Security Protocols and Application — Final Exam Part 2/2
Solution

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 ?

He must prove that he is the legal representent of the website he is requesting a certificate for.

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

It must have an EV identifier, must have a CRL or an OCSP. May not have wildcards, may not have MD5 hashes.

Q.3 Which elements of a certificate should a browser verify in order to know if a certificate is really an EV certificate ?

The certificicate must have the EV identifier. It must be signed by a CA which is allowed to issue EV certificates.

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.

The victim loads the main page, the green glow appears. The victim automatically loads the javascript from the non-ev site. The attackers makes a MITM attack and inserts a script that modifies the main page. The green glow stays.

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:

The victim loads the main page, the attacker makes a MITM attack to insert code that load a DV certified pop-up. Once the pop-up is loaded it makes the browser load the original page again. The original page is loaded without modification and obtains the green glow. Thanks to the same origin policy the pop-up can interact and modify the original page and the destroy itself. The green glow does not go away.

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:

The victim loads the main page, the attacker makes a MITM attack to record the cookies and parameters of the request and returns a page the will make the browser reload the page with the same parameters again. In this second request the attacker does not intervene and thus the browser loads the original and displays the green glow. The attacker can now try to intercept any new request and play the same game again.

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

The rebinding attack does not allow the attacker to modify the content of the page protected by the EV certificate. The attacker doesn't even get to see the content of the page. But since he has all parameters and cookies of the request he could probably request a copy of the page for himself. The advantage of the attack is that it does not depend on JavaScript (at least if the requests are GET requests).

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:

The attacker makes a MITM attack when the teacher connects to a HTTP site. He injects a frame that loads `https://epfl.ch/register_grade.html` *without displaying it. He makes a MITM attack on this connection to modify the page to his will and sets an expiry date in 2013. The modified page gets cached by the teachers browser. When the teacher connects to the original site, the cached page is loaded from his local cache.*

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).

Do not display the green glow if: some elements are not EV, the EV status changed over consecutive loads, allow same origin only from same EV level, separate EV and DV cache.

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

Do not load elements from other sites. Always serve fresh pages, even if not modified since the last access.