Biometrics and mPayments

Christoph Busch

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

Identitet 2016

Oslo - February 11th, 2016



Biometric Capture Device and Reference Data

Biometric Capture Device Smartphone

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 recognition
- Touchpad: allows signature recognition
- Background authentication (observation of the user)

Ĵ

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



Image Source: Apple 2013

Biometric Smartphone and national ID-card

It won't take long

 that NFC enabled Smartphones will interact with doors and RFID chips (i.e. national ID-card)



- Short range wireless communication at 13,56 MHz
 - based on RFID standard (ISO/IEC 14443)
- Operating in proximity distance up to 20 cm

Biometric Capture Device Token

A secure Biometric-Transaction-Device (BTD) which is quasi a Biometric Secoder



- Trustworthy hardware (e.g. Common Criteria evaluated)
- Can not be manipulated by malware
- can capture a biometric characteristic
- Can establish a reliable communication to an Online-Banking-Server (OBS)

Levels of Security

EU Directive on Payment Services

Directive established in November 2015



http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=EN

Christoph Busch

EU Directive on Payment Services

Directive established in November 2015

- Article 97 defines Authentication
 - I. "Member States shall ensure that a payment service provider applies strong customer authentication where the payer:
 - (a) accesses its payment account online;
 - (b) initiates an electronic payment transaction;
 - (c) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses."
 - 3. "... Member States shall ensure that payment service providers have in place adequate security measures to protect the confidentiality and integrity of payment service users' personalised security credentials."

EU Directive on Payment Services

Directive established in November 2015

- Article 97 defines Authentication
 - 2."... Member States shall ensure that, for electronic remote payment transactions, payment service providers apply strong customer authentication that includes elements which dynamically link the transaction to a specific amount and a specific payee."
- Article 98 Standards for Authentication and Communication
 - 2."... standards shall be developed by EBA ... ensure an appropriate level of security for payment service users and payment service providers ..."

Why multiple Modalities?

Financial Transactions

Level of Security

number and strength of biometric factors should scale with transaction volume



[Gru2015] W. Grudzien, "Current trends in the payments and transactions landscape" Bundesverband Deutscher Banken, October 2015

Christoph Busch

Level of Biometric Security

Levels of Biometric Security

Three factors can be considered - robustness again the following attacks

- Zero-effort impostor attack: algorithm errors (False Match)
- Attacks on the biometric capture device
- Attacks on the stored reference data

Zero-effort impostor attack

False-Match-Rate (FMR)

- proportion of the completed biometric non-mated comparison trials that result in a false match
- Note: non-mated comparison trials are also referred to as impostor trials

$$FMR(t) = \int_{t}^{1} \Phi_{i}(s) ds$$



Attacks on the Biometric Capture Device

Presentation Attacks



Gummy Finger Production in 2000 !

Attack without support of an enroled individual

- Recording of an analog fingerprint from flat surface material
 - > z.B. glass, CD-cover, etc.with iron powder and tape
- Scanning and post processing:
 - Correction of scanning errors closing of ridge lines (as needed)
 - Image inversion
- Print on transparent slide
- Photochemical production of a circuit board mold



[ZWI2000] A. Zwiesele et al. "BioIS Study - Comparative Study of Biometric Identification Systems", In: 34th Annual 2000 IEEE International Carnahan Conference on Security Technology, Ottawa, pp. 60-63, (2000)

Christoph Busch

Gummy Finger Production in 2000 !

Reported in a publication by the German Federal Police

 A. Zwiesele et al. "BioIS Study - Comparative Study of Biometric Identification Systems", In: 34th Annual 2000 IEEE International Carnahan Conference on Security Technology, Ottawa, pp. 60-63, (2000)

BioIS Study

Comparative Study of Biometric Identification Systems

A.Zwiesele, BKA Wiesbaden¹ - A.Munde, BSI Bonn² Dr. C.Busch, H.Daum, IGD Darmstadt³

Abstract

On 1st April 1999, after a preparatory phase lasting more than twelve months, work on the a.m. BiolS Study finally commenced. This study was initiated by the Federal Criminal Investigation Office of Germany (BEA) in close cooperation with the German Information Security Agency (BSI). The study was executed by the Fraunhofer Institute of Graphical Data Processing (IGD).

The study includes a field investigation, in which 11 physiological (static) and behaviour-specific (dynamic) systems, which were available and supported in Germany, were installed and put into operation in a defined scenario. The field investigation was conducted with approximately 40 users representing different age, employment, educational and ethnic groups.

The main objectives of the field investigation are as follows:

- To gather experience with the biometric systems and to identify any weaknesses that need to be examined in greater depth during the future course of the study.
 To obtain statistical information regarding the frequency with which authorised users
- To obtain statistical information regarding the frequency with which authorised users are rejected by the various systems. This information will then be taken as a basis for establishing the existence of certain user groups which individual systems have difficulties in identifying. In the event that such groups do exist, the possible reasons for their rejection need to be examined. To observe the behaviour of the users over a prolonged period of time, in order to establish whether on out any changes can such a stronger the second stronger can be able to be able to be able to be the second stronger to be able to be a

a prolonged period of time, in order to establish whether or not any changes can be observed. There might, for instance, be a certain familiarisation effect, which is reflected in a change in the rejection rate.

The field investigation is to be followed by a further technical study phase, designed to investigate the following points:

> Federal Criminal Investigation Office of Germany German Information Security Agency Fraunhofer Institute of Graphical Data Processing

0-7803-5965-8/00/\$10.00 @2000 IEEE

4.) Dupability: The aim of this part is to analyze and assess the effort that is necessary to dup biometric systems. It not only covers the systems taking part in the study, but also examines their respective functional principles independently of their technical implementation.

 Influence of the various programmable system parameters: This part attempts to investigate the represensations of the various system setups for the identification attributes. The findings are intended to permit recommendations to be made regarding the prefered settings for each of the biometric systems under investigation.
 Influence of the various environmental factors on the identification reliability of the system of the identification reliability of the system.

the systems: The purpose of this part is to determine the repercussions of changes in environmental conditions for the identification attributes. One example of such factors might be the way in which different lighting conditions affect the systems' ability to recognise faces.

The study was completed on the 15^{th} of May 2000. It is the aim of this lecture to inform the audience of the results of the study and the knowledge which could be gained.

Introduction

"In comparison to PINs and passwords, a biometric signature has crucial advantages and provides an unambigous proof of dentity..." "Comprehensive empirical tests are being conducted to get rid of the last doubts and insecurities from the angle of consumer and data protection..." "Widespread employment of biometric systems just around the corner..."

...that is what the manufacturers are promising, but as a study by the Federal Criminal Investigation

Liveness Detection

ISO/IEC 30107-1:2016 Presentation Attack Detection

Attacks on Biometric Systems



Source: ISO/IEC 30107-1

nspired by N.K. Ratha, J.H. Connell, R.M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," IBM Systems Journal, Vol 40. NO 3, 2001.

Attacks on the Biometric Sensor

ISO/IEC 30107 - Biometric Presentation Attack Detection Scope

- terms and definitions that are useful in the specification, characterization and evaluation of presentation attack detection methods;
- a common data format for conveying the type of approach used and the assessment of presentation attack in data formats;
- principles and methods for performance assessment of presentation attack detection algorithms or mechanisms; and

Outside the scope are

- standardization of specific PAD detection methods;
- detailed information about countermeasures (i.e. anti-spoofing techniques), algorithms, or sensors;
- overall system-level security or vulnerability assessment.

Definitions in ISO/IEC 30107 PAD - Part 1: Framework

presentation attack



presentation to the biometric capture subsystem with the goal of interfering with the operation of the biometric system

 presentation attack detection (PAD) automated determination of a presentation attack

Definitions in ISO/IEC 2382-37: Vocabulary

http://www.christoph-busch.de/standards.html

impostor

subversive biometric capture subject who attempts to being matched to someone else's biometric reference

• identity concealer

subversive biometric capture subject who attempts to avoid being matched to their own biometric reference

ISO/IEC 30107 - Definitions

presentation attack instrument (PAI) biometric characteristic or object used in a presentation attack

artefact

artificial object or representation presenting a copy of biometric characteristics or synthetic biometric patterns

Types of presentation attacks



ISO/IEC 30107-1 Examples of Artificial and Human Attack Presentation

Complete	gummy finger, video of face
Partial	glue on finger, sunglasses, artificial/patterned contact lens
Lifeless	cadaver part, severed finger/hand
Altered	mutilation, surgical switching of fingerprints between hands and/or toes
Non-Conformant	facial expression/extreme, tip or side of finger
Coerced ¹	unconscious, under duress
Conformant	zero effort impostor attempt
	Complete Partial Lifeless Altered Non-Conformant Coerced ¹ Conformant

Biometric framework with PAD



Source: ISO/IEC 30107-1

Christoph Busch

ISO/IEC IS 30107-1 Standard

now available in the ISO-Portal

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=53227

	Online Browsing Platform (OBP)
ISO	☆ Search BO/IEC 30107-1:2016(en) ★

ISO/IEC 30107-1:2016(en) Information technology — Biometric presentation attack detection — Part 1: Framework

able of contents	
Foreword Introduction 1 Scope	Foreword
 2 Normative references 3 Terms and definitions 4 Symbols and abbreviated terms 5 Characterisation of presentation attack 5.1 General 5.2 Presentation attack instruments 6 Framework for presentation attack dete 6.1 Types of presentation attack dete 6.2 The role of challence-response 	ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see <u>www.iso.org/directives</u>).

Christoph Busch

Presentation Attack Detection - Testing

Testing Methodology in ISO/IEC 30107 Presentation Attack Detection - Part 3: Testing and reporting

- Security Evaluation
 - For evaluations using the Common Criteria Framework
 - Protection Profile (PP) (e.g. from German BSI)
 - Security Target (ST)
 - Evaluation Assurance Level (EAL)
 - Assessment of the attack potential
 - "if there is at least one artefact that can reproducibly successful attack the PAD-component - then the PAD failed the test"
- Other approaches
 - for evaluations in academic and technology development
 - tolerating the fact that statistical distribution for small tests is unknown and for sure not normal
 - , a score based metric can tell us, if the method improved"

Presentation Attack Detection - Testing

Definition of harmonized metrics in ISO/IEC 30107-3

- Attack presentation classification error rate (APCER) proportion of attack presentations incorrectly classified as normal presentations at the component level in a specific scenario
- Bona fide presentation classification error rate (BPCER) proportion of bona fide presentations incorrectly classified as attack presentations at the component level in a specific scenario

Smartphone Access Control - with PAD

Eye recognition study - 2015

 Presentation Attack Detection (PAD) videos on iPhone 5 S and Nokia 1020



- Method based on Eulerian Video Magnification (EVM)
 - Normalized Cumulative Phase Information

Smartphone Access Control - with PAD

Method based on Eulerian Video Magnification (EVM)



[RRB2015] K. Raja, R. Raghavendra, C. Busch: "Video Presentation Attack Detection in Visible Spectrum Iris Recognition Using Magnified Phase Information", in IEEE Transactions on Information Forensics and Security (TIFS), June, (2015)

Christoph Busch

Smartphone Access Control - with PAD

Eye recognition study - 2015

- Method based on Eulerian Video Magnification (EVM)
 - Normalized Cumulative
 Phase Information
- Zero Error Rates:
 - APCER = 0 %
 - BPCER = 0 %



[RRB2015] K. Raja, R. Raghavendra, C. Busch: "Video Presentation Attack Detection in Visible Spectrum Iris Recognition Using Magnified Phase Information", in IEEE Transactions on Information Forensics and Security (TIFS), June, (2015)

Contact

Contact:

