012

- duration: 2h00
- no document allowed
- a pocket calculator is allowed
- communication devices are not allowed
- the exam invigilators will not answer any technical question during the exam
- the answers to each exercise must be provided on separate sheets
- readability and style of writing will be part of the grade
- do not forget to put your name on every sheet!

Extended Validation (EV) Certificates

Q.1 What are the specific criteria that an applicant must fulfill in order to have an EV certificates issued for a website ?

Q.2 What elements are mandatory in an EV certificate and which are explicitly forbidden ?

Q.3 Which elements of a certificate should a browser verify in order to know if a certificate is really an EV certificate ? We consider an attacker who is able to obtain false DV certficates but not false EV certificates. The attacker is also able to position himself as a man-in-the-middle and intercept traffic between a victim and a webserver. The victim is using a browser that is vulnerable to the attacks on EV certificates seen in the seminar.

Q.4 The victim connects to an EV certified website that loads javascript code from a non-EV certified website. Describe in three or four short steps how the attacker can modify the contents of the page displayed in the browser without losing the green glow.

Q.5 In this case the victim loads a page from an EV certified website that does not load elements from another site. The attacker owns a DV certificate for this site and wants to abuse the same origin policy to inject code in the original page without losing the green glow. Explain in a few steps how the attacker would carry out his attack:

Q.6 In the same situation (an EV site that does not load elements from another site), the attacker wants to carry out an SSL rebinding attack. Explain in a few steps how the attacker would carry out his attack:

Q.7 What are the advantages and the limitations of the SSL rebinding attack compared to the attack exploiting the same origin policy?

Q.8 Finally the attacker wants to try one last trick. He tries to exploit a cache poisoning attack. He wants to modify the page `https://epfl.ch/register_grade.html` to make sure he gets a good grade when the teacher connects to this site and grades his exam. Explain in a few steps how the attacker would carry out his attack:

Q.9 What could the developers of browsers do (or may already have done) to better protect against the four attacks described in the previous questions (mixed origin, same origin, rebinding, cache poisoning).

Q.10 As creator of a website, can you find a way to protect your site against some of these attacks ?