Abstract

Current authentication practices suffer from many loopholes. To access an online banking facility, a customer with Internet access would need to register with the institution for the service, and set up some password for authentication process. Basically there are two types of password inputs allowed by banking websites these days. The first one is the traditional input in which we enter the password using keyboards and the second one is the virtual input in which the system accepts password using a virtual keyboard available in login pages of all bank websites. Virtual keyboards are considered as additional security steps for accessing online banking websites but this paper will describe how weak this implementation can be and what security measures can be adopted to maintain the confidentiality.

References

- White paper on "Threats to Online Banking- Symantec Security Response", Dublin
- Analysis of New Threats to Online Banking Authentication Schemes by Oscar Delgado, A. Fuster-Sabater and J. M. Sierra
- UCAM CL. TR-731 ISSN 1476-2986: A new approach to Online Banking by Matthew Johnson
- Video demonstrating a Trojan Attack against Caja Murica Bank of Spain http://www.hispasec.com/laboratorio/cajamurcia_en.swf
- Demo of Attack against Citi Bank India www.tracingbug.com/index.php/articles/view/23.html

**Index Terms**

Computer Science  
Security

**Keywords**

Virtual Keyboard  
Shoulder Surfing  
Displacement Factor  
Traversal  
Trojan