# On the Insecurity of Microsoft's Identity Metasystem

S. Gajek, J. Schwenk, X. Chen
Horst-Görtz Institute for IT Security

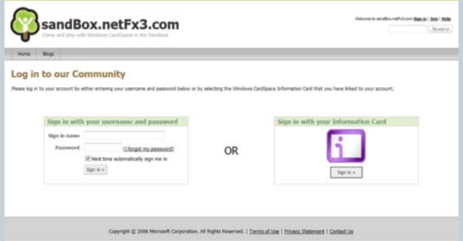
Technical Report HGI TR-2008-003
May 2008.

**PRESENTED BY TAO WANG**

# Summary

- Identified a vulnerability shared by browser-based authentication protocol
- A proof of concept implementation of the attack building on dynamic pharming [VA Ka07]
- Proposed two countermeasures

# Attack



sandBox.netFx3.com

Come and play with Windows CardSpace in the Sandbox

Welcome to sandBox.netFx3.com Sign in | Join | Help

Search

Home | Blogs

Log in to our Community

Please log in to your account by either entering your username and password below or by selecting the Windows CardSpace Information Card that you have linked to your account.

Sign in with your username and password

Sign in name

Password (I forgot my password)

☑ Next time automatically sign me in

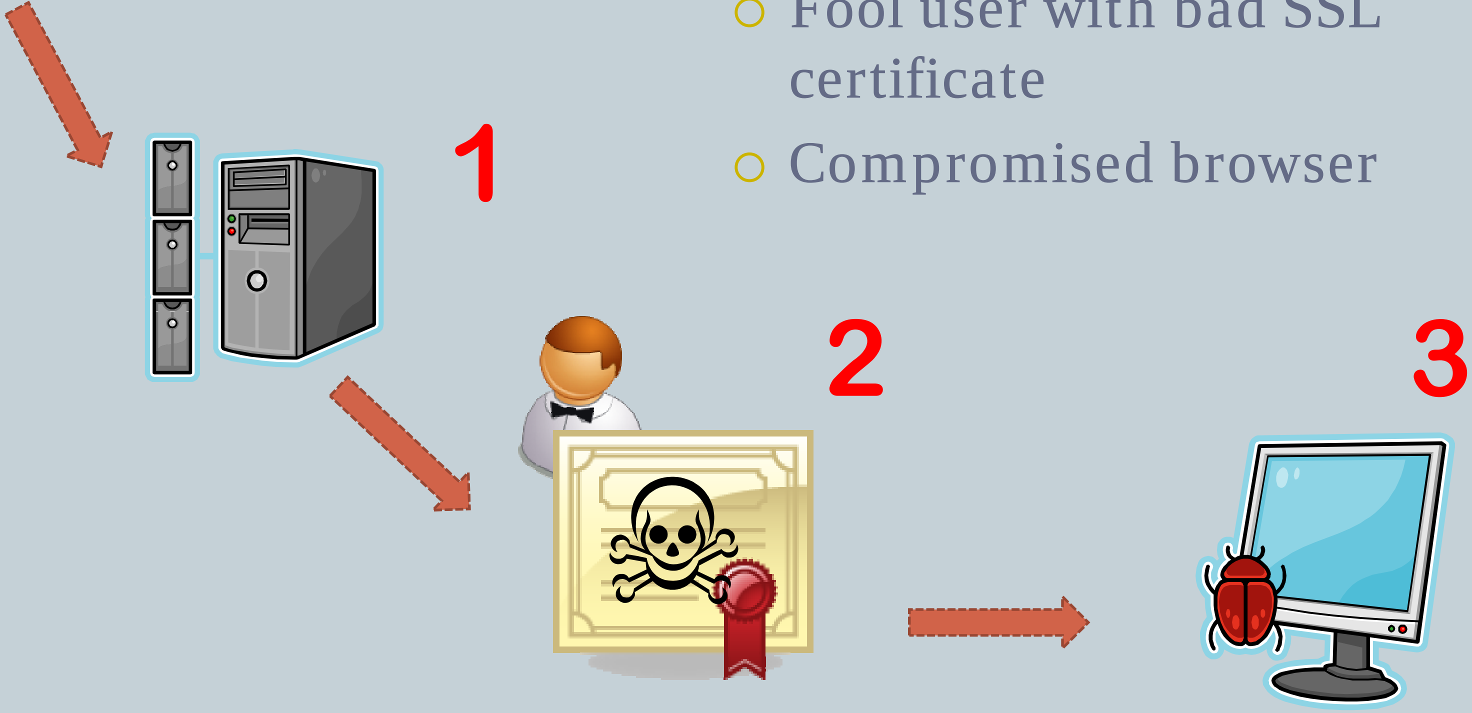
Sign in »

OR

Sign in with your Information Card

Sign in »

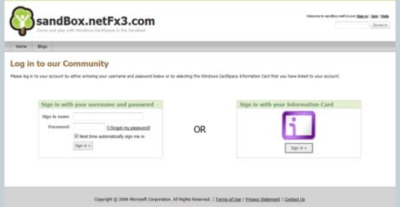
Copyright © 2006 Microsoft Corporation. All Rights Reserved. | Terms of Use | Privacy Statement | Contact Us



- Compromised DNS
- Fool user with bad SSL certificate
- Compromised browser

# Critical comment

- How likely would that happen?
  - DNS
    - Well studied
  - Certificate warning
    - Troublesome process to install an invalid root certificate
    - IE 7 & Firefox's full page warning



sandBox.netFx3.com

Come and play with Windows CardSpace in the Sandbox

Welcome to sandBox.netFx3.com Sign in | Join | Help

Search

Home | Blogs

Log in to our Community

Please log in to your account by either entering your username and password below or by selecting the Windows CardSpace Information Card that you have linked to your account.

Sign in with your username and password

Sign in name:

Password: (I forgot my password)

☑ Next time automatically sign me in

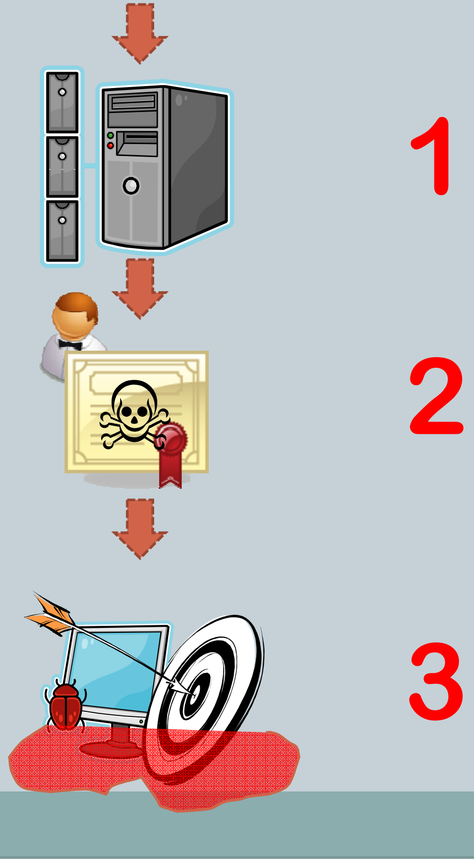
Sign in »

OR

Sign in with your Information Card

Sign in »

Copyright © 2006 Microsoft Corporation. All Rights Reserved. | Terms of Use | Privacy Statement | Contact Us



# Appreciative comments

- Demonstrated the severity of SOP problem
  - Shared by all browser based authentication systems
  - Weakest link theory
- Proposed two countermeasures
  - Easy to implement
  - Protection around Cardspace’s security token

# Question

- What would be the most urgent thing to do?

**Enhance CardSpace to address the issue identified**

**Evaluate the security of CardSpace and its running environment as a whole**

**Update SOP**