A proxy-based security solution for web-based online eHealth services

Sampsä Rauti, Heidi Parisod, Minna Aromaa, Sanna Salanterä, Sami Hyrynsalmi, Janne Lahtiranta, Jouni Smed, and Ville Leppänen

University of Turku
Introduction

- eHealth refers to healthcare practices supported by electronic processes and communication
- Users have continuously improving possibilities to promote their own health
- We concentrate on web-based health services
- An example: Taltioni service used in Finland is such online environment with various health-related applications
Introduction

• Web-based eHealth services face many information security related challenges

• Pieces of malware (malicious programs) that have infiltrated into the user's own computer can cause a significant security risk for any online service where the users display, input and store their personal data

• For example, a piece of malware residing in the user's web browser can steal or change the information that the user sends to an online service or vice versa

• We concentrate on these client-side security threats
eHealth applications

• eHealth applications can contain general health information related to for example health education but also private information related to consumer's patient records
Patient data

- For example, the HL7 standards are followed in Finland
- Patient record systems list patient name, date of birth, sex, patient address, phone number, marital status, SSN, religion, citizenship and nationality etc.
- The information stored and displayed in these systems can be of very sensitive and private nature
- There are potentially many motivated attackers
Taltioni

- Taltioni aims at building a single service platform and database that contains information on health and well-being for Finns, healthcare providers and producers of well-being services

- Taltioni is meant for citizens to create and maintain their well-being related information

- The basic idea is that the information in Taltioni is mostly created by citizens but some of it is provided by healthcare professionals as well
Some Taltioni applications

- **Oma Terveys** application brings together all kinds of health information - public and private - on the user. The user can display results of laboratory tests, information on vaccinations, times for doctor appointments and prescriptions. The application also gathers data on diseases that need constant attention, for example blood sugar and blood pressure levels.

- **Wellmo** is an application that helps the user to achieve a healthy lifestyle. It collects all kinds of data related to the user's well-being. More specifically, it is used to store information on the user's physical exercise, weight, sleep and alcohol use.

- **Lääkekortti.fi** service helps the user to manage data on medication and vaccinations.
Threat

- This kind of web applications are susceptible to the client-side attacks
- Of course this is not Taltioni-specific problem, the same threat is present in all web applications that handle sensitive data
- The client side is exposed to the greatest information security threat. It is usually much easier for an attacker to attack the user's computer than to compromise the server side of an online service.
The attacker's motivation

- **Ransomware.** Health records can be held captive to extort money.
- **Channel.** The web-based online health service can be turned into a proxy for malware.
- **Harm.** Health devices operated via a web-based service can be accessed and the function of the device, related data, measurement intervals or quality control data may be altered.
- **Fraud.** The information captured from the service could be used to commit identity theft related frauds.
- **Business.** If the service is used for doctor-patient interaction, the attacker can act as either one. This could be exploited to make the patient to use false online pharmacies.
Scenario: spying and modifying data

- Assume a malicious adversary would like to spy on and possibly alter the data the user inputs when using an eHealth application.
- The malicious program used by the adversary infects the unsuspecting user's computer and browser.
- Whenever a certain web page (web application) with a correct URL address is loaded, the malware starts to observe the user's actions.
- When the user submits data, the malware intercepts the transmission, extracts all data and modifies the values according to the adversary's needs.
- The browser sends the data to the server, including the values modified by the malware.
Scenario: spying and modifying data

• When the server sends its reply to the user's browser, the piece of malware can modify it data in the server's reply, so that the user does not notice the changed values.
• The user thinks that the original transaction was delivered to the server intact.
• Both the server and the user are oblivious to the fact that their communication has been compromised.
The need for a new security solution

- This kind of attacks are already happening
- For example, Zeus is a piece of malware that is able to spy and modify user transactions on the fly
- eHealth applications can be considered more critical than many other web applications
- It is clear that we need new ways to mitigate these threats
Our solution

- Our idea is to change the application running on the user's browser so that it will become very difficult for malware to compromise it.
- Changing the application's executable code while preserving its original functionality is called **obfuscation**.
- The user will not notice any changes in the functionality of the application, but the code is different on each user's machine.
- We make attacking the web application even harder by obfuscating it again continuously during its execution.
- When the structure of the application's code is continuously changed, the malware has very little time to analyze and modify it.
Our solution

- In our solution, the obfuscator acts as a proxy, a service that acts between the clients and the server side
- The obfuscator is totally invisible to the user of the obfuscated application
- The obfuscator is also independent of the web application that is being protected and also does not depend on the server
Our solution

- Our solution mitigates scenarios spying and modification attacks by changing the application's structure.
- The adversary still has ways to capture the data that the user inputs in the application, but analyzing the application and the data is now harder for a piece of malware.
- Modification attacks are often even more dependent on the known structure of the application.
- Especially generic, automated malware attacks will become much more difficult.
Conclusion

- The sensitive information flowing in web-based eHealth systems can be compromised in client-side attacks, which is a serious threat to web-based eHealth services and their users.
- We have proposed a proxy-based solution that could be integrated to existing web-based eHealth applications to make attacks more difficult to perform.
- Of course, there are also many other application areas where this kind of web application protection could be used.
- The adversary can probably always find some way to spy and modify online transactions with sufficient amount of time and work.
- Still, mitigating automated and generic attacks will be an important goal in the future.
Thank you!

Questions or comments?