Strong(er) Authentication

Another round of motivation and inspiration

SWITCH

Serving Swiss Universities

Lukas Hämmerle
lukas.haemmerle@switch.ch

Email sent to some ETHZ staff and students

```
Date:  Thu, 22 May 2008 09:24:33 -0500
From:  Ethz Support Team <support@ethz.ch>
Subject:  Account Update
To:  undisclosed-recipients: ;
Reply-To:  account.desk@y7mail.com
X-ISG_D-AGRL-MailScanner:  Found to be clean
X-Spam-Status:  No

Dear User

This mail is to notify all users that the site will be
undergoing upgrade in a couple of days from now.
```

So far so harmless, but let’s read on…

Now it get’s more interesting…

Hence, as a user of our site, you are required to send us your
email account details to enable us acknowledge account activeness

Furthermore, be informed that we will be deleting all mail account
that is not active so as to create more space for new users.

Therefore you are advice to send us your mail account details
As requested below

*User name:.........
*Password:..............
*Date of birth:................
*Security question:............
*Security answer:......................

All users are advise to complete this update.
Regards

Mark Anderson
Tech/Maintenance officer

Should I care about such mails?

- This is **only the most recent example** of many such mails that universities/FHs users receive

- Phishing mails are not only targeting e-banking users!
  - Stolen university accounts seem also attractive to phish,
  - But it is not quite clear yet for what purpose: Probably identity theft

- Do you trust your staff member’s/student’s security awareness to not respond to such mails?

What can I do against it?

- Why not evaluating strong(er) authentication methods than the standard username/password?
  - … at least for some users groups

- You are not happy with these authentication methods?
  - X.509 user certificates
  - SMS tokens
  - TAN lists
  - RSA SecurID or mobile FreeAuth OTP

  We already presented some of them to work with AAI.

- There are even more alternatives… even Swiss ones...

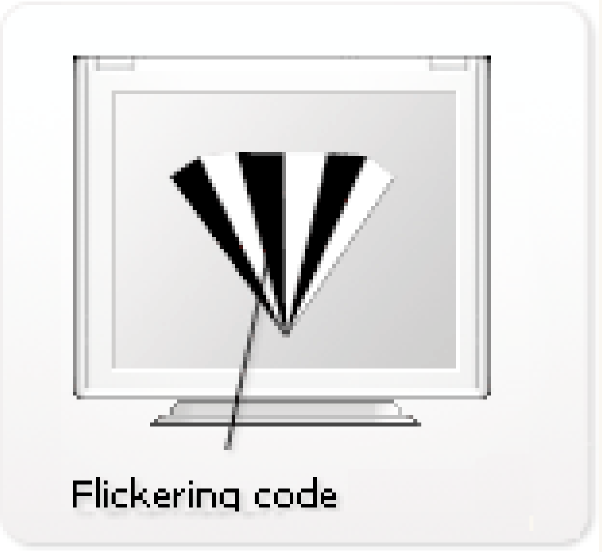
The new kid on the block: AXS Token

- BFH Spin-off
  - Known from Start-Up (SF1)

axsionics
secure e-access solutions

- 3-factor AXS hardware token (trusted platform)
  - Application decides how many factors have to be provided
  - Very versatile (“Internet Passport”)
  - Can be used for almost any authentication
  - Fingerprint is used as 3. factor

- Device communication via Screen
  - Using Flickering Code
  - Even works with iPhone
  - Safe from man-in-the-middle attacks if used transaction based



AAA/SWITCH: e-Infrastructure for e-Science

- SWITCH would love to **support** you in order to **explore and foster** stronger authentication methods for AAI

- Why not getting it funded by AAA/SWITCH subsidies?
  - AAA also stands for **A**AI **A**uthentication + **A**ssurance Levels

- **October 31, 2008:** Deadline for submission of proposals for the fall 2008 competitive bid
  - Or ask your university contact person about the university projects

- More information on: http://www.switch.ch/aaa/