Secure Access Control over Wide Area Network - IKTPLUSS Project SWAN

Raghu Ramachandra, Martin Stokkenes, Pankaj Wasnik, **Christoph Busch**

Norwegian University of Science and Technology - Gjøvik
http://www.christoph-busch.de

Finse Winter School - April 26, 2016

Norwegian Biometrics Laboratory (NBL)

- Faculty-Members:
  - Christoph Busch
  - Patrick Bours
  - Bian Yang
  - Faouzi Alaya Cheikh
  - Sule Yildrim
  - Erik Hjelmås
  - Raghu Ramachandra
  - Katrin Franke (adjunct member)
  - Ivar Farup (adjunct member)
  - Mohammad Derawi
- PhD-Students:
  - Ctirad Sousedik
  - Edlira Martiri
  - Guoqiang Li
  - Kiran Raja
  - Martin Olsen (graduated)
  - Martin Stokkenes
  - Nabeel Al-Bahbooh
  - Patrick Schuch
  - Soumik Mondal (graduated)
  - Marta Gomez (guest)
  - Pankaj Wasnik

- Key-factors::
  - Since 2008, 6 EU FP7 projects,
  - 2 Norwegian funded project
  - 1 US-government funded project
  - 2 research projects with the German BSI
  - 4 industrial projects,
  - cooperated with > 30 research partners
  - approx 140 peer-reviewed publications

Outline

- Introduction to SWAN
- Consortium
- Project idea
- Content of the research

The SWAN Project

SWAN - Secure Access Control over Wide Area Network

- IKTPLUSS program
- October 2015 - September 2019
- Funding of 23.055.000 NOK
- Partners from 4 European countries

The SWAN Consortium

Partners:

- Norwegian Biometrics Laboratory (NBL)
  @ Gjøvik University College (GUC)

- Department of Informatics @ University of Oslo
- Morpho, France
- Institut de Recherche Idiap, Switzerland
- Association of German Banks, Germany
- Zwipe AS, Oslo

Sponsor: IKTPLUSS

The SWAN Consortium

Partners:

- Norwegian Biometrics Laboratory (NBL)
  ~~@ Gjøvik University College (GUC)~~
  @ Norwegian University of Science and Technology (NTNU)
- Department of Informatics @ University of Oslo
- Morpho, France
- Institut de Recherche Idiap, Switzerland
- Association of German Banks, Germany
- Zwipe AS, Oslo

Sponsor: IKTPLUSS

The Research Council of Norway

Project Idea

Access Control

Authentication can be achieved by:

- Something you know:
  Password, PIN, other secret

- Something you own:
  SmartCard, USB-token, key

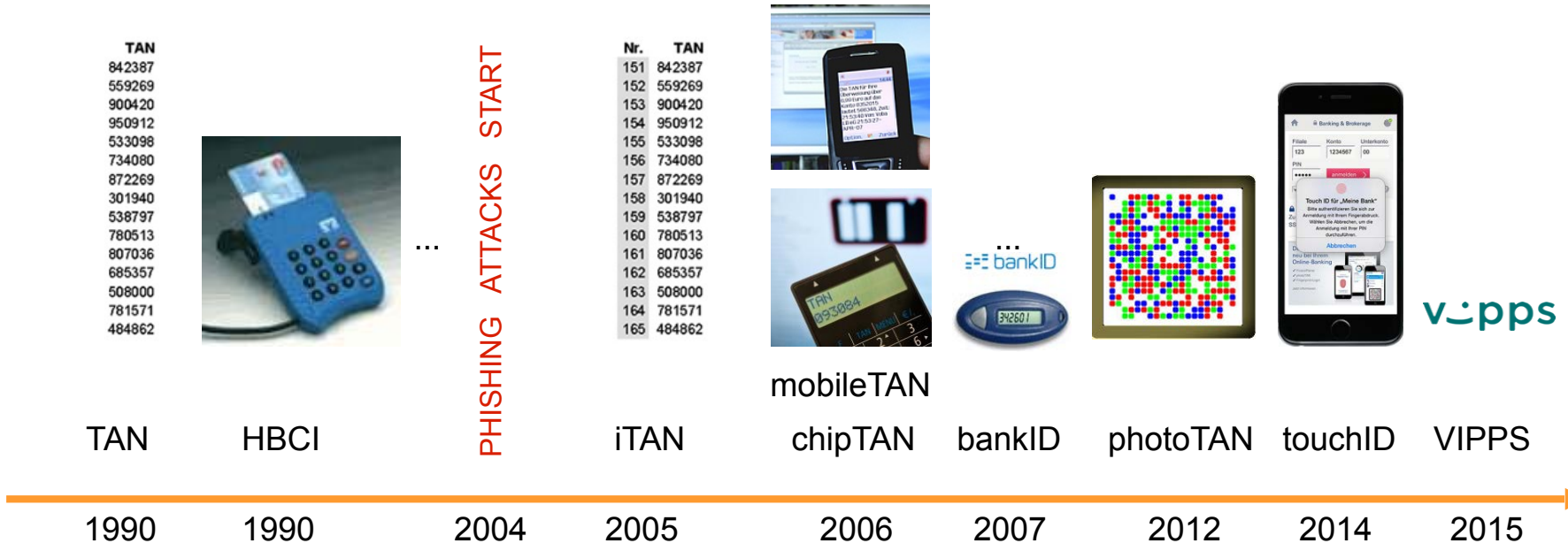
- Something you are:
  Body characteristics

Something you know or own
you may loose, forget or forward to someone else,
with biometrics this is more difficult.

- security policy not violated by delegation
- non-repudiation of transactions
  „This was initiated by *Igor Popov* misusing my card“

Access Control in the Banking Environment

A European perspective



Inspired by: BdB (2015)

Smartphone Access Control

Foreground authentication (user interaction)

- Deliberate decision to capture (willful act)
- Camera-Sensor
  - Fingerprint recognition
    - Apples iPhone 5S / Samsung Galaxy 5
    - Fingerphoto analysis
  - Face recognition
  - Iris and eye recognition
- Touchpad: allows signature recognition

Image Source: Apple 2013

Background authentication (observation of the user)

- Microphone
  - Speaker recognition
- Accelerometer
  - Gait recognition
  - concurrent - unobtrusive

Security ?

Operators will think:

„*The biometric sensors must be robust against fake attacks*“

Privacy Protection - Sensitive Data ?

Operators will think:

„Biometric systems must be compliant to data privacy and data protection principles“

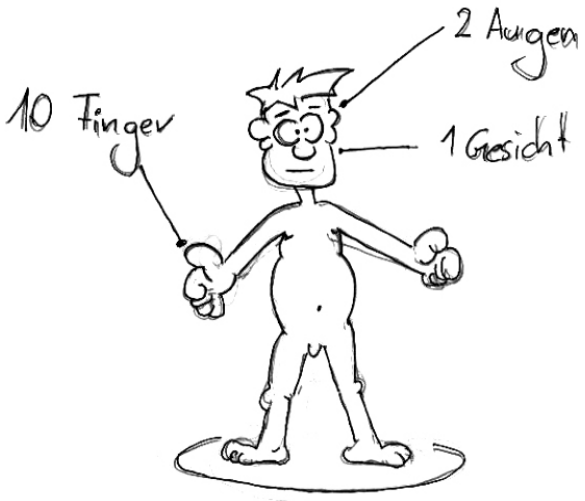
Wart Fingerprint

Source: TU Brno, 2013

Privacy Protection - Revocability?

Data subjects may think:

„The number of biometric characteristics is limited (e.g. we have only 10 fingers) - we can not revoke the biometric reference“



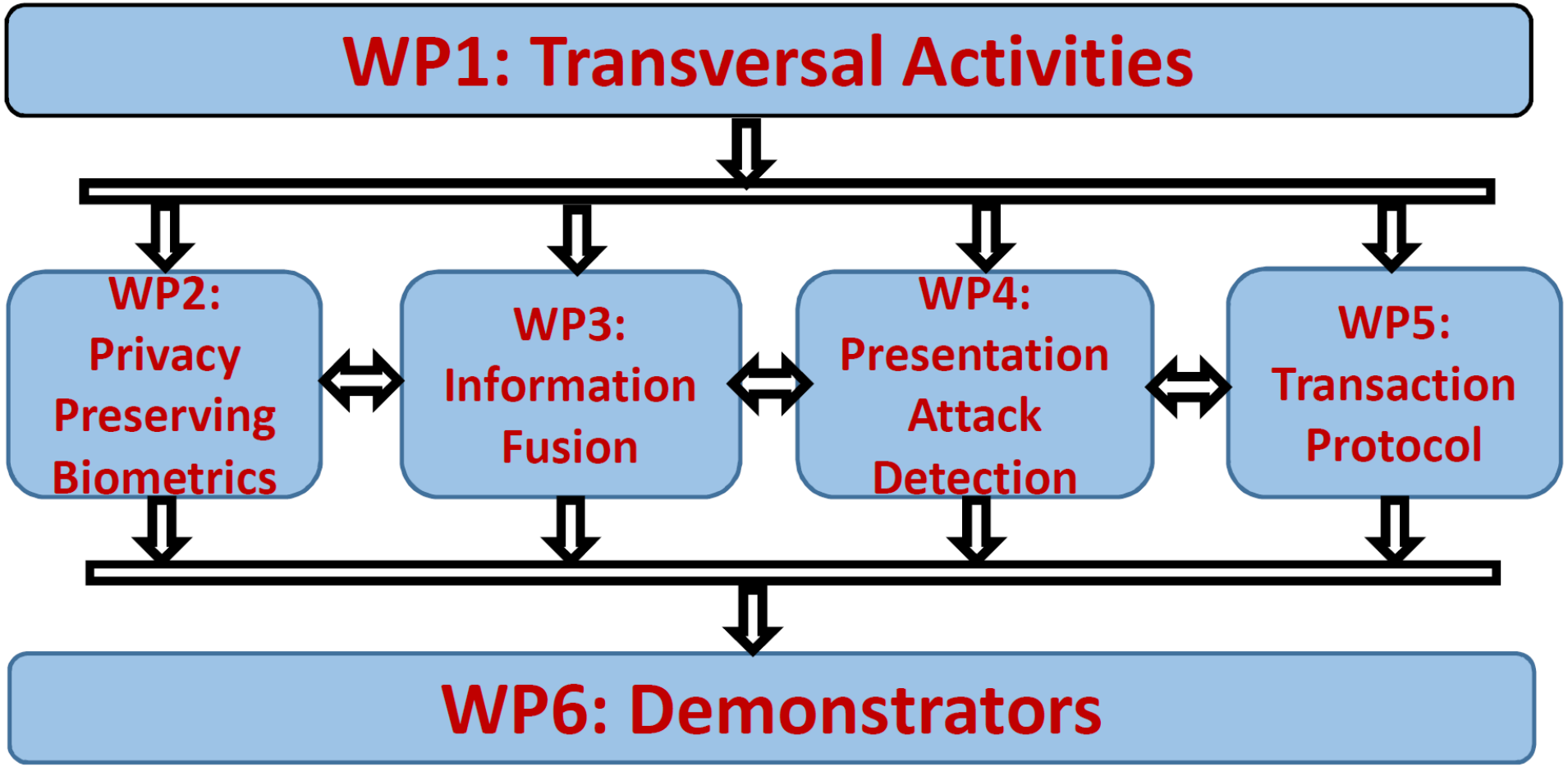
SWAN

Objectives

- To develop and demonstrate biometric solutions that are fast, trustworthy and secure for real-time authentication of individuals at banking transactions.
- To enable privacy-preserving bank transaction authentication protocols over wide area network with a privacy-by-design approach.
- To study vulnerabilities and limitations of the biometric modalities such as a 2D face, fingerprint, eye, and voice
- To develop transaction authentication protocols using biometrics that can overcome the need for centralized storage of biometric data.

SWAN

Work Structure



Conclusion

Biometrics is possible with todays smartphones

- a multi-biometric authentication scheme with scaling factors is a good choice with respect to security threats

Biometric standards are available

- financial transaction schemes should follow privacy standards

SWAN follows the two channel concept

- is based on international ISO/IEC standards
- is privacy friendly as no biometric reference is stored on a banking server

More and detailed information on SWAN at:

http://nislab.no/biometrics_lab/swan

http://www.christoph-busch.de/projects-btap.html

Contact

Contact:

NTNU

Prof. Dr. Christoph Busch

Norwegian University of Science and Technology
Computer Science Department
Teknologiveien 22
2802 Gjøvik, Norway
Email: christoph.busch@ntnu.no
Phone: +47-611-35-194