

Display Security for Online Transactions

Mohammed AlZomai¹, Bander AlFayyadh¹, and Audun Jøsang²

¹ Information Security Institute
QUT, Australia

{m.alzomai, b.alfayyadh}@student.qut.edu.au,

² UNIK Graduate Center
University of Oslo, Norway
josang@unik.no

Abstract. Secure online transactions with human users normally require visual display units for verifying the correctness of important elements of the transaction before it is being submitted. When commodity computer platforms get exposed to the Internet, even for a short period, there is a real and substantial risk that they get infected with malware that can modify anything on the computer, including what is displayed to the user and what is being sent over the Internet. This threat makes visual verification of transaction data unreliable, and undermines other security mechanisms used for online transactions. This paper proposes a method for display security that will make the verification of displayed data more robust and reliable.

1 Introduction

We generally rely on what we see on a computer display to read information we receive, to verify that we type correctly, and to ensure that the data being sent through an online transaction is according to our intentions.

In general, all this depends on the integrity of the computing platform to which the VDU (Visual Display Unit) is connected. In practice it is extremely difficult to assess the integrity of a general purpose computing platform, and thereby to ensure that what the VDU displays is correct [1, 2, 4, 3, 5, 6].

The prospect that the computer display can lie to us is both frightening and real. This problem is amplified by the fact that we often read data from platforms that are not under our control, and that there can be strong financial incentives for trying to manipulate the systems and the way data is displayed.

This paper describes a method for making displayed data secure for online transactions, i.e. to ensure that what is displayed on the VDU correspond to what is being sent through an online transaction.

2 Conclusion

Current display security technologies are not able to provide high assurance of the integrity of displayed data. We have shown that it is possible to make the security of displayed data independent of the security of the client platform.

Bibliography

- [1] A. Alsaid and C. Mitchell. Dynamic Content attacks on Digital Signatures. *Information Management & Computer Security*, 13(4):328–336, 2005.
- [2] A. Jøsang, D. Povey, and A. Ho. What You See is Not Always What You Sign. In *Proceedings of the Australian UNIX and Open Systems Users Group Conference (AUUG2002)*, Melbourne, September 2002.
- [3] K. Kain, S.W. Smith, and R. Asokanm. Digital Signatures and Electronic Documents: A Cautionary Tale. In *Proceedings of IFIP Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security*, 2002.
- [4] K. Scheibelhoferm. Signing XML Documents and the Concept of What You See Is What You Sign. Masters thesis, Graz University of Technology, Austria, 2001.
- [5] Adrian Spalko, Armin B. Cremers, and Hanno Langweg. The fairy tale of ‘What You See Is What You Sign - Trojan Horse Attacks on Software for Digital Signatures’. In *IFIP Working Conference on Security and Control of IT in Society-II (SCITS-II)*, Bratislava, Slovakia, June 2001.
- [6] Arnd Weber. See What You Sign: Secure Implementations of Digital Signatures. In *Proceedings of the International Conference on Intelligence and Services in Networks*, pages 509–520, 1998.