Wireless Authentication for the Web Services

Valery Kirkizh*, Maria Komar†, Kirill Alexandrov‡, Vitaly Petrov‡
*Saint-Petersburg State University of Aerospace Instrumentation, Russia
†Yaroslavl State University, Russia
‡Tampere University of Technology, Finland
vkirkizh@vu.spb.ru, maria.s.komar@gmail.com,
kirill.aleksandrov@fruct.org, vitaly.petrov@tut.fi

Abstract

Wireless authentication is a growing research direction within the last several years. In contradiction to currently deployed solutions, mainly focused on login/password scheme, wireless keys allow user not to enter any critical information on the computer, rather than present a physical proof of his privileges. In general, the procedure works as follows. The key establishes a connection with the computer using some short radio technology: Wi-Fi, Bluetooth, NFC, RFID, etc. and sends its ID. Computer validates the ID or either forwards to it to the online server, user is trying to log in. If the validation succeeds, the user gets access to the system, otherwise his request is rejected.

The major problem of the present protocol is that the ID being sent as a plain text. As such, the eavesdropping attack becomes possible, that ruins the system security. In the following demo, we highlights this drawback and also propose the particular cryptographic algorithm usage to solve the problem. Our solution works for operation system login and FRUCT Social Network access. However, it can be easily extended for almost any application of web service.

Index Terms: Semantic Web, Internet of Things, Machine-to-Machine Communications, Social Networks, Bluetooth, Wireless Authorization, Smart Spaces.