Web Application Security with Contactless Identity Cards using Near Field Communication

Arvo Sulakatko, Alex Norta

Information and Communication Technology
Tallinn University of Technology
Ehitajate tee 5, Tallinn, Estonia
arvo.sulakatko@jsc-solutions.net, alex.norta.phd@ieee.org

Abstract. For over a decade, web servers have been able to encrypt their communication with the client by using Secure Socket Layer Protocol [1]. While this option only prevents casual eavesdropping for generic web sites and applications, for other applications the server must know who the client is. The client operating systems and web browsers may install a client-side certificate in their keystore that awaits selection. An essential requirements for identity services is to prevent identity theft. With the advancement of cost effective contactless cards, such a solution is with reach. Currently, only contact cards have been used to serve as client certificate keystores. Since all new android devices are equipped with NFC[3] reader chips, the research opportunity arises how to store on contactless cards an identity for web applications. Such cards with a set of secret PIN codes can not be copied and must be in physical posession of the user. Until recently, a web application was neither able to interact with the certificates used to secure the connection, nor was a web application able to sign any data. With the availability of implemented W3C WebCrypto API[2], a possible solution is within reach. We propose an architecture to extend Google Chrome for Android and use PIN1-protected client certificates from Contactless Identity Cards that use Near Field Communication to perform an SSL handshake. After loading a web application, it inspects the Contactless Identity Card and performs additional tasks such as signing data by prompting a request for PIN2.

Keywords: Web Applications, Secure Hardware, NFC

References

[1] Davis, M., Gray, S., Kuehr-McLaren, D., Morrison, I., Shoriak, T.: Systems, methods and computer program products for authenticating client requests with client certificate information (Jul 11 2000), http://www.google.com/patents/US6088805, uS Patent 6,088,805
[2] Hofstede, N., Van den Bleeken, N.: Using the w3c webcrypto api for document signing. In: WASH. pp. 10–16 (2013)
[3] Yadav, A., Sharma, A.: Near field communication (2014), http://jiaats.cyberoot.org/Journals-Pdf/JEEE/jeee-3.pdf