The truth about ABN-AMRO's e.dentifier2

Arjan Blom[1], Gerhard de Koning Gans[2], Erik Poll[2],
Joeri de Ruiter[2], and Roel Verdult[2]

[1] Flatstones, The Netherlands.
arjan@flatstones.nl

[2] Institute for Computing and Information Sciences, Digital Security Group,
Radboud University Nijmegen, The Netherlands.
{gkoningg,erikpoll,joeri,rverdult}@cs.ru.nl

Proposal for talk and/or poster at ICT.OPEN

We present a security analysis of an internet banking system used by ABN-AMRO, in which customers use a USB-connected device – a smartcard reader with a display and numeric keyboard – to authorise transactions with their bank card and PIN code. Such a set-up could provide a very strong defence against online attackers, notably Man-in-the-Browser attacks, where an attacker controls the browser and host PC. However, we show that the system we studied is seriously flawed: an attacker who controls an infected host PC can still get the smartcard to sign transactions that the user does *not* explicitly approve, which is precisely what the device is meant to prevent.

The flaw is not due to a simple implementation bug in one of the components (e.g. the device or the software components on the PC). It is a more fundamental design flaw, introduced in assigning responsibilities to the different components and designing the protocols between them.

The system was developed by the Swedish company Todos AB, a company since acquired by Gemalto. The manufacturer's website claims this device is "the most secure sign-what-you-see end-user device ever seen", a claim that is clearly false. ABN-AMRO is one of the three biggest banks in the Netherlands, with 6.8 million customers. Given the popularity of internet banking in the Netherlands, this means that millions of these devices are in the field.

More fundamental questions raised by this embarrasing security flaw are how it could possible have been missed in security evaluations – or indeed, how it could have been introduced in the design without anyone noticing – and how such flaws could and should be detected, or better still, prevented.

A paper about this will be presented at the NordSec 2012 conference in Sweden [1], one week after ICT.OPEN.

References

1. Arjan Blom, Gerhard de Koning Gans, Erik Poll, Joeri de Ruiter, and Roel Verdult. Designed to fail: A USB-connected reader for online banking. In *17th Nordic Conference on Secure IT Systems (NordSec 2012)*, volume 7617 of *Lecture Notes in Computer Science*. Springer-Verlag, 2012.