



Need and perspectives to realize liveness detection

IBPC 2012, March 9th@NIST, Gaithersburg

Ralph Breithaupt, BSI Federal Office for Information Security





- 1. "Fakes are not always a bad thing..."
- 2. BSI strategy regarding spoofing
- 3. Challenges in Vulnerability Assessment
- 4. Open questions & To-Do-list



Federal Office for Information Security





1. "Fakes are not always a bad thing..."





- In 2011 Bavarian police asked BSI for assistance in the investigation of a bombing attempt
- The suspect stored valuable information on his new mobile phone equipped with newest biometric protection
- Provided with his fingerprints it was easy to break the biometric protection in the first attempt
- Unfortunately the police did not keep the phone charged
 ⇒ the booting process still required both pincodes!
 We had to resort to our standard methods.

Lessons learned:

- always keep confiscated phones charged !
- raise awareness !:
- "Security is often cited as the biggest impediment to the broad adoption of mobile wallets, and we believe our jointly-developed NFC reference designs will give consumers greater confidence that mobile wallets are not only an easier way to pay but are much more secure than other means," *added AuthenTec CEO Larry Ciaccia*





3. BSI – strategy regarding spoofing

1. Threat Assessment

continuously collect & develop attack methods, "State of the Art" -Tests

Fake-attacks

2. Countermeasures

development of fake detection technologies, close contact to manufacturers

3. Tests & Certification

development of test & certification methodologies, international standardization



2.1 BSI-strategy: 1. Threat Assessment

since 2007 (LF I & II):

- collecting & evaluating publicly known fakes
- development of new fake types
 - \rightarrow BSI-Fake-Toolbox
- Vulnerability analysis of:
 - relevant finger-scanner-technologies
 - relevant finger-scanners with fake-detection
- Knowledge exchange & cooperation with manufacturers, laboratories, universities, police departments and other governments
- Testing service for manufacturers





2.2 BSI-strategy: 2. HW-Countermeasures

New approaches for secure fingerprint scanners:

BOTTOM-UP: "Lifefinger III"



- Improvement of the "state of the art" with additional sensors
- Basis: newest FP-scanner with high level SD
- Multimodal combination of liveness
 & selected skin properties detection

TOP DOWN: "3D-OCT-Finger"



- complete scan of the finger in 3D with up to 3000dpi w. 1,5mm depth
- detection of various anatomical skin features - all at once
- combinable with liveness detectors





2.2 BSI – strategy: Lifefinger III – Results



a) original FAR of LF1 b) FAR of LF1 + new sensors With alternative fusion: FAR = 0.0%, FRR = 1,41% ! ()



"Development of a new sensor type that detects" many skin and FP properties at the same time"





- detailed 3D-measurement of the finger up to a depth of 1,5mm with "Optical Coherence Tomography" (OCT) [standard medical instrument for iris & retina]
- Resolution of up to 12µm in all 3 dimensions (small scanning area and low speed in 1st project)
- Detection of the fingerprint structure on the surface and in deeper layers (epidermis-dermis barrier). Comparison of both $FP \Rightarrow$ detection of thin & full finger fakes!
 - detection of sweat producing spiraling tubes + many more



Federal Office







2.2 BSI - strategy: OCT-Finger results



- OCT shows a very high potential for SD
- However the results did not meet the expectations, due to:
 - a relatively high number of faulty measurements
 - filters and classificators could not be optimized
- Main issues were:
 - huge amount of data
 - very high complexity of filters/classificators (many different approaches at once)
 - The computational needs were too high for parameter optimization and practical use (5d for 1 evaluation of all ~5000 measurements!)

 OCT-CUDA: Massive parallel data analysis on GPUs – Speedup of ~40+ (<1 sec)



2.3. BSI-strategy: Certification of Spoof Detection

 international basis for the comparison of spoof detection solutions

The makenal of the second	
Deutsches M TT-Sicherheitszer	rtillkat monordum
85-452-0643-2009	
IBO 21001 Certificat auf der Basis versift-Grundschwitz	P Later
Informationeverbund des Kammunalen Rachenzentrums Minden Rausmitiens/Liepe	
gung bie drido data	
Der Driteitundeurgegenmlahl ist der beformationserbund des Ramm Revendengslagen (RRC) in Lange. Dieses Sodern besticht sich auf de Rechnisterbundt, sie leibter gemeinden oder für Auches zur Verlagung Systemis erbeitunde bei die der Bertreitunden RZ in bestehetung.	natulner Reutersambures Minden en velledindigen Detheb des 5 janliertikes Anwendungen oder IT-
Our steer autgeführte Untersuchungsgegensteend wurde verst Frank der 193 27507 Auflie auf der Basis von 17 Geunalentes, in Dierententieren des Burchsamtes für Sicherheit in der Internationspraches gegent, die Schlaufingerungen des Aufliche Burtiste und des erforte Internation	fan Stamm, Icancindor Audior far ang mil dem Zahlfebrumposhema e in Auditeordt orthofismel Na fantisme
De clarité divers Zachilles bestations avantations anno 500 27161 sur la de Mahahmetante un Mahahmet aux Annu A ven 100462 310 Anardelige ou Umentany aux Alabelanges de algement aven sonne Desse Jachilles de la Mahahmetante aux Annu A de Dessentations Desse Jachilles et teams generate Landrina de Dessentations Barter de la Mahahmetante de la Mahahmetany fait en la Barter de la Mahahmetante de la Mahahmetany fait en la Barter de la de la children and annual de la desse de la de la children de la de la desse de la desse de la de la de la de la desse de la desse de la desse de la de la de la de la desse de la desse de la de la de la de la de la desse de la desse de la de l	er Beser von Er-Grundborutz umfaltet 61.5000 undrächt demit entransferen vordernen einer Kortike Zulick zum Fri- gentlanden durch zum Bunchesamt für immelhangegennistent durch dass in ochr Jum euserstette patristoret.
dem volotiedigen Zenifgen, romport.	
Bures, 17. Marc 2001 Burdesent for Sicherteit in der internationationsk	
In Adding	
 Unter der Bedregung dass die ab 31 2012010 juhlich durch prolitiken Englisies abgröchlissen werden. 	uternen Gerenburgunte mi
Residences for Section 44 and the Section 44 and 50	and and a second strategy
Prove +48 (RC28 08000 Fee +48 (RC28 080-0471 - bene	···· 0.021-030-01

- support for vendors of biometric devices to:
 - reward their existing efforts in spoof detection development
 - encourage further development in that area
- setting a starting point for international standardization & cooperation (& competition) in that area to make biometrics continuously more secure & trustworthy
- a CC-certificate is one possibility to define & to demand a certain standard of reliability



2.3. BSI-strategy: Common Criteria-first results

Construction Construction	
Deutsches mit TrSicherheitszertillkat	
55-102-0143-2809	
180 21201 Certifical auf der Basis vers 17.6hverbeheite	
Informatione-verbund des Kommunalen Rechenzentrums Minden-Ravemberg/Lippe	
gallig bie 3100 3912	
Der Dittelschurgspejendarb in der Mittelsanderschund der Rümesander Rechmanscher Minister Rechmangslages (PKI) in Lenge, Desse Sotien besteht sich auf den untersindiger Obliet des Normanisterung zur der Der Samitiker der Ert für Auflichen zur Vinfligung peletien Anwendungen oder ET- Spelerte Ferdünftlich der darbe mittelsamber ID Interationaum.	
Oer ober sulgeführe Untersuldurungsgesindere wurde verit Frankreiter Stann, Executive Audor tar 192 2100 - Audio auf der Basie voll. 7 Generalische ist Demissionenung wir der Zheitgemagnationen des Burdenannes für Schurchel in der Internationenschnick gesetzt. Die im Austreacht ochsatissen	
Benefamper regin our constraints text on an annual part of the constraints of the Constra	
Debtel Zwittlind gill dur für den angegebenen Untersuchungsgegendand und nar im Zausenrienkung mit dem volksindigen Zertifisierungsreport.	
Barris, 17, May 2008	
in Advag	
Banka (
 Unter der Bechgung, dies die ab 12 2020 j	
Residence for both that is no the method state. Endnamy Also the field of the first is a second state of the first term	

- two dedicated Protection Profiles (PPs) have been developed to address the specific characteristic of spoof detection devices
 - The first PP (FSDPP_OSP) is based on Organizational Security Policies and focuses on a pure functional test of the biometric spoof detection
 - The second PP (FSDPP) defines a dedicated level for vulnerability assessment (based on EAL 2) in order to describe an entry level into the classical assurance packages
- Both PPs are published on CC- & BSI- websites
- An evaluation methodology has also been developed but not yet published (FSDEG_V2.1 by TÜV-IT)





3. Challenges in Vulnerability Assessment

SD in biometrics is something completely different in the field of CC

- testing with fakes means "dirty" handy work
- automated tests are barely possible
- Knowledge of possible attacks is always incomplete and constantly growing
- In the information-/Youtube- age one easy golden fake is enough to undermine the security of a device in general
- Functionality Tests = Vulnerability Tests
- no known complete statistical model/foundation for tests
- successful fakes today are cheap and can be made / used without much expertise (low effort)





3. Challenges in Vulnerability Assessment

Doing the numbers game:

- Standard security level for VTs in CC: 99,99..%!!!
- → Huge number of tests are necessary for a clean statistical analysis:

e.g.:

40 fake-materials *

5 additives *

mixture recepies with other materials [2c](10) *

mixture ratio variants (10) *

physical parameter variants [thickness] (10) *

fake type variants (30) * [rule of 30, CI of 95%]

= 200,000 fake types 6,000,000 tests! we need a different approach!





3 Challenges in VT: BSI approach

BSI focused on certification of solely the SD component

- can be used as an additive in the certification of a biometric system
- can be transferred to other biometrics easier

worst case assumption:

- always use the best kinds of fakes
- all fake types are tested separately no over all mean value
- if one fake type is "reproducibly" successful the system fails!

The **Fake-Tool-Box** is the starting basis for functional tests (has to be updated regularly! - leading to new certificates)

complete statistical analysis will not be practicable

- a reduced test setup must be fixed for comparability
- details of those tests are not known to the manufacturer





4. Open questions:

How can we reduce the necessary numbers?:

- Reducing tests by simulating parameter variants:
 - develop a feasable model of material influence out of view test samples (example: thickness)
 - automated tests may partially be possible to determine critical parameter values

How can we increase comparability?

Are there better ways to include VA in biometry in CC?



4. To-Do-List



- EU-Project B.E.A.T (FP7-SEC-2011) "Biometrics Evaluation and Testing" Standardization of SD evaluation in biometrics in general
- CCDB Supporting document on

"Characterizing Attacks to Fingerprint Authentication Mechanisms"

National Cryptologic Centre (CCN, Centro Criptológico Nacional, Spain) + ATVS University of Madrid (UAM).

- CC-Certification of FP-scanners.
- Proposal for a VA-methodology Project in ISO SC27 to support and complement the current work in SC37
- Practical cooperation within the BVAEG-group



4.3 Future Projects



Upcoming BSI-Projects 2012 - 2014:

"Face Trust"

- Vulnerability evaluation of face biometry systems against spoof attacks
- Development of new technical countermeasures for SD
- Preparation of a vulnerability assessment methodology for CC

• "OCT-Finger II"

New & optimized BSI-OCT-hardware in combination with new classifiers (with CUDA-acceleration), 10x scanning speed, higher resolution, better signal-noise ratio, bigger scanning area, etc – last development step prior to industrial prototype – parallel use for *Iris* (and *Retina*) biometry





... thank you for your attention!



Bundesamt für Sicherheit in der Informationstechnik (BSI) Federal Office for Information Security

Ralph Breithaupt Godesberger Allee 185-189 53175 Bonn, Germany

Tel: +49 (0)22899-9582- 5043 Fax: +49 (0)22899-10-9582- 5043

ralph.breithaupt@bsi.bund.de www.bsi.bund.de