



## On the Insecurity of Microsoft's Identity Metasystem CardSpace

### Yet, another identity management system broken

**Bochum, Germany, May 27, 2008**

Identity theft has become the fastest growing crime on the Internet. To alleviate the threats Microsoft has enrolled a novel Web authentication system called CardSpace [1]. It bases on open standards, such that various applications can make use of the identity metasystem, including commodity browsers like Microsoft Internet Explorer 7 or Firefox 2 (with some add-on). Due to the fact that Microsoft used open standards to design and implement the metasystem and many global players (e.g., Google, Yahoo, Verisign) have already announced to work closely with CardSpace [1], CardSpace authentication has the potential to become widely deployed on the Internet and replace the mature password-based authentication in many interesting settings ranging from eCommerce to eHealth or eVoting applications.

The idea of CardSpace authentication is perspicuous. Instead of using passwords, CardSpace organizes user's personal digital identities as visual information card (InfoCard). Simply by clicking on the card, a process of authentication is invoked which requires the user only to confirm the information to be transmitted. The identity metasystem and the underlying cryptographic protocols provide the remainder and assure that a security token is retrieved and forwarded to the requester. Loosely speaking, it acts like a „guarding angel“ and protects the user from disclosing sensitive information to identity thieves.

Xuan Chen and Christoph Löhr, two outstanding IT-security students at Horst Görtz Institute for IT Security (HGI), have implemented an attack against CardSpace and show that an identity thief may filch the authentication token issued by CardSpace. This is a crucial security problem. By replaying the token, they prove evidence that it is feasible to impersonate the user and gain access to the user's services. In order to demonstrate not only the feasibility, but also the attack's practicability, Chen and Christoph present a proof of concept implementation where they apply dynamic pharming [3]. Their attack is reproducible without minor technical sophistication. Against this background, Chen and Christoph conclude that it is realistic to expect attacks against CardSpace soon in the wild. More information, detailing the attack and presenting countermeasures can be found in their Technical Report [3].

### IT Security Research in Bochum

Prof. Schwenk's group is part of the Horst Görtz Institute for IT Security (HGI), one of the largest university-based security research centers in Europe. Prof. Schwenk's group is internationally renowned for their work in Internet security and Applied Cryptography. Ruhr

University Bochum has the most comprehensive offerings in IT security education (Bachelor, Master, distance learning) in Germany.

### **Further Information**

Prof. Dr. rer. nat. Jörg Schwenk  
Chair for Network and Data Security  
Ruhr University Bochum  
Universitätsstr. 150  
D-44780 Bochum  
Germany

Phone: (+49) (0)234 / 32-26692  
eMail: [joerg.schwenk@nds.rub.de](mailto:joerg.schwenk@nds.rub.de)

### **Web Links**

- [1] <http://msdn.microsoft.com/en-us/library/bb882216.aspx>
- [2] <http://self-issued.info/?p=68>
- [3] <http://demo.nds.rub.de/cardspace>