

SIM token

Vladimír Kajš,
SIM Product Manager
New Product Development

Telefónica

O₂

Headline:

"Hackers stole more than 10 Mil CZK!!!"

The biggest Czech retail banks suffered massive attacks in spring 2006

The weak point is the client

Attacks were organized via electronic channels

Ekonom.iHNed.cz 31. 8. 2006 00:00

Internetbanking: Slabinou je klient

Banky zažily první organizovaný útok na účty prostřednictvím elektronického bankovníctví. A co váš účet? Je v bezpečí?

Není pohodlnějšího ovládní bankovního účtu než z domácího křesla přes internet. Ovšem za pohodlí se platí vysokou cenou nemalou - ztrátou většiny peněz z účtu. Stalo se tak nedávno u obchodní banky, na jejich případ upozornil dosud. Právě. Patřící k...

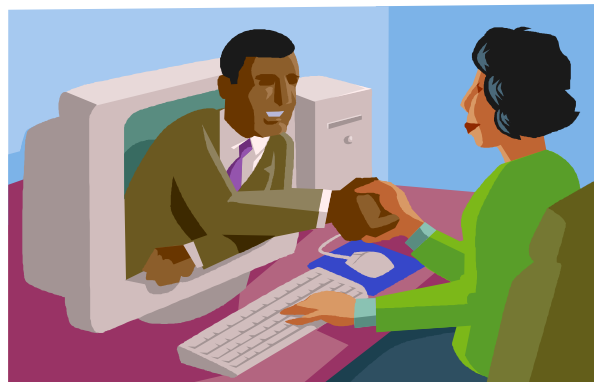
Successful attacks were done over the phone...

SIM swap fraud of \$200,000 in South Africa – bank account cleared with the help of plain text SMS with OTP

Deep in the forest of the virtual world ...

1 ...GSM and Internet opened new ways of communication between service providers (customers) and their end-users

- Voice (Helpdesk, call-centers, ..)
- Internet (e-banking, self-care, VPN access, ...)
- SMS (GSM Banking, ...)
- Point of sales



... are lurking real robbers!

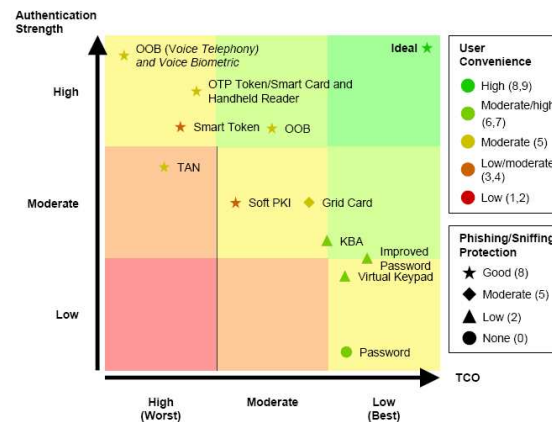
2 Identity theft brings problem of 3 losses:

- Finance
- Trust
- Information

Banks especially are looking for an effective tool!!!



Figure 1. Consumer Authentication Methods Compared

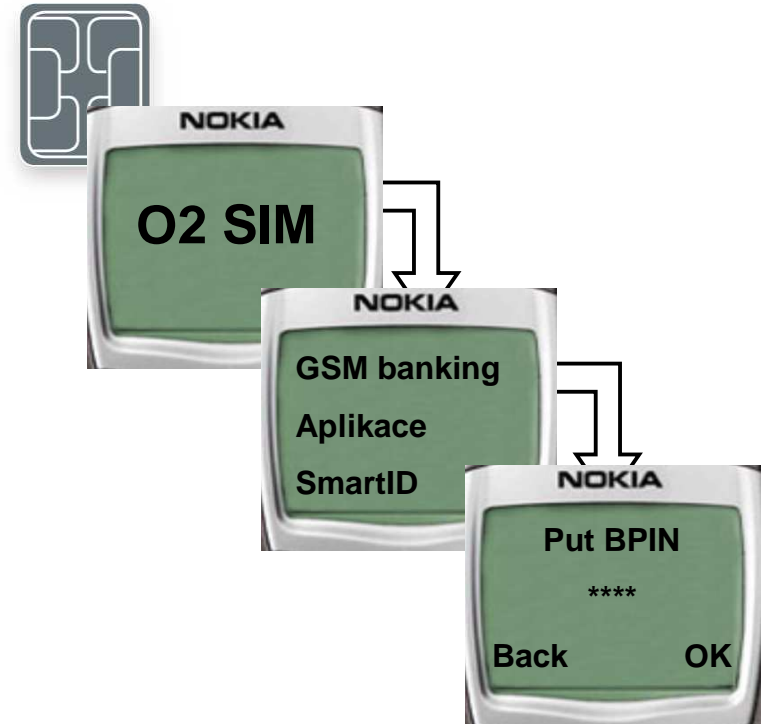


Source: Gartner (April 2006)

192254-1

But the SIM-knight protects the honest men...

- There are two O2 SIM applications utilizing strong encryption
 - Via **GSM banking**, end-users can handle their account via secured SMS
 - **SmartID** is a unique general end-user's ID device in the virtual world



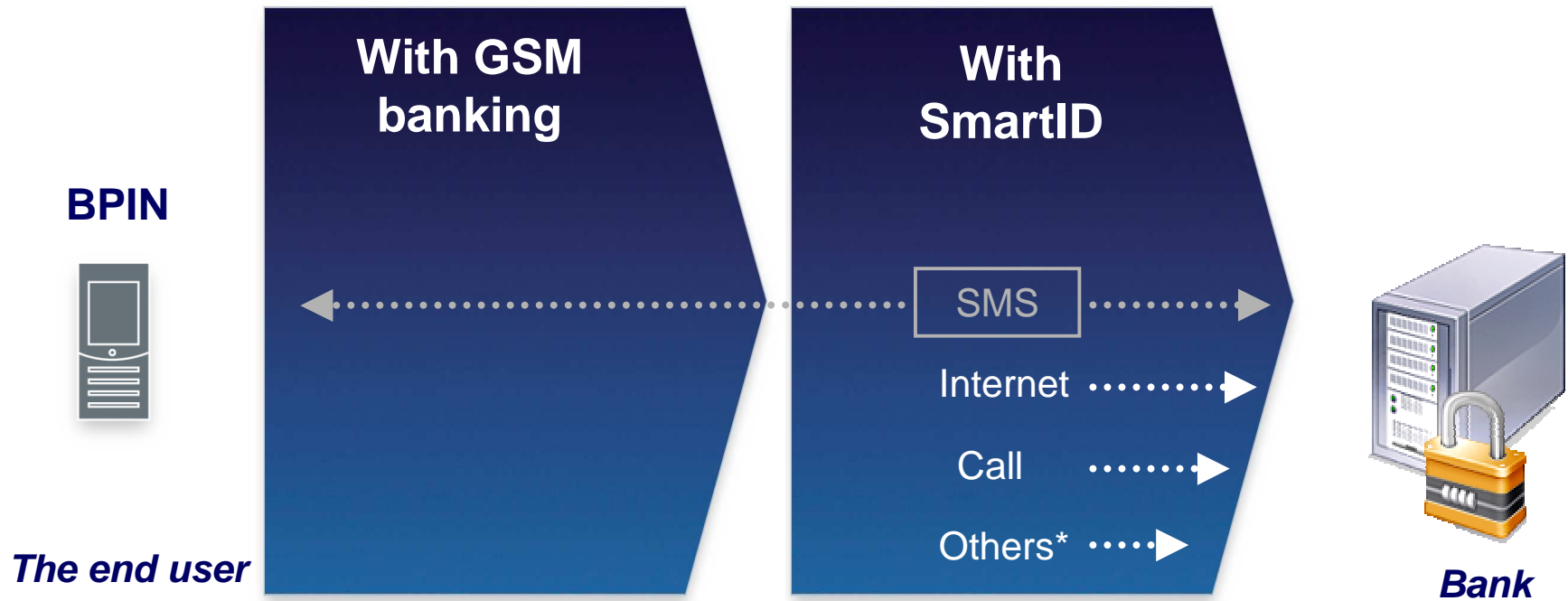
Two-factor authentication

BPIN protects access to the SIM applications

Telefonica

O₂

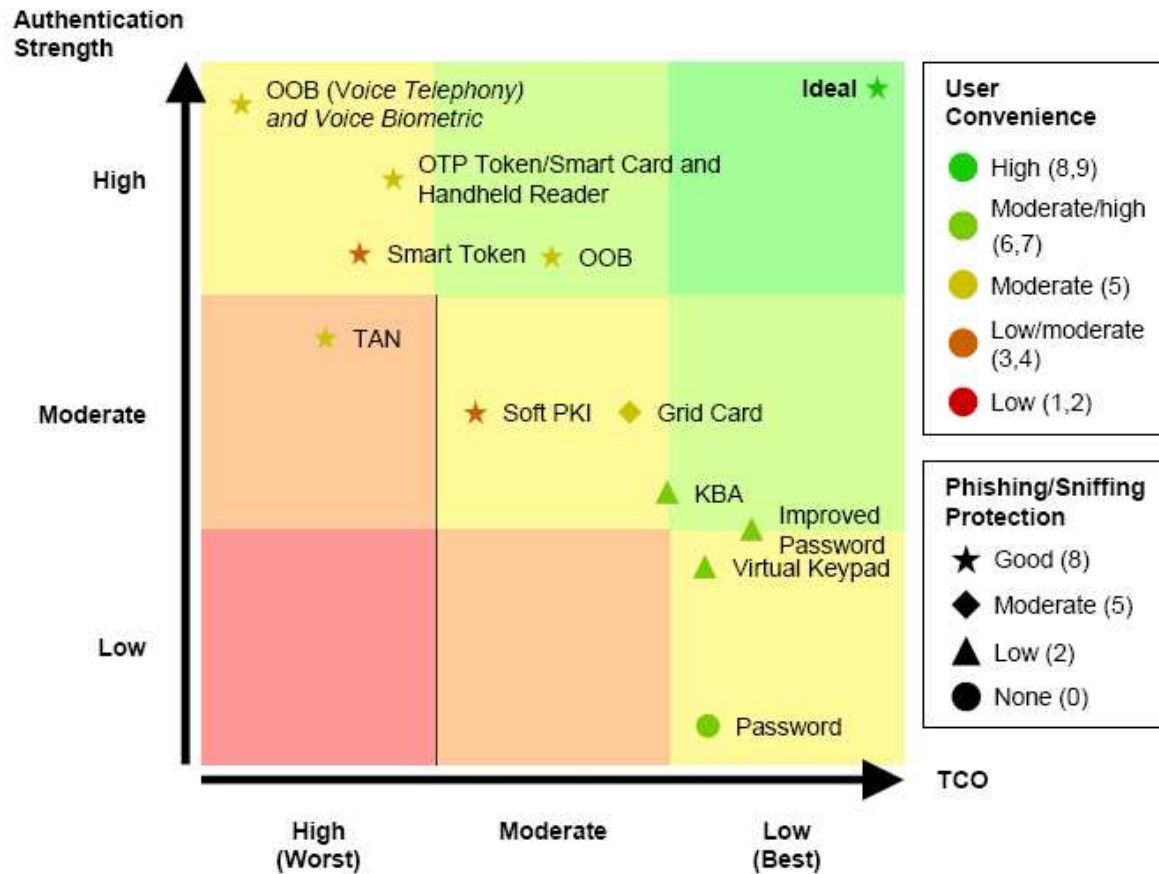
...so they can be identify everywhere!!!



* e.g. Point of Sales, ATM, terminals, Internet kiosks, etc.

Independent Gartner's survey

Figure 1. Consumer Authentication Methods Compared



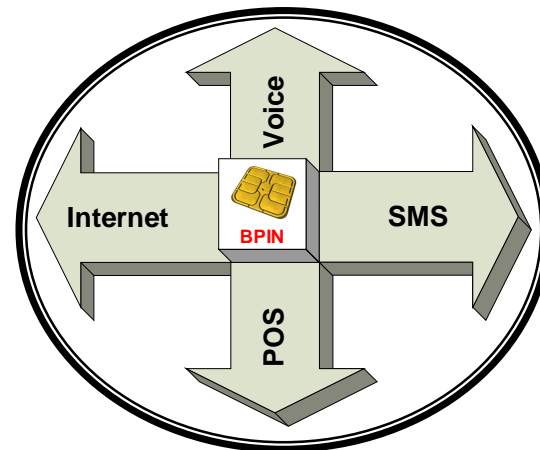
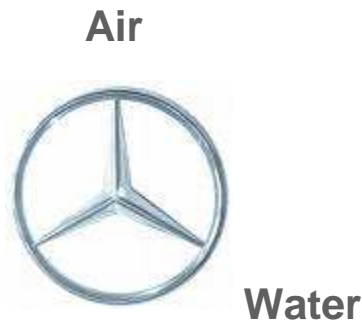
139254-1

The objective is to secure all the ways...

BPIN



- ...between the end-user & customer
 - B2B communication (company versus employees, vendors, other companies)
 - B2C communication (between customer and its “customers“)
- ...while
 - ... the end user uses SIM card
 - ... the opposite side uses authentication server



SIM creates a discreet SMS tunnel

SIM Toolkit is used as a user friendly interface for a SMS data interchange between the user and his service provider (e.g. GSM banking)

Customer's benefits

- Secure transaction system
- Low transaction price
- M2M data processing
- OTA provisioning

User's benefits

- "I can manage my services anytime and anywhere under GSM signal
- GSM banking utilization
 - Money transfer, balance check, Prepaid recharging, etc.



SIM protects services at Internet portal

Application generates and displays a dynamic codes (One Time Password) for a portal access. At the same time is serves as a tool for confirmation of user's requirements

Customer's benefits

- Independent on GSM signal
- Very low or even zero transaction price
- OTA management
- Lower cost related to compete technologies

User's benefits

- "I can manage my services through Internet anytime and anywhere"



Smart calls to Customer care or HelpDesk

The user doesn't have to remember provider's CC call number and he doesn't have to identified himself anymore during the call. OTP is a dynamic part of the called number

Customer's benefits

- Cost per operator's per 1minute=1€
- Average time of identification id 30-40 sec (saves operator's time)
- Today 4% of all calls have to be cancelled due to the fact that user is not able to provide valid identification data to an operator

User's benefits

- BPIN is my authentication
- Zero chance to pass bad value to a CC operator



Summary

- SIM
 - Is OTA (Over the Air) configurable
 - Is a smart card
 - Smart cards are generally considered as a secure HW
 - BPIN protecting application fulfills 2-factor authentication requirement
- Handset
 - Is a terminal including keyboard and display
 - Mobile is the only thing a man is willing to return back for
 - in case he forgets it at home
- Lifecycle period
 - Handset -> one Xmas
 - SIM -> many years

Conclusion

SIM is the hottest candidate as a general identification tool at all

Thank you

vladimir.kajs@o2.com



Telefonica

O₂