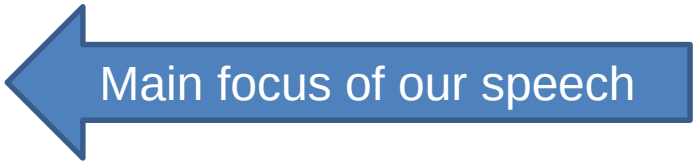
CS; SSART-Treffen, November 18, 2015

Internet Banking:
Increasing power of cyber crime

.. and what to do?

Different targets for cyber crime

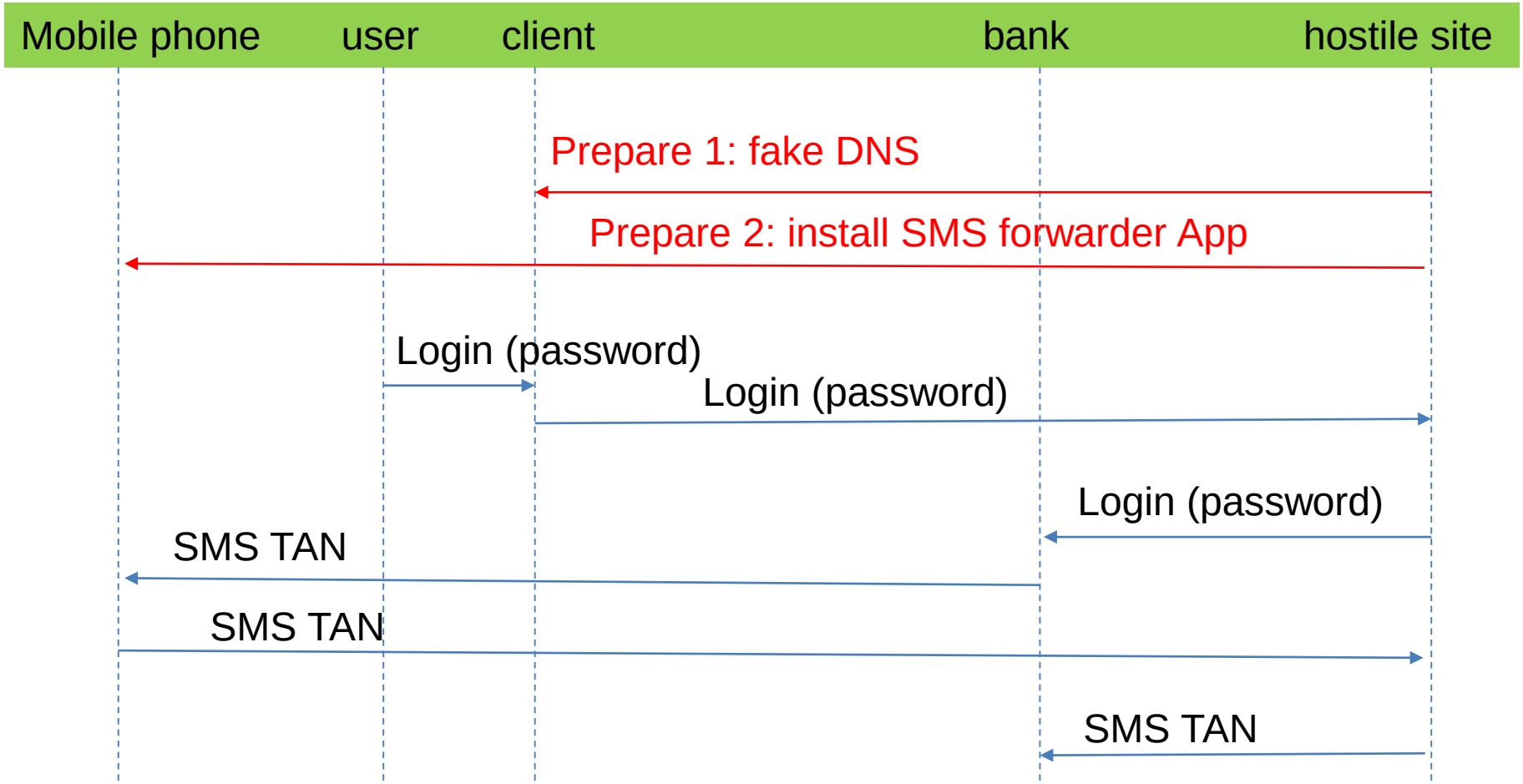
- Collect large data volumes (financial data)
- Collect customer related data
- Impact the victim's service
- Fake a service
- Obtain money



The main attack vectors (as seen in the real world)

Attack vector
Server-targeted
SSL, m-i-t-m
Session steal; hijack via Web
Client based (native) malware
Combined attack to PC and smartphone (Retefe)
Phishing and social engineering

The Retefe Trojan (2014): Automated attack on SMS based banking



A simple and effective social engineering based variant

- Distribute phishing mail which collects contract number, password and mobile number.
- Login (1st step)
- Call victim via telephone, refer to mail and ask for SMS (“identity check”).
- Login (2nd step), prepare transaction
- Ask victim for SMS (“re-check”)
- Confirm transaction.
- Announce “security reset”.
- Remove the money

Increasing trouble for mTAN

- SMS based mTAN
  - Still widely in use
  - image problems due to recent attacks
- Challenge-response with limited GUI
  - easy access via social engineering
- Ease of access to SMS
  - Access via telecom provider
  - Access via air interface
  - SMS forwarding is common (iMessage in iOS)
  - Access to SMS is a “standard right” for Apps in Android

Thesis: SMS need replacement

Smart Phones as authentication tokens

- The Smart Phone as a «super token»
  - Exellent user interface
  - Processing and key storing capabilities
  - Secure deployment and update
- Is the Smart Phone an independent device?
  - Device management via cloud
  - Communication via cloud
  - Synchronization with PC

Thesis: Mobile devices will be the tokens of choice

Increasing pressure for a “mobile only” access

- Security via single device operation
- The potential
  - High comfort (enter password; do transactions)
  - Always available
  - Traditional strong authentication (“have and know”)
- The challenge: “independent channels”
  - Two Apps
  - Sandboxing within one single App
  - https://www1.cs.fau.de/content/unsicherheit-von-app-basierten-tan-verfahren-im-onlinebanking
  - http://www.heise.de/security/meldung/Forscher-demontieren-App-TANs-der-Sparkasse-2853492.html

Thesis: Single device mobile access will become a standard.

Mobile solutions (single device)

client	Transaction signing	usability	Transaction security
Browser	None	+++++	0
	SMS	+	++
	OTP App	+	+
	Signing App	+++	++++
	Additional signing token	0	+++++
App with binding	None	+++++	+
	SMS	+	++
	OTP	+	+
	Integrated Signer Module	+++++	++
	Separate Signing App	++++	+++
	Smart Watch	++++	++++
	Additional signing token	0	+++++

Mobiles / Wearables

- Still growing smart phone population
- Smart Watches to show up
- Are Smart Watches independent devices?

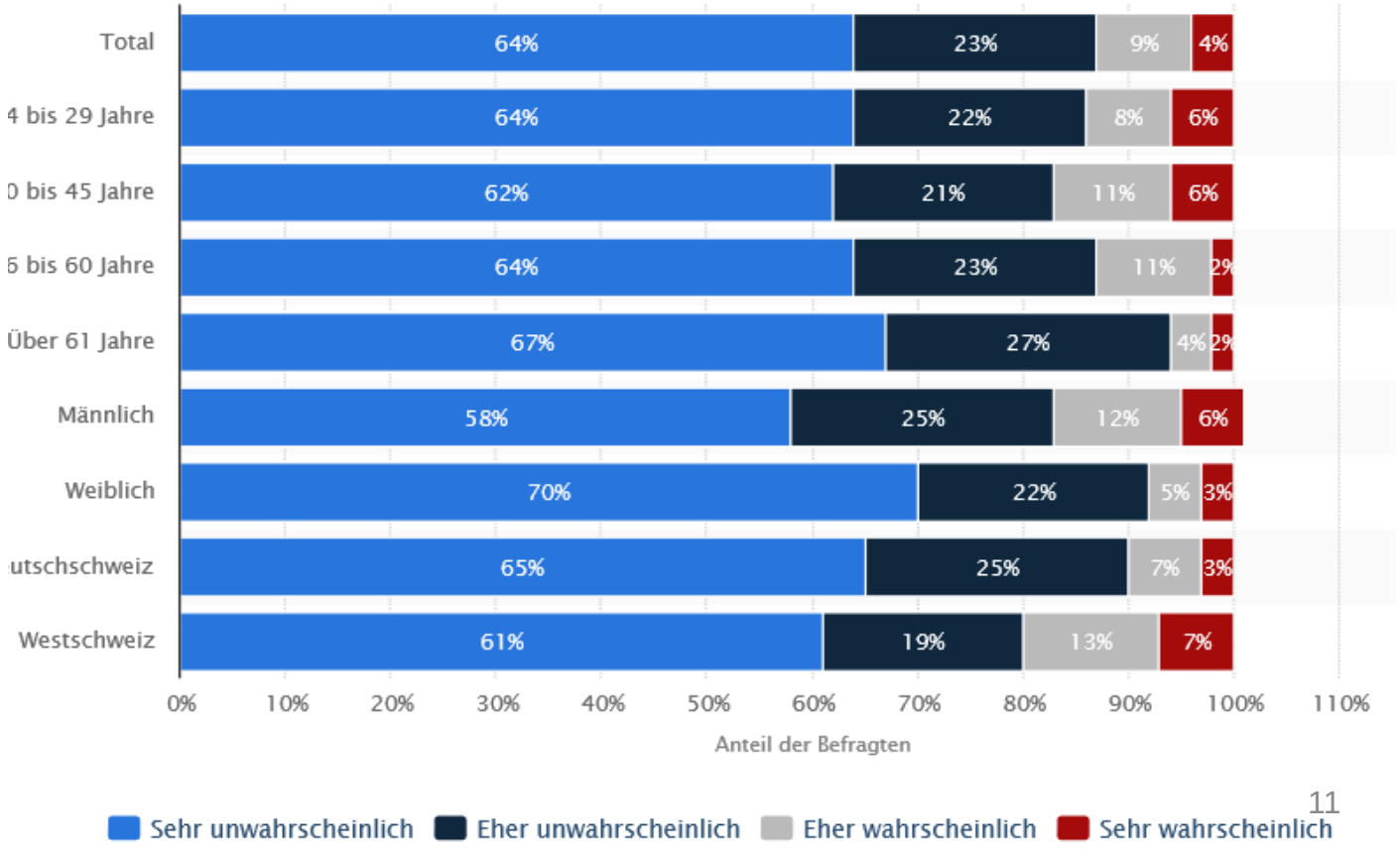
Thesis: Wearables might become interesting tokens.

The Smartwatch potential

Wie wahrscheinlich ist es, dass Sie sich in den nächsten 12 Monaten eine Smartwatch kaufen?

Diese Statistik zeigt die Ergebnisse einer Umfrage zum Marktpotenzial der Smartwatch in der Schweiz nach Alter, Geschlecht und Region im Jahr 2015. Insgesamt 22 Prozent der weiblichen Befragten gaben an, dass es eher unwahrscheinlich ist, dass sie sich in den nächsten 12 Monaten eine Smartwatch kaufen.

Source: Statista



And further: A new banking paradigm ?

- PFM by specialized non-banks http://www.qontis.ch/
- Services across banks www.sofort.com
- Mobile payment applications
  - paymit (UBS, ZKB, SIX)
  - P2P (Migros Bank)
  - Twint (Postfinance)

Thesis: Banks will need secure systems with foreign components.

Summary of our Theses

- SMS need replacement.
- Mobile devices will be the tokens of choice.
- Single device mobile access will become a standard.
- Wearables might become interesting tokens.
- Banks will need secure systems with foreign components.

Danke

Paul Schöbi
paul.schoebi@cnlab.ch
+41 55 214 33 33

Christian Birchler
christian.birchler@cnlab.ch
+41 55 214 33 40

Thomas Lüthi
thomas.luethi@cnlab.ch
+41 55 214 33 41

René Vogt
rene.vogt@cnlab.ch
+41 55 214 33 31

Esther Hänggi
esther.haenggi@cnlab.ch
+41 55 214 33 36