TLS security protocol for online banking, Facebook has 'serious weaknesses,' researchers say

February 3 2013

The protocol that provides security for online banking, credit card data and Facebook has major weaknesses, according to researchers at Royal Holloway University.

The Transport Layer Security (TLS) protocol is used by millions of people on a daily basis. It provides security for online banking, as well as for credit card data when shopping on the Internet. In addition, many email systems in the workplace use it, as well as a number of big companies including Facebook and Google.

Professor Kenny Paterson from the Information Security Group at Royal Holloway and PhD student Nadhem AlFardan found that a so-called 'Man-in-the Middle' attack can be launched against TLS and that sensitive personal data can be intercepted in this way. They have identified a flaw in the way in which the protocol terminates TLS sessions. This leaks a small amount of information to the attacker, who can use it to gradually build up a complete picture of the data being sent.

Professor Paterson said: "While these attacks do not pose a significant threat to ordinary users in its current form, attacks only get better with time. Given TLS's extremely widespread use, it is crucial to tackle this issue now.

"Luckily we have discovered a number of countermeasures that can be

used. We have been working with a number of companies and organisations, including Google, Oracle and OpenSSL, to test their systems against attack and put the appropriate defences in place."

Provided by Royal Holloway, University of London