On The Online Banking Security

Anton Sergeev, Victor Minchenkov
St. Petersburg State University of
Aerospace Instrumentation
190000 Bolshaya Morskaya 67, Russia
{slaros, victor }@vu.spb.ru

Abstract

Online banking (Internet banking) is a set of services and technologies allowing managing financial transactions (such as money transfers, tracking accounts, viewing credit card activity and etc.) on a secure website. The main goal is to provide simple way for customers to access accounts through the Internet using web-based systems. Currently online banking has become a hot topic in the modern in banking and financial management e.g. "close to 40% of U.S. households do some banking online".

The main question for the customers of online banking is how safe is it? Is it really so secure to make financial transactions via unsecure public networks as in the bank office? What are the main threats and dangers for such systems?

In this work we try to answer these questions. The main goal is to analyze and audit security mechanisms of online banking and check how strong they are. We start with reviewing and classification of the existing software for online banking. The common and application specific capabilities, functions and features are described. Then we continue the analysis from the position of information security and data protection focusing on security protocols, cryptographic algorithms, PKI (key usage, storage and distribution) issues. Then the most realistic attack models are compared. One of the hardest attack models is the man-in-the-middle attack when hacker has no physical access to a client computer and a remote server but can view/modify the data transmitted over the network between them. The goal of unauthorized user is to make a disclosure of the transmitted information (attack on Confidentiality), modify it without authorization (attack on Integrity) or even steal the secret keys and other authorization information (attack on Authorization).

We also analyze the known vulnerabilities and security problems of the client-side technologies (such as Java applets, Java script, ActiveX) that are widely used in web-banking. Summarizing all the found vulnerabilities and problems in the security mechanisms of online banking we suggest and describe several possibly successful attacks. As the result of our work we should conclude that the security schemes and protocols of the existing online banking systems do not provide a sufficient level of information security.

Index Terms: Online Banking, Internet, Security, Data Protection, Man-In-The-Middle, Attack.