EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

Voice Cloning als Gefahr für Online Stimm-Authentifizierung

Bachelorarbeit

von Hannah Mildner

Gliederung

- Motivation
- Verfahren
  - Passwortersatz
  - Online-Banking-Verfahren: Passwort + Stimme
    - Mit Abfrage der Überweisungsdaten
    - Mit Abfrage eines Zufallsworts
    - Mit Abfrage von Überweisungsdaten & Zufallswort
- Voice Cloning
- Zusammenfassung

Motivation

- Sicherheit (Trojaner)
- Mobilität

Motivation

Stimme

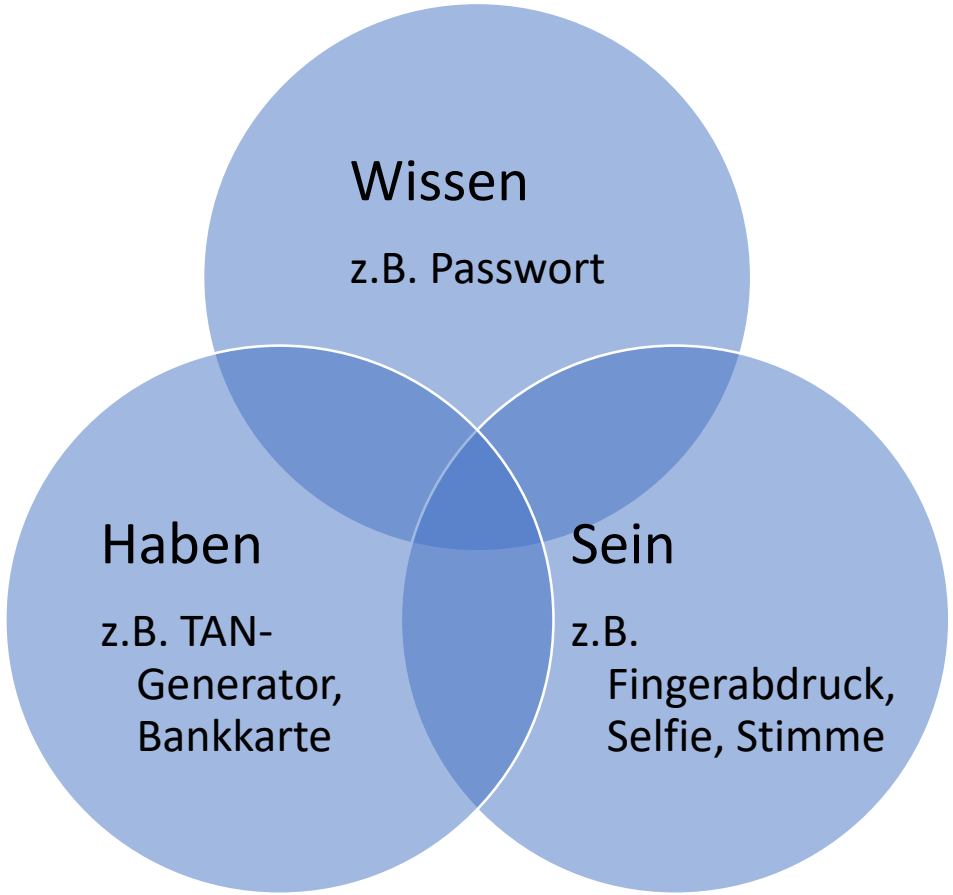
- einzigartig
- Abfrage mit dem Smartphone
- wird automatisch mitgeführt
- Man muss sich nichts merken

Motivation

Stimme

- einzigartig
- Abfrage mit dem Smartphone
- wird automatisch mitgeführt
- Man muss sich nichts merken
- gleichgestellter Authentifizierungs-Faktor

2-Faktor-Authentifizierung



Motivation

Stimme

- Dynamisch
- Keine einfache Kopie möglich
- Stimme und gesprochener Text sind miteinander verknüpft

(Überweisungsdaten & Stimme)

➡ Schutz vor Manipulation

Fingerabdruck, Selfie

- Statisch
- Kann durch Kopie überlistet werden
- Authentisierungsmethode und Text nicht automatisch verbunden

Passwortersatz – Wo?

Santander

Tangerine
Forward Banking™

بنك أبوظبي التجاري
ADCB

TB
TATRA BANKA

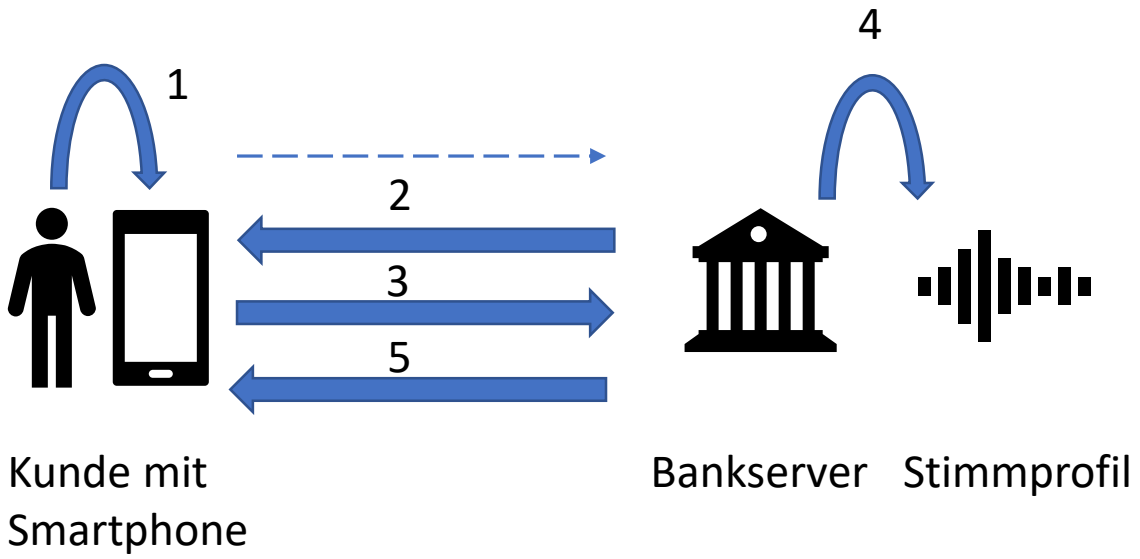
ANZ

HSBC

BARCLAYS

Tinkoff Bank

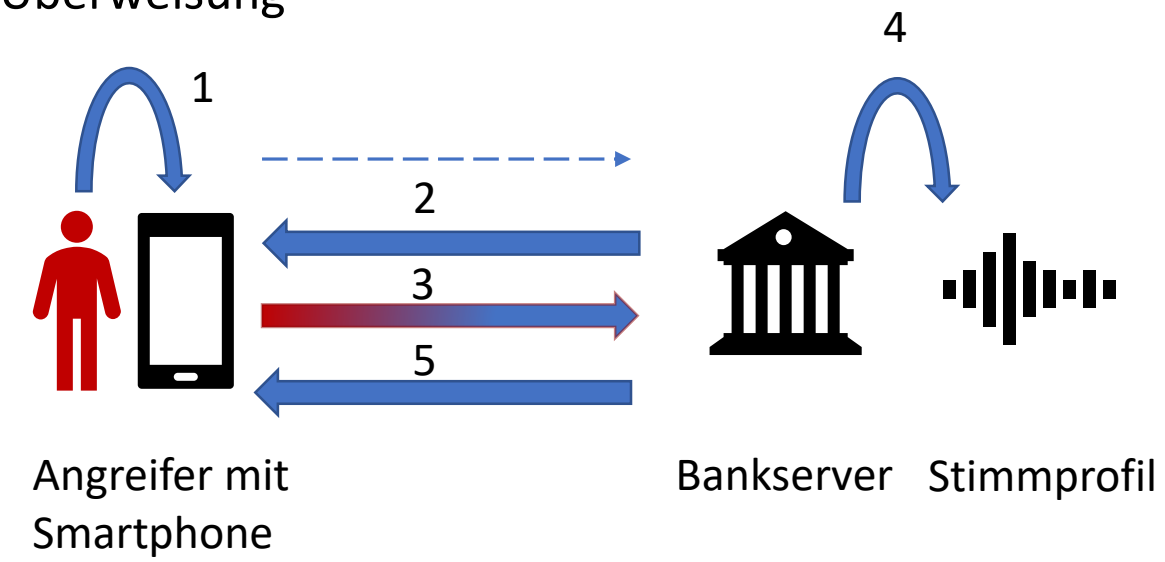
Passwortersatz



1. Name eingeben & Anfrage an Bank senden
2. Anruf aufbauen
3. „Mein Name ist mein Passwort“ sprechen
4. Stimmprofil abgleichen
5. Rückmeldung

Passwortersatz: Phishing Angriff

1. Phishing Anruf
2. Betrügerische Überweisung

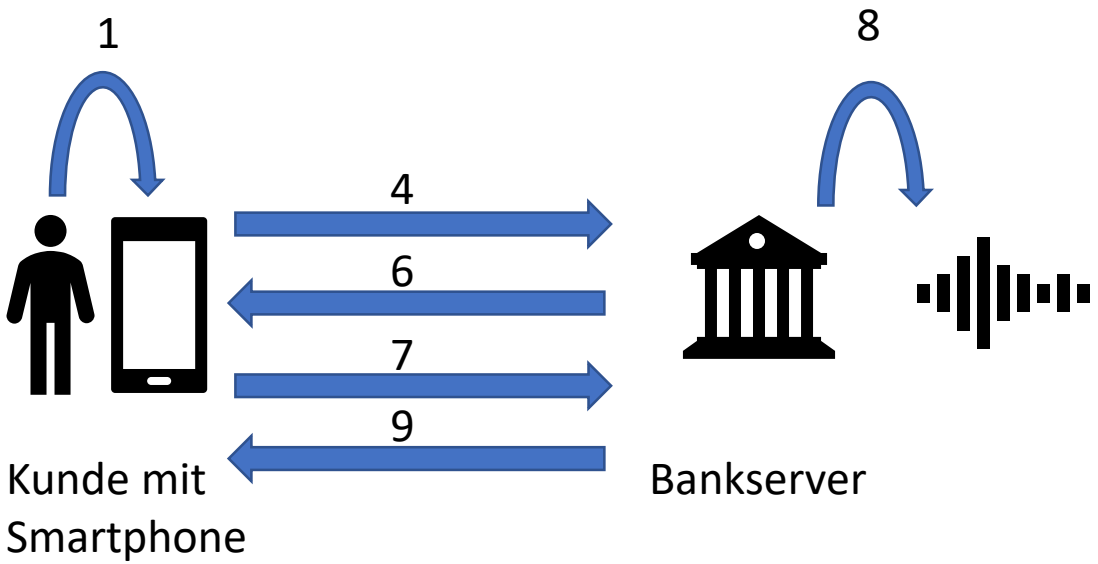


- Angriff immer möglich
- Benutzername und Spracheingabe wird benötigt

Verfahren

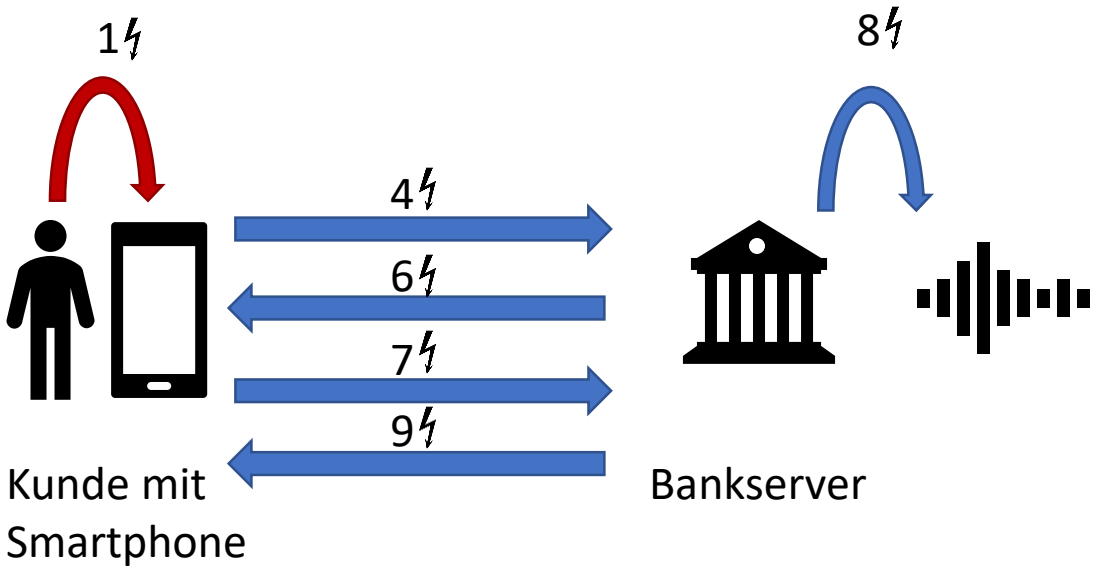
1. Login in Banking-App mit Benutzernamen und Passwort
2. Stimme zur Bestätigung der Überweisung

Verfahren mit Abfrage der Überweisungsdaten



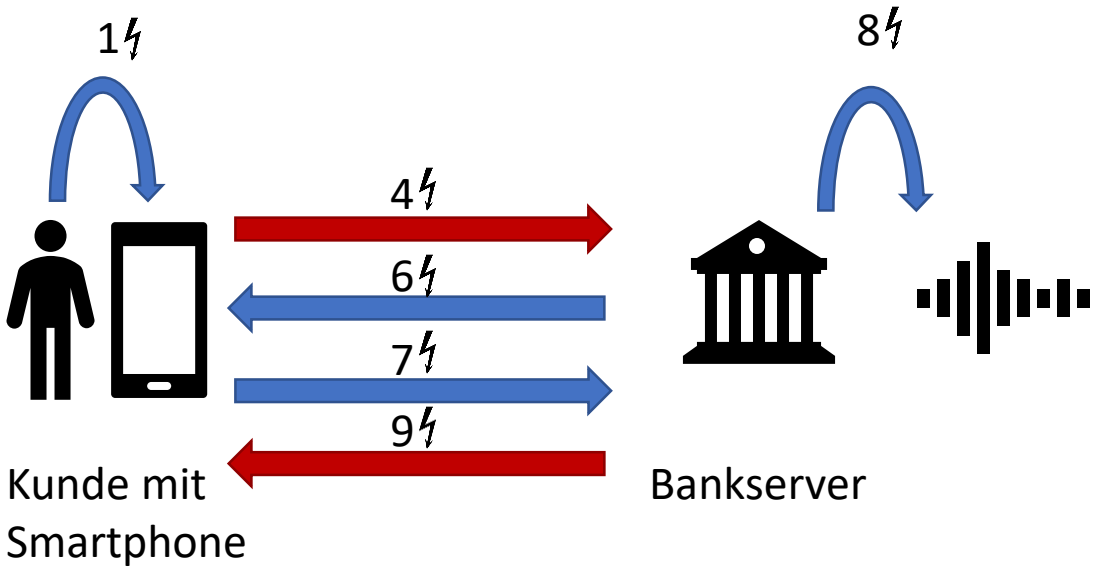
1. Benutzername & Passwort eingeben
2. Überweisungsdaten eingeben
3. Überprüfen
4. Überweisungsauftrag an den Bankserver
5. Registrieren
6. Anruf aufbauen
7. Sprechen von IBAN, Betrag
8. Abgleich Stimmprofil & Daten
9. Rückmeldung

Angriffspunkte



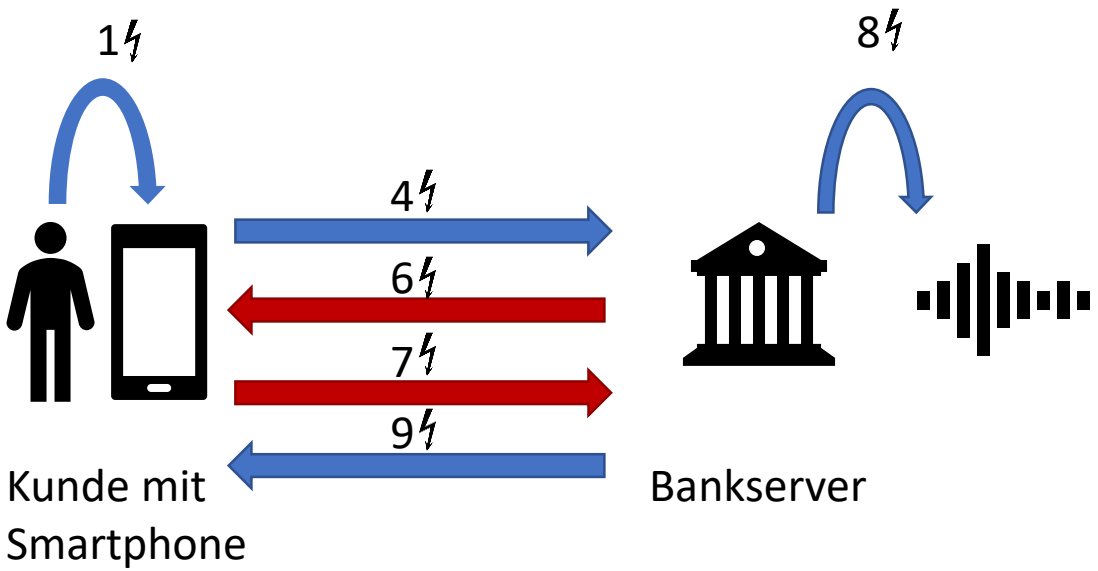
- Phishing
- Trojaner

Angriffspunkte



- Man-in-the-Middle

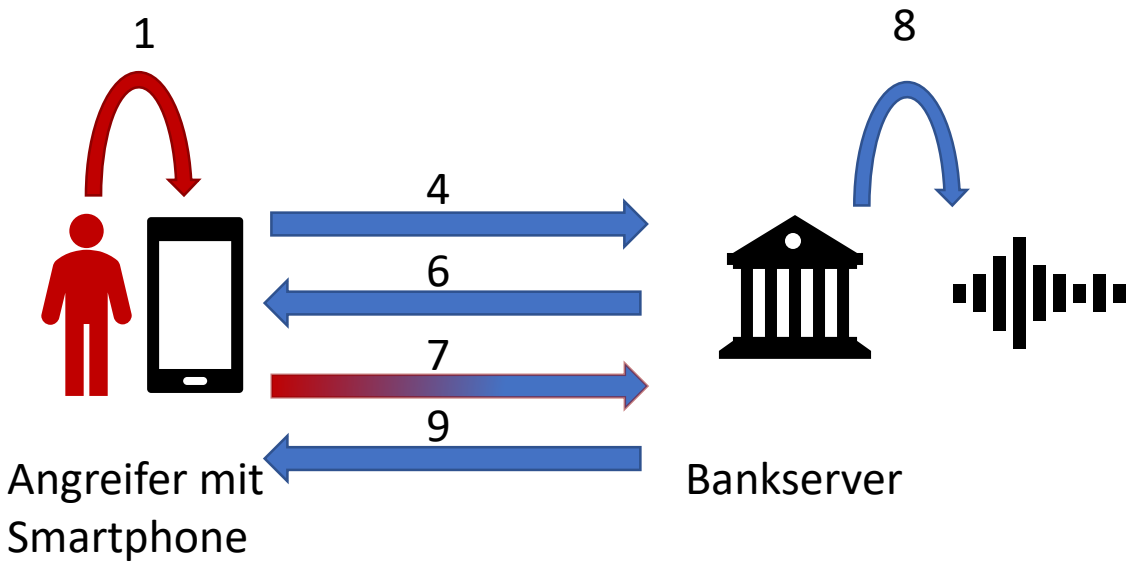
Angriffspunkte



- Angriff mithilfe aufgezeichneter Stimmaufnahmen
  - Replay Angriff

Replay Angriff

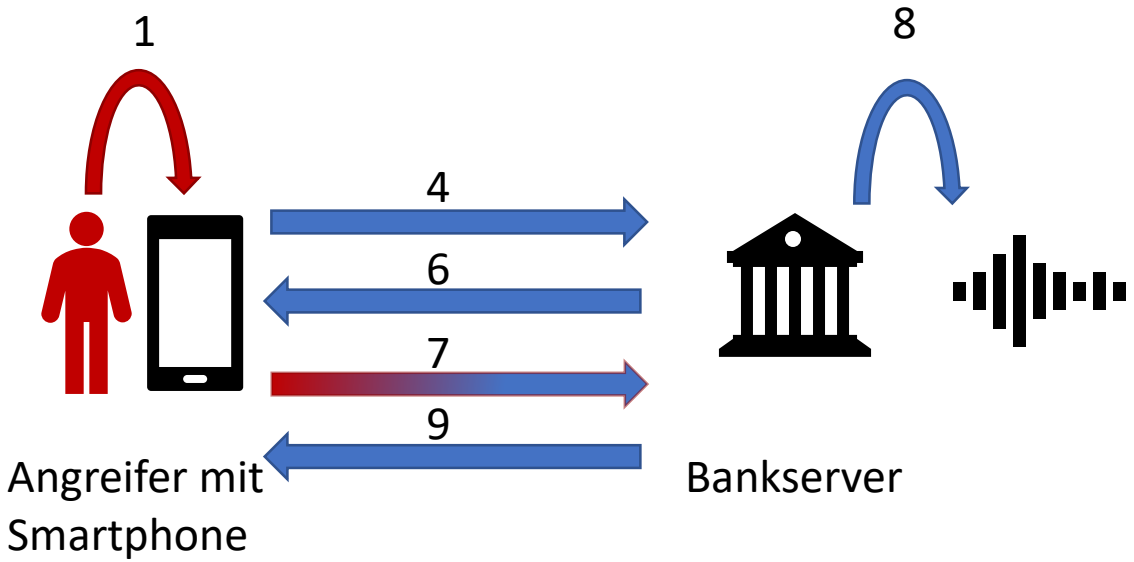
1. Trojaner
2. Betrügerische Überweisung



- Angriff immer möglich
- Nur die gleiche Überweisung
- Zugangsdaten und Spracheingabe werden benötigt

Zusammengesetzter Replay Angriff

1. Trojaner
2. Betrügerische Überweisung



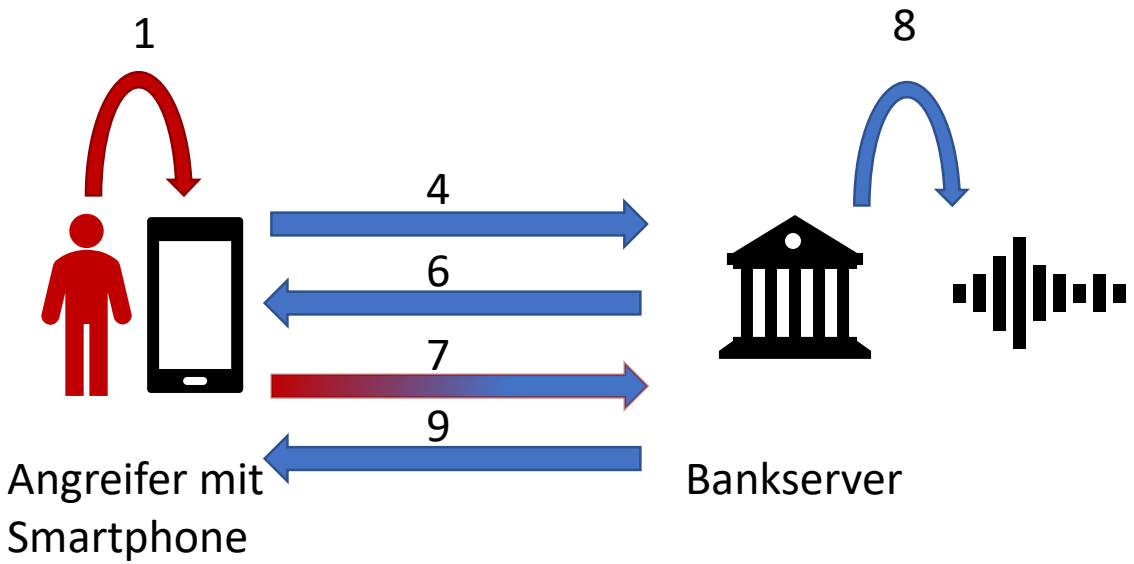
- Angriff immer möglich
- Beliebige Überweisung
- Zugangsdaten und Spracheingabe werden benötigt
- Sprachansage muss vom Angreifer vorher vorbereitet werden

50 Euro an IBAN DE81 235 848..
10 Euro an IBAN DE68 945 765..
800 Euro an IBAN DE81 848 111..

→ 800 Euro an IBAN DE86 532 689..

Zusammengesetzter Replay Angriff

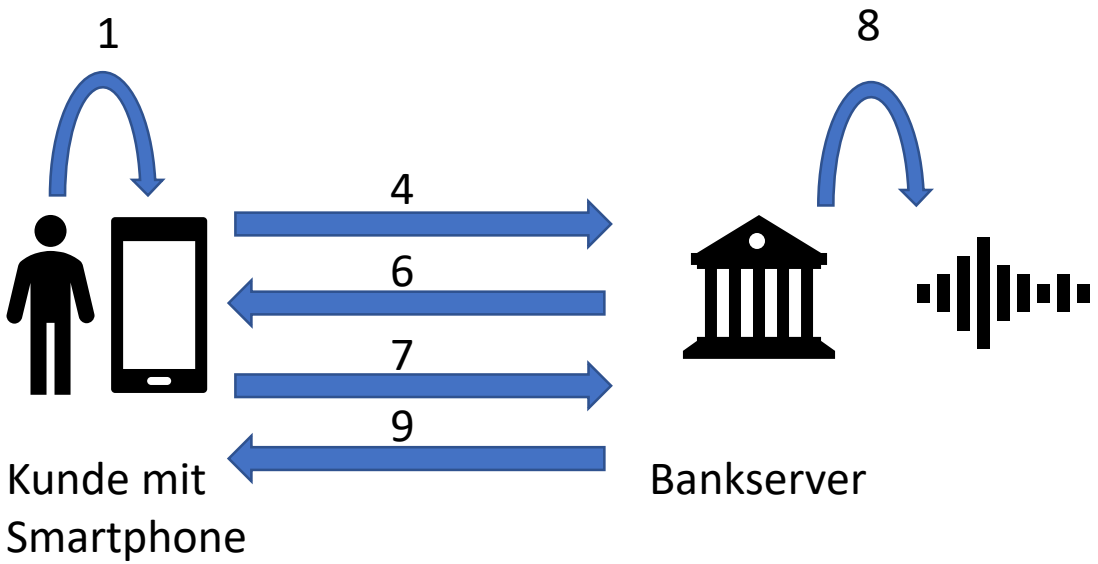
1. Trojaner
2. Betrügerische Überweisung



- Angriff immer möglich
- Beliebige Überweisung
- Zugangsdaten und Spracheingabe werden benötigt
- Sprachansage muss vom Angreifer vorher vorbereitet werden

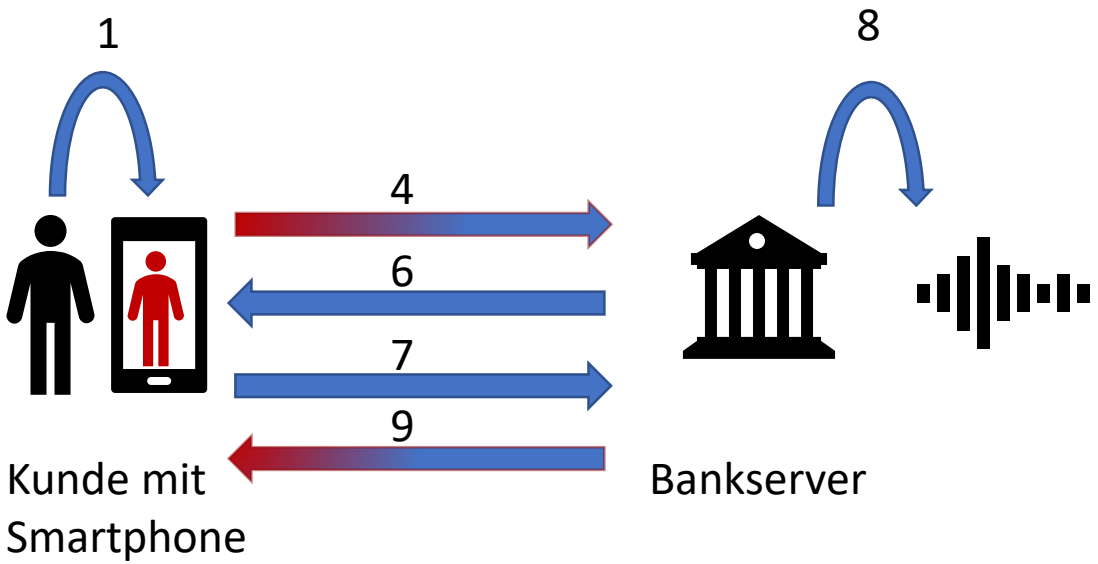
⟹ Zufallswort

Verfahren mit Zufallswort



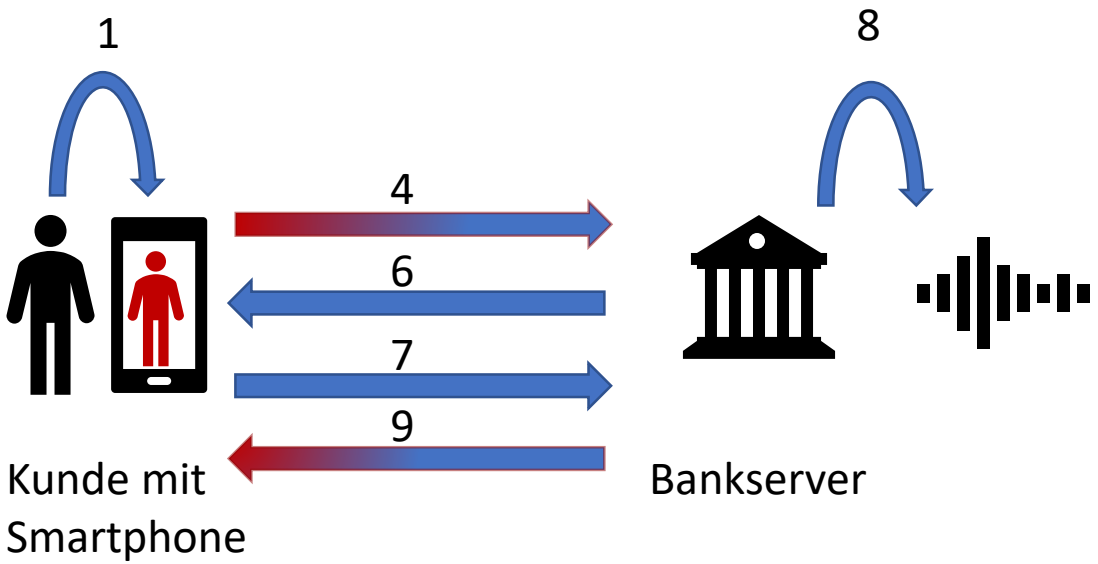
6. Anruf aufbauen & Ansage des Zufallsworts
7. Sprechen des Zufallsworts

Man-in-the-Middle Angriff



- Angriff nur während der Überweisung des Kunden möglich
- Beliebige Überweisung

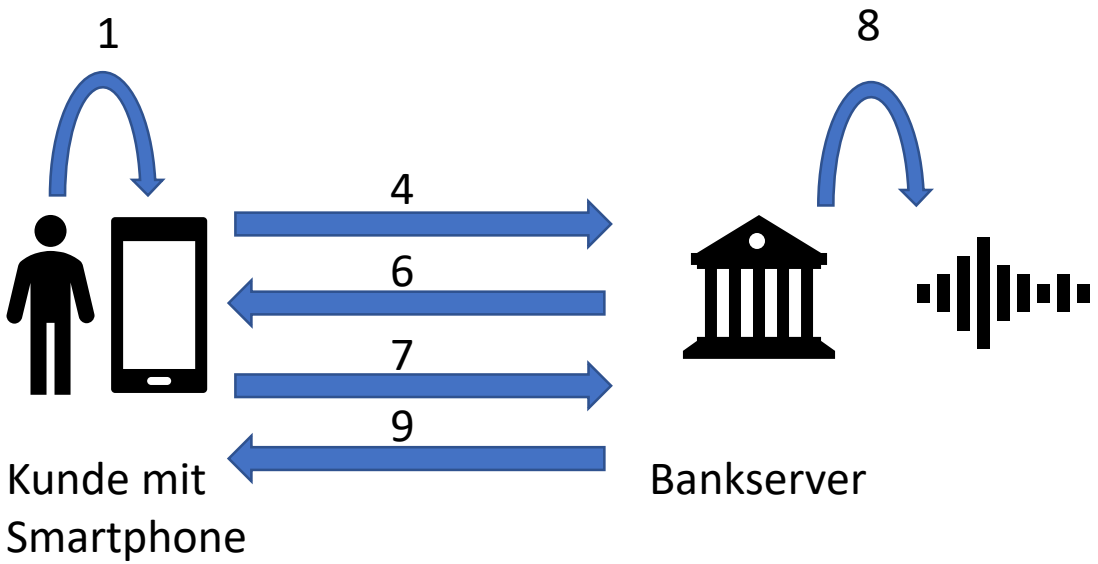
Man-in-the-Middle Angriff



- Angriff nur während der Überweisung des Kunden möglich
- Beliebige Überweisung

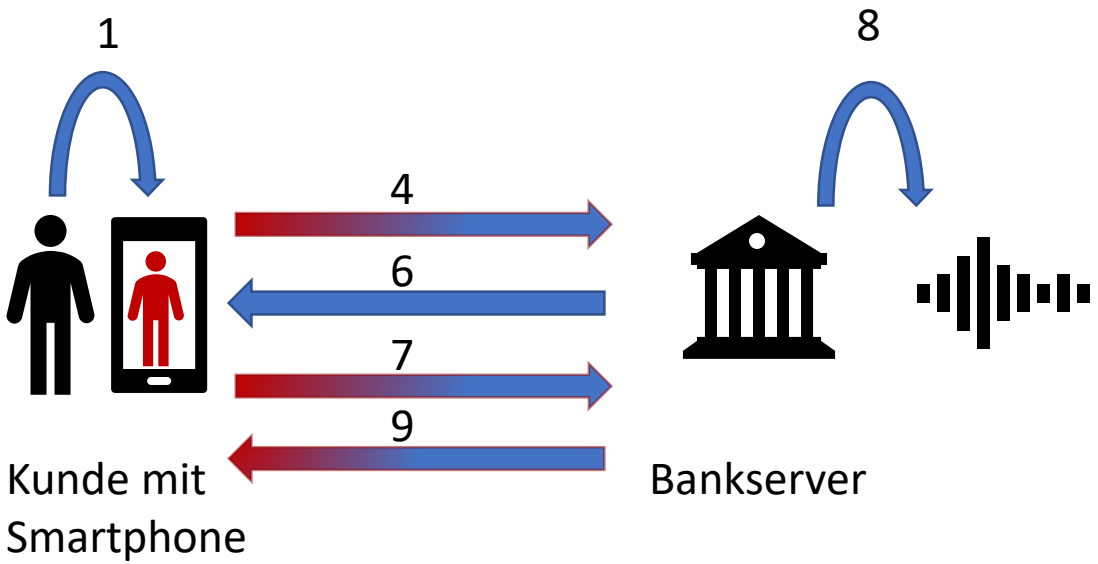
⟹ Überweisungsdaten & Zufallswort

Verfahren mit Überweisungsdaten & Zufallswort



6. Anruf aufbauen & Ansage des Zufallsworts
7. Sprechen von IBAN, Betrag und Zufallswort

Man-in-the-Middle Angriff mit zusammengesetztem Replay Angriff



- Angriff nur während der Überweisung des Kunden möglich
- Beliebige Überweisung
- Sprachansage muss vom Angreifer vorher vorbereitet werden

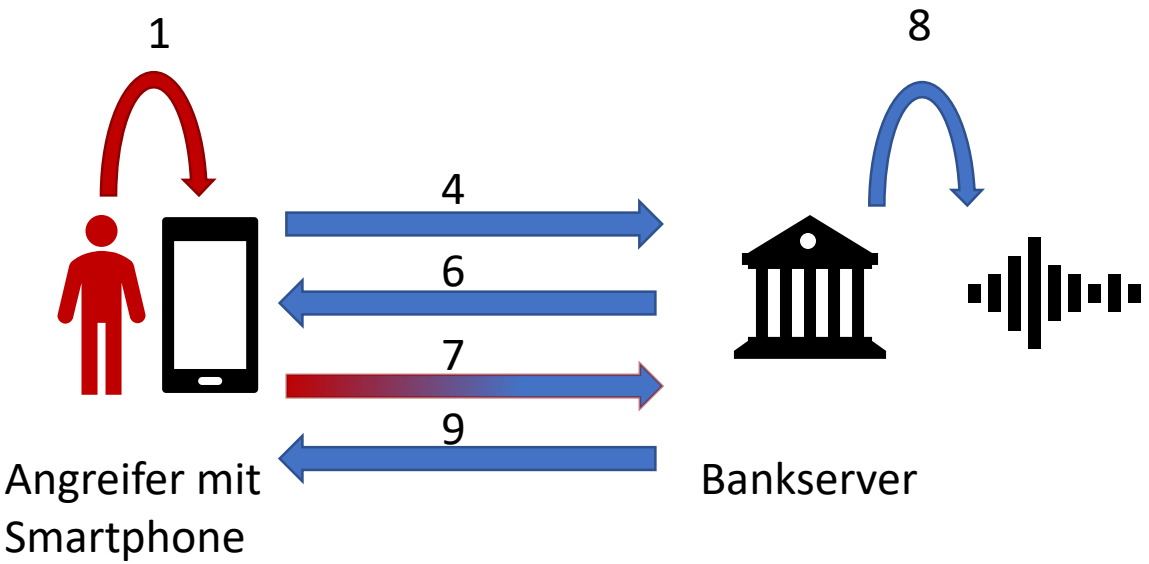
Gefahr: Voice Cloning ist so gut, dass sie die Stimme fast perfekt klonen kann.

Voice Cloning Angriff

1. Sammeln von Stimmaufnahmen
2. Stimmmodell erstellen
3. Künstliche Stimme mit Eingabe erzeugen

Voice Cloning Angriff

1. Trojaner
2. Betrügerische Überweisung



- Angriff immer möglich
- Beliebige Überweisung
- Zugangsdaten und Spracheingabe wird benötigt
- Sprachmodell muss vorher erstellt werden

Voice Cloning - Methoden

- Formantsynthese (Parameter Modell) [ab 1960]
  Formanten: Resonanzen des Vokaltraktes
- Konkatenativer Ansatz (Verkettungsansatz) [ab 1970]
- HMM (stochastisches Modell)
- Neuronale Netze

Beispiel eines Voice Cloning Programms

- Lyrebird Beta Version
- Mindestens 30 vorgegebene Sätze eingeben
- Bisher nur in Englisch verfügbar
- Erstellung der Stimme benötigt wenige Minuten (hier 3 Minuten)
- Bsp.: Meine geklonte Stimme

Zusammenfassung

- Hoffnung für die Authentifizierung
- Voice Cloning Programme aktuell fast so gut wie aufgenommene Original Stimme
- Programme benötigen sehr wenig Aufnahmen

  Lyrebird benötigt nur eine 1 Minütigen Aufnahme um die Stimme perfekt klonen zu können

Voice Cloning stellt eine große Bedrohung für die Stimm-Authentifizierung dar

Danke für Ihre Aufmerksamkeit!