Display-TAN

Secure Mobile Banking

Dr. Bernd Borchert

Problem: Mobile Banking Security

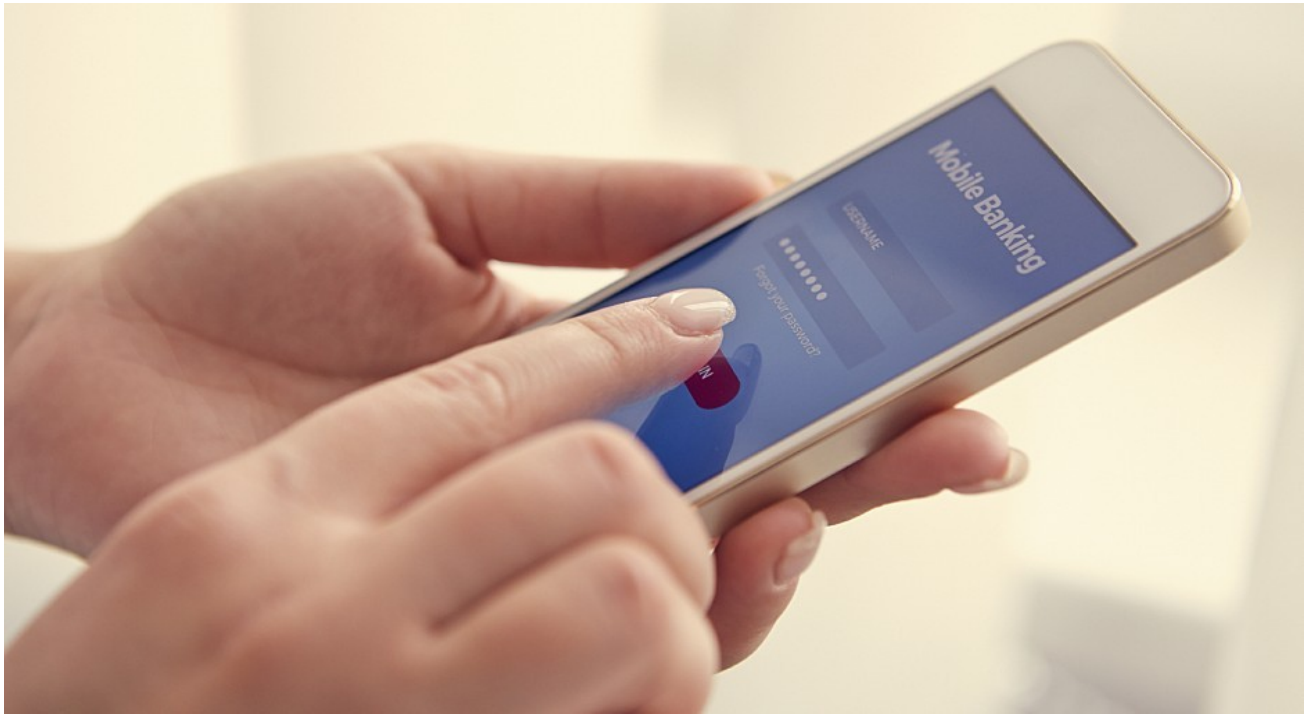
What is the problem Display-TAN claims to solve?

Mobile Banking Security

Executing money transfers on the Smartphone alone is convenient - nothing else is needed.

But it is **insecure:** Smartphone malware may have taken over the smartphone secretly and then is able to access the user credentials and to spy (or abuse) all of them:

- Password
- Secret Key
- Fingerprint
- received SMS
- etc.



After spying, the malware is able to secretly execute a malicious money transfer on its own - without the user involved.

The core problem is: it is just one device - a single trojan has access to everything.

Smartphone Malware – does it exist?

How is malware able to enter a smartphone?

The “sand-box” architecture of a smartphone may be broken via

- malicious apps
- browser drive-by
- SMS, WLAN, Bluetooth, NFC
- USB
- hardware parts
- the smartphone may already be compromised at sale.

Of course, once the malware has taken over the smartphone, it hides, so that the user is unsuspicious.

Prices for malware SDKs to be integrated into innocent appearing apps are around 20,000 Euro for Android and 500,000 for iOS.

Can't the bank app find out whether the smartphone is compromised?

The bank app has only very restricted rights, like every other app, while the malware has every right on the smartphone (the malware sits within the Operating System, which is the “master” on the smartphone - the apps are “slaves”).

Therefore, the malware can fool the app when the app tries to find out whether the phone is compromised. For example: When the app asks: “Is this smartphone rootet?” it gets from the rootet smartphone the answer: “No!”

Magnitude of the problem

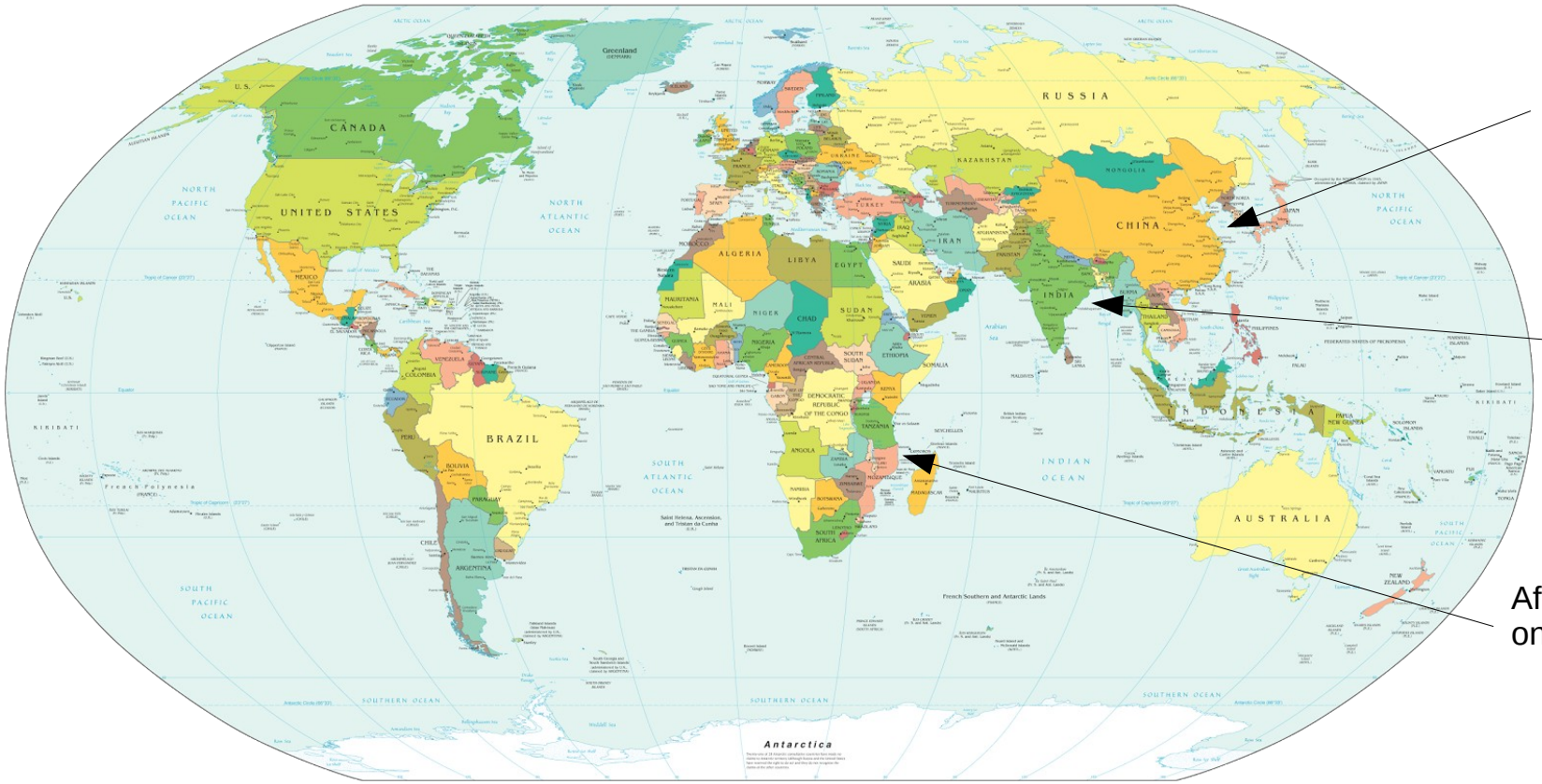
2017: ~ 3 billion existing smartphones, growing

2017: more and more people are using their smartphone for payments and money transfers, it may be a **billion** people already by now

--> soon, **2 billion** or more people will execute financial transactions on their smarpthone

--> soon, **2 billion** or more people will have the problem of potential smartphone malware fraud

--> this problem deserves a solution



East Asia (2 billion): tech-crazy

India (1.3 billion): cash forbidden

Africa (1 billion): only-mobile money

Do new Smartphone Features help?

Does Fingerprint help?

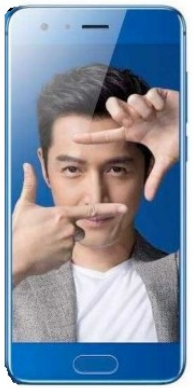
Not really. The fingerprint module is not in direct contact with the bank server – in between is the smartphone Operating System (OS) .

If the OS is infiltrated by malware, it may for example tell the bank that a fingerprint check was done and was correct, but in fact nothing was checked. The bank will accept the answer – it has no way to check what is really going on on the smartphone.

Does a Secure Element like a SIM-card help?

Not really. An infiltrated OS may send a malicious transaction to the Secure Element which then the Secure Element will sign – the Secure Element is not able to recognize that the transaction is not from the user.

Moreover, the infrastructure for SIM-cards as Secure Elements is no longer supported (Telekom and Swisskom are out, Oct. 2016)



Does anything else help?

- Selfies: too insecure – can be copied by the malware.
- SMS: well known to be insecure (forbidden for Mobile Banking by German banks association already 2009)
- Trusted Execution Environment (TEE): may help, but no infrastructure/large distribution yet.

Summary so far: An extra device is necessary to have sustainable security

Current Secure Solutions

Examples of secure solutions for Mobile Banking:

ChipTAN (Sparkasse)

Photo-TAN Device (Commerzbank)

Nice solutions, because they are really secure!

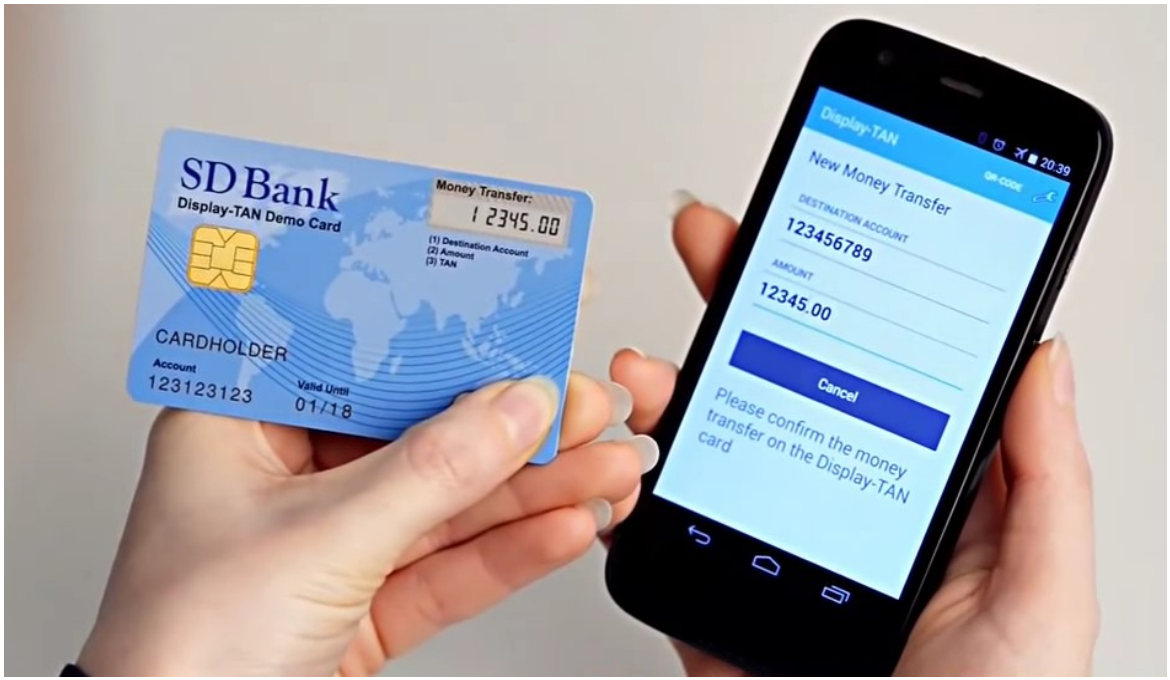
But ... problem:
The customer needs an extra device!
This is not “mobile”.

Can there be a solution? an extra device, but still Mobile Banking is “mobile”?

It seems to be impossible ...

Solution Display-TAN

Bank card with display und Bluetooth



Secure AND mobile:

- secure, because everything security-critical is done on the smartcard, not on the smartphone

- mobile, because the bank customer does not need anything more than what he carries anyway: smartphone and bank card

- Video: https://www.youtube.com/watch?v=Ge-_ApouLwk

Variant “NFC-TAN”: no display, and with NFC. No costs, but less secure, and does not work with iPhones.

Company

The company is a Spin-Off of the Computer Science Dept. of Univ. Tübingen

The product Display-TAN and its predecessor NFC-TAN (without display) were developed within a research project about Internet end-device security.

Already 2009 a patent was submitted and later granted, which suggests not to store and process the secret key within the smartphone but within a smartcard instead, which is contacted by the smartphone via NFC of Bluetooth.

The assets of the company mainly consist of

- 2 granted patents concerning the Display-TAN method
- SDK's and know-how for the rapid integration of the method into banking apps
- know-how for the integration of the method on the bank site
- cooperation with the hardware producer SmartDisplayer Inc. Taiwan

The company has basically no Marketing/Sales activity – what may explain that the Display-TAN method was not implemented at banks yet.

Business Model

The preferred business model is to involve IT Service Providers as partners: they do the implementation of a display-TAN project at a bank, while Display-TAN supplies Software SDKs and consulting for the overall architecture.

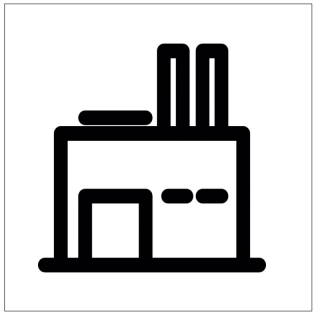
Display-TAN
Company

- Consulting
- Software
- Cards

IT Service Provider

Bank

Bank Customer



Card Manufacturer

Income is mainly measured as a percentage of the price of the smartcards.

Market

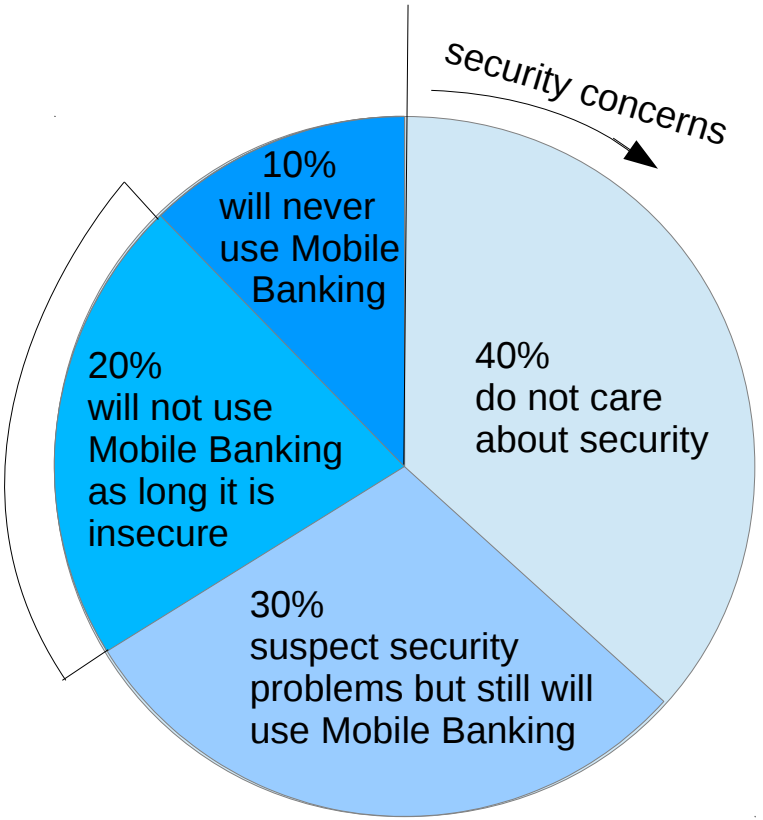
The banks contacted so far (mainly in Germany) are still hesitating to consider Display-TAN as new Mobile Banking method for them. They point out

- that their smartphone-alone solution is cheap and they can offer their customers “mobility” with that method,
- the smartphone-alone method does not have a higher fraud rate than the secure methods,
- “Bank cards are a technology of the past” – the long-term agenda is to move from the smartcard to the smartphone
- the regulators (ECB, EBA, etc.) have basically given the go-ahead for the smartphone-alone methods within their newest commentary on PSD2 from Feb. 2017.

Nevertheless, there are recent user polls which show that many bank customers have strong reservations regarding Mobile Banking because of its low security (68%, ING-Diba study from May 2017, 59% VISA study Oct. 2017), many of them won't use Mobile Banking for that reason.

Exactly this segment of the bank customers Display-TAN aims to address: The customers who are security-sensitive and/or want to execute large amount money transfers, say 5-digit sums, in a mobile fashion.

This segment may consist of 5-10% if not 10-20% of the bank customers, depending on whether they have to buy the card for the purchase price from the bank or if it is for free for them.



Bank customers (estimation Germany)