Visual Mutual Authentication - an approach to secure online banking

Denise Doberitz and Sebastian Gajek

Horst Görtz Institut für IT-Sicherheit
Ruhr-Universität Bochum

Today, most applications are only as secure as their underlying system. Since the design and technology of malware has improved steadily, their dectection is a difficult problem. As a result it is nearly impossible to be sure whether a computer, that is connected to the internet, can be considered trustworthy and secure or not. The question is, how to handle applications, that require a high level of security, such as online banking. In consequence we are interested in a solution, that allows us to establish a secure and trusted communication, although the underlying system is untrusted.

In this paper we present an approach, that is based on Visual Cryptography. In [NaorS94] Shamir and Naor presented the concept of Visual Cryptography, that handles the plaintext to be encrypted as a graphic, that is processed pixel by pixel and thus implies interesting characteristics concerning security and fault tolerance. In [NaorP97] Naor and Pinkas demonstrated how to use Visual Cryptography for the authentication of one party without trusting the underlying system. Based on this, we develope a scheme for mutual visual authentication of a user and a server, that allows us to establish a trusted channel between the two parties, and can be used for secure communication.

We describe the Visual Mutual Authentication - Scheme and demonstrate its application as a protocol on the example of online-banking. The protocol provides a practical and user-friendly approach to secure online banking, that is not only resilient to malware, but also resistant to phishing.
Using Visual Cryptography, the user's key is a transparency that has to be applied on the computer monitor. With the tansparency, the decrypted message can simply be read from the monitor by the user. We transfer this application to a TAN-scheme and integrate a one-time pad structure. As a result, we achieve a user friendly scheme with a high level of secrecy.

References

[NaorS94] Moni Naor and Adi Shamir. Visual Cryptography, EUROCRYPT '94, *Volume 950 of Lecture Notes in Computer Science*, pp. 112. Springer-Verlag, 1995.

[NaorP97] Moni Naor and Benny Pinkas. Visual Authentication and Identification. CRYPTO '97, *Volume 1294 of Lecture Notesin Computer Science*, pp. 322-336. Springer-Verlag, 1997.