Die fabelhafte Welt des Mobilebankings

Nomorp: No More Protection

Vincent Haupert und Nicolas Schneider

27. Dezember 2017

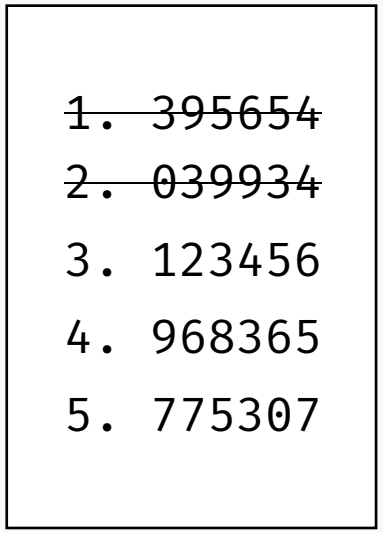
IT-Sicherheitsinfrastrukturen
Department Informatik
Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)

Vom Online- zum Mobilebanking

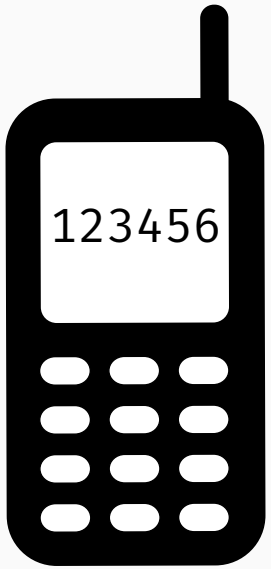
Onlinebanking

TAN-Verfahren

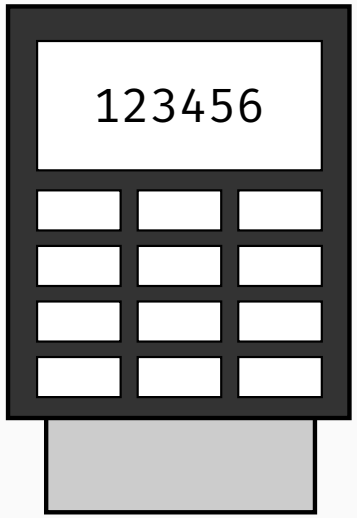
Vom Online- zum Mobilebanking



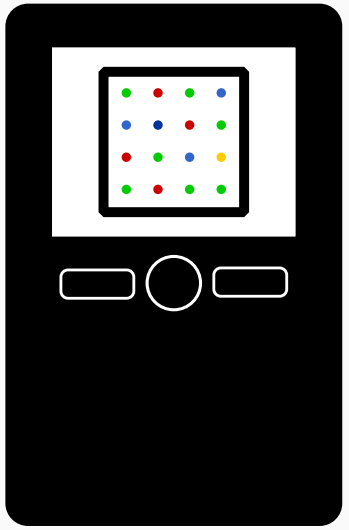
iTAN



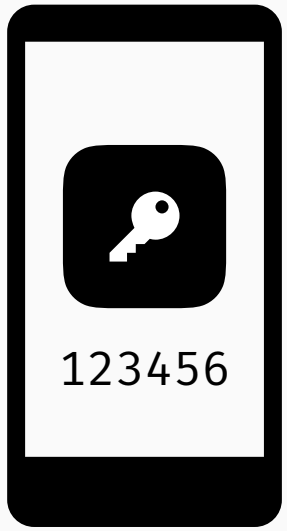
smsTAN



chipTAN

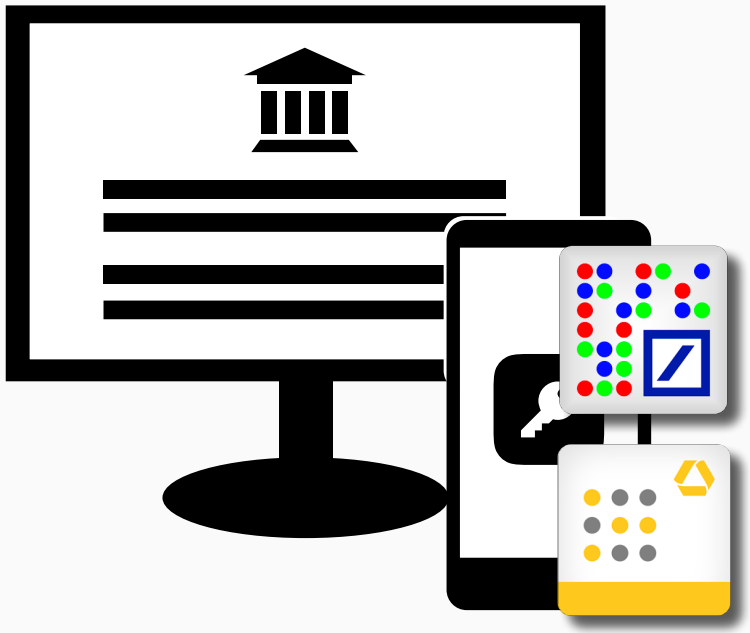


photoTAN

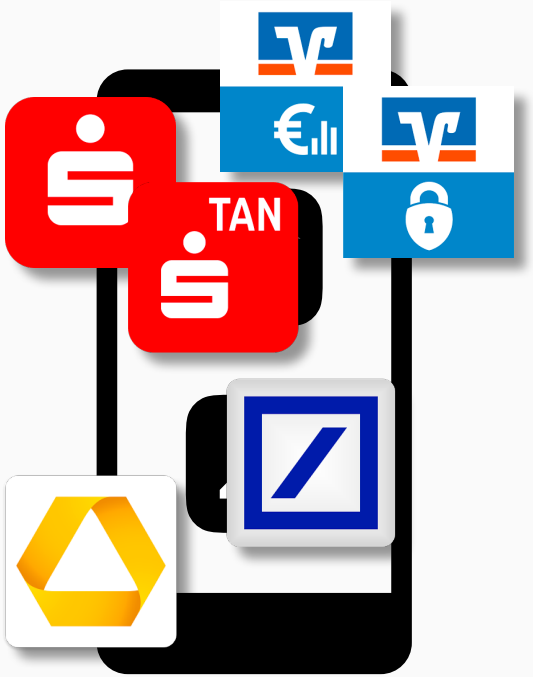


appTAN

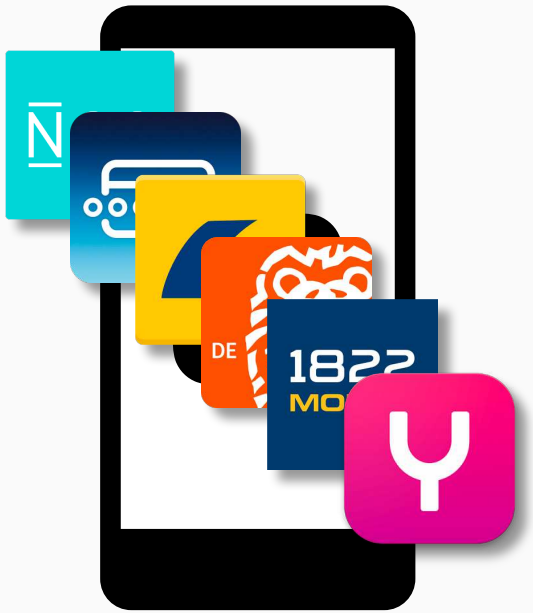
Vom Online- zum Mobilebanking



Zwei-Geräte-Authentifizierung

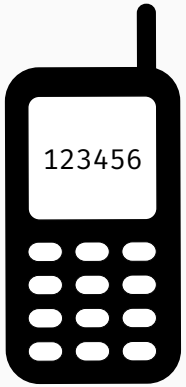


Zwei-App-Authentifizierung



Ein-App-Authentifizierung

Geräteentwicklung smsTAN



Spezialgerät

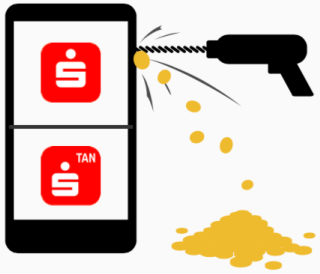
„Hier bedient man sich der Technik der Übertragung über zwei unterschiedliche Kanäle [...]. Dies impliziert bereits, dass die Verwendung des mobileTAN-Verfahrens z. B. über nur ein mobiles Smartphone für beide Kommunikationsstrecken nicht zulässig ist und daher in den Kundenbedingungen für das Online-Banking explizit ausgeschlossen wird.“

— Die Deutsche Kreditwirtschaft [DK]

Mehrzweckgerät

32c3: (Un)Sicherheit von App-basierten TAN-Verfahren im Onlinebanking

pushTAN-Angriff



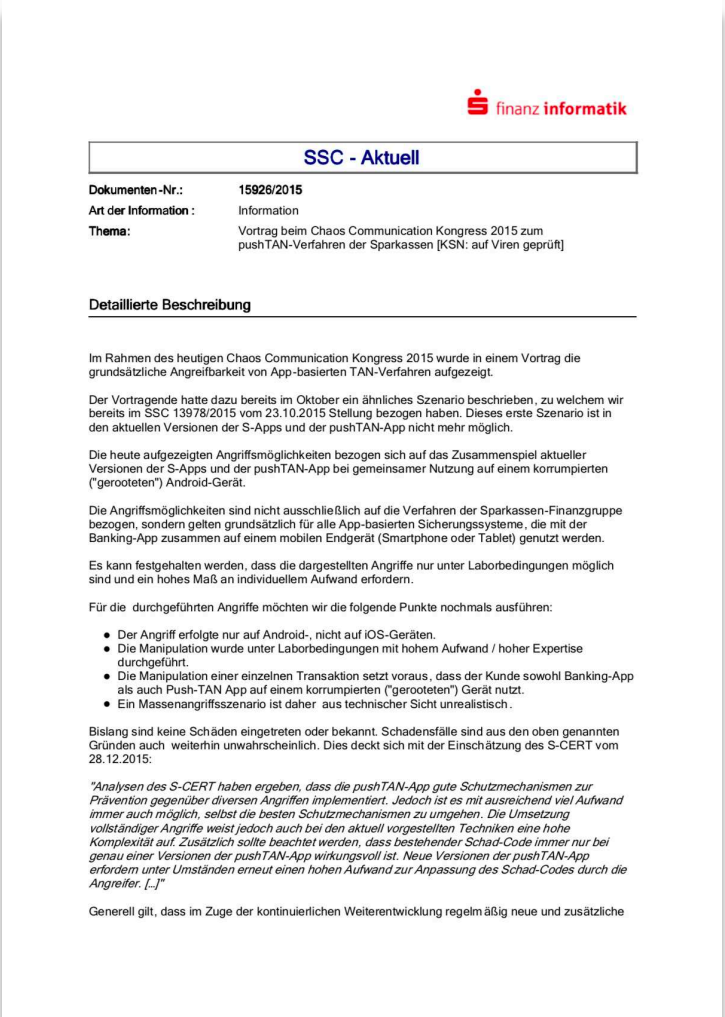
Mögliche technische Angriffe

- *S-pushTAN-App* kopieren
- Protokoll der *S-pushTAN-App* reversen und eigenen Client entwickeln
- Transaktionsmanipulation

10

Stellungnahme Sparkasse bzgl. 32c3:

- Laborbedingungen (*Xposed*, Root)
- Funktioniert nur bei genau einem Gerät, genau einer App, genau einer Version
- Updates sorgen für hohen individuellen und manuellen Aufwand



finanz informatik

SSC - Aktuell

Dokumenten-Nr.: 15926/2015
Art der Information : Information
Thema: Vortrag beim Chaos Communication Kongress 2015 zum pushTAN-Verfahren der Sparkassen [KSN: auf Viren geprüft]

Detaillierte Beschreibung

Im Rahmen des heutigen Chaos Communication Kongress 2015 wurde in einem Vortrag die grundsätzliche Angreifbarkeit von App-basierten TAN-Verfahren aufgezeigt.

Der Vortragende hatte dazu bereits im Oktober ein ähnliches Szenario beschrieben, zu welchem wir bereits im SSC 13978/2015 vom 23.10.2015 Stellung bezogen haben. Dieses erste Szenario ist in den aktuellen Versionen der S-Apps und der pushTAN-App nicht mehr möglich.

Die heute aufgezeigten Angriffsmöglichkeiten bezogen sich auf das Zusammenspiel aktueller Versionen der S-Apps und der pushTAN-App bei gemeinsamer Nutzung auf einem korrumpierten ("gerooteten") Android-Gerät.

Die Angriffsmöglichkeiten sind nicht ausschließlich auf die Verfahren der Sparkassen-Finanzgruppe bezogen, sondern gelten grundsätzlich für alle App-basierten Sicherungssysteme, die mit der Banking-App zusammen auf einem mobilen Endgerät (Smartphone oder Tablet) genutzt werden.

Es kann festgehalten werden, dass die dargestellten Angriffe nur unter Laborbedingungen möglich sind und ein hohes Maß an individuellem Aufwand erfordern.

Für die durchgeführten Angriffe möchten wir die folgende Punkte nochmals ausführen:

- Der Angriff erfolgte nur auf Android-, nicht auf iOS-Geräten.
- Die Manipulation wurde unter Laborbedingungen mit hohem Aufwand / hoher Expertise durchgeführt.
- Die Manipulation einer einzelnen Transaktion setzt voraus, dass der Kunde sowohl Banking-App als auch Push-TAN App auf einem korrumpierten ("gerooteten") Gerät nutzt.
- Ein Massenangriffsszenario ist daher aus technischer Sicht unrealistisch.

Bislang sind keine Schäden eingetreten oder bekannt. Schadensfälle sind aus den oben genannten Gründen auch weiterhin unwahrscheinlich. Dies deckt sich mit der Einschätzung des S-CERT vom 28.12.2015:

"Analysen des S-CERT haben ergeben, dass die pushTAN-App gute Schutzmechanismen zur Prävention gegenüber diversen Angriffen implementiert. Jedoch ist es mit ausreichend viel Aufwand immer auch möglich, selbst die besten Schutzmechanismen zu umgehen. Die Umsetzung vollständiger Angriffe weist jedoch auch bei den aktuell vorgestellten Techniken eine hohe Komplexität auf. Zusätzlich sollte beachtet werden, dass bestehender Schad-Code immer nur bei genau einer Versionen der pushTAN-App wirkungsvoll ist. Neue Versionen der pushTAN-App erfordern unter Umständen erneut einen hohen Aufwand zur Anpassung des Schad-Codes durch die Angreifer. [...]"

Generell gilt, dass im Zuge der kontinuierlichen Weiterentwicklung regelmäßig neue und zusätzliche

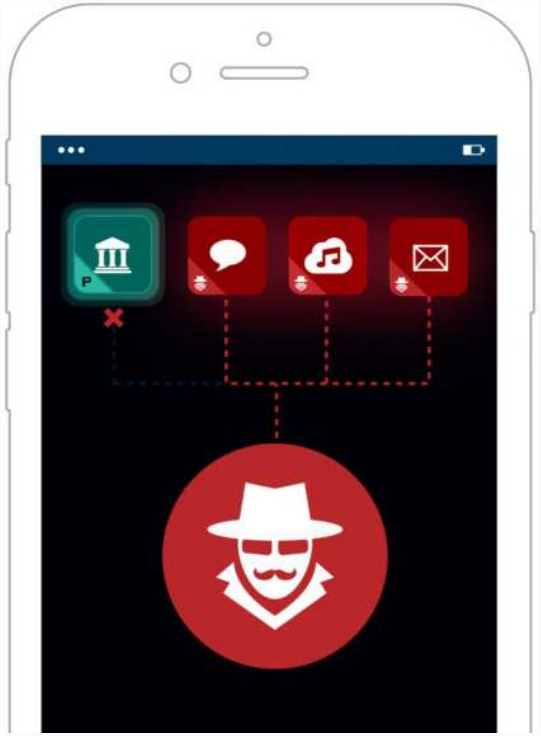
App-Sicherheit durch Dritte

App-Sicherheit durch Dritte: Übersicht

Promon SHIELD [PS1]

- Schutz von Apps in nicht-vertrauenswürdigen Umgebungen
- Universal und plattformunabhängig
- Anwendbar innerhalb weniger Minuten

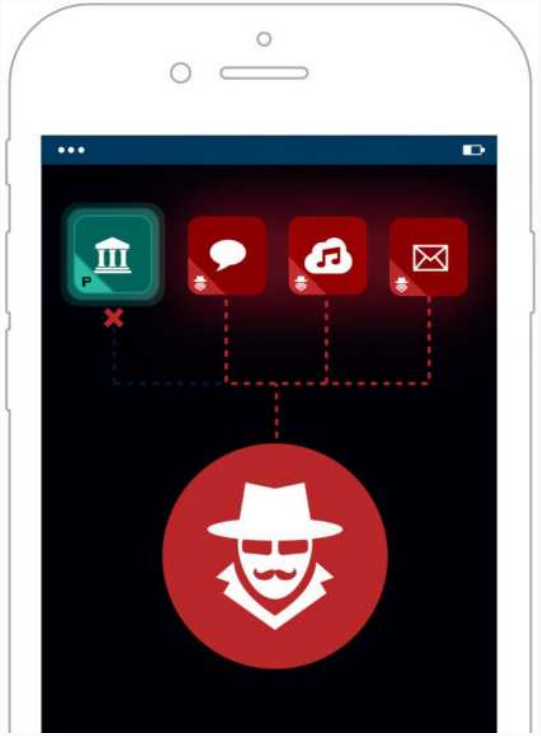
> *Es erkennt und verhindert jede Gefahr in Echtzeit und reagiert, indem es die notwendigen Schritte einleitet, um die App vollständig zu schützen. Die App wird dadurch sicher verwendbar, sogar auf hochgradig infizierten Geräten.*
>
> — Promon SHIELD Produktvideo [PS2]



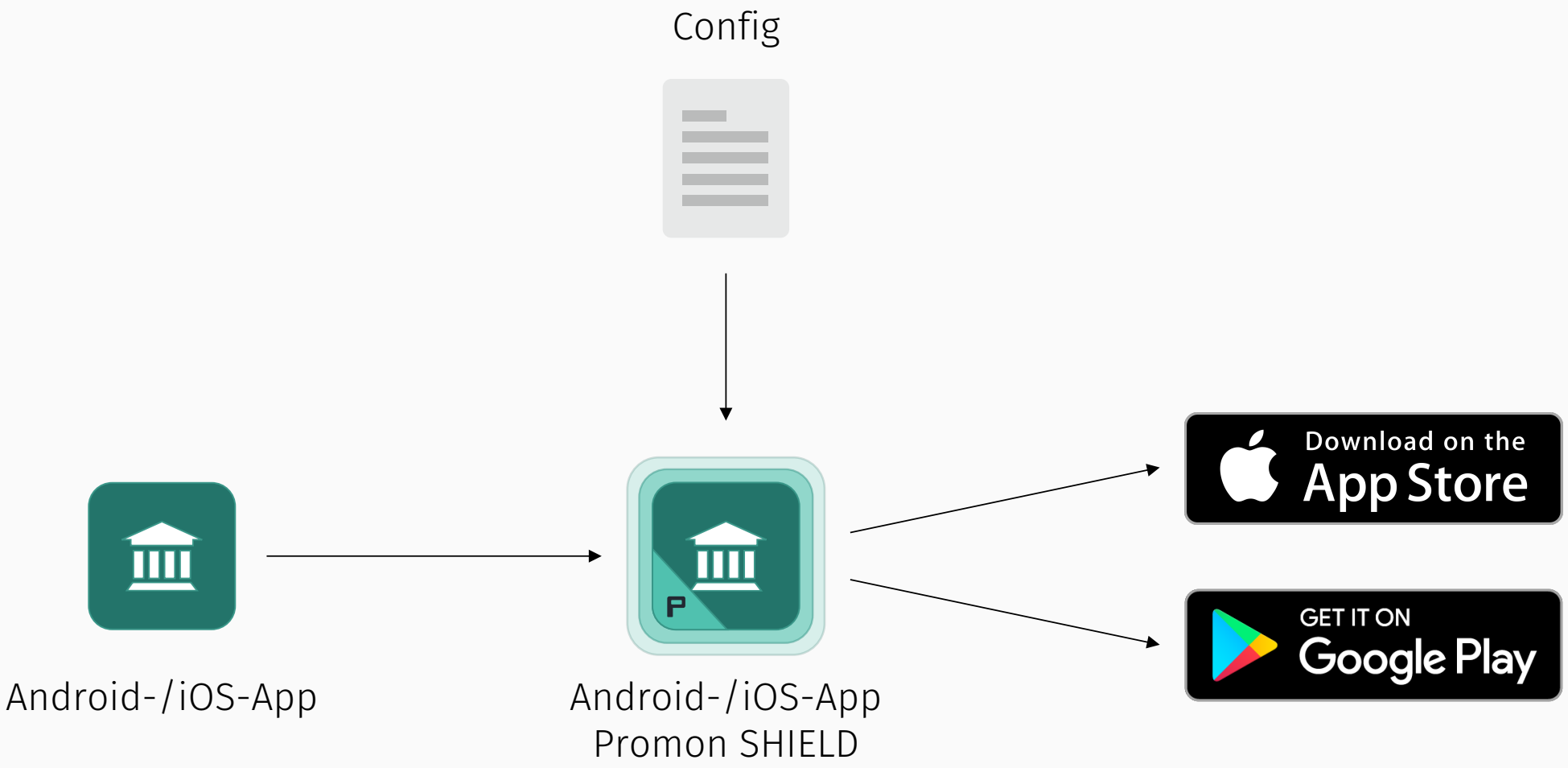
App-Sicherheit durch Dritte: Promon SHIELD

Promon SHIELD

- App-Härtung
  - Tamperproofing
  - Anti-Hooking
  - Anti-Debugging
  - Anti-Emulator
  - Obfuskierung
  - Gerätebindung
  - Root-Erkennung
- Best Practices
  - Certificate Pinning
  - Eigene Tastatur
  - Verschlüsselung von Anwenderdaten



App-Sicherheit durch Dritte: Promon SHIELD



Promon

citi
Mobile
DKB
BB Bank
MLP
psd
Bank
BW|Bank
TAN
W&W
wüstenrot
comdirect
FIM
bank
norwegian
FOREX
BANK
fd
MY

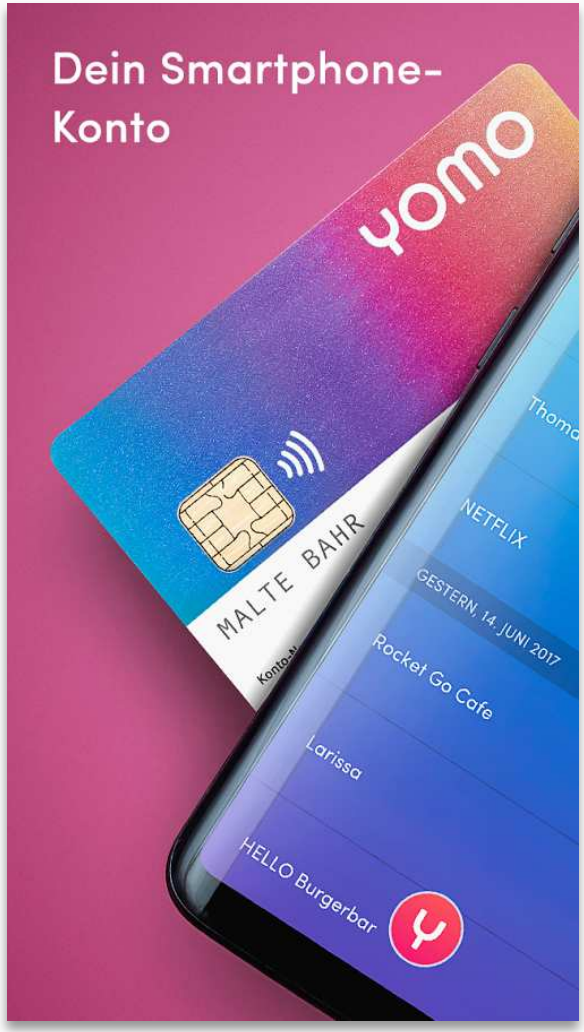
Promon SHIELD am Beispiel Yomo

Promon SHIELD am Beispiel Yomo

Yomo – das Girokonto für dein Smartphone

- Ein-App-Verfahren nach dem Vorbild von N26
- Neuste App unter den Promon-Verwendern

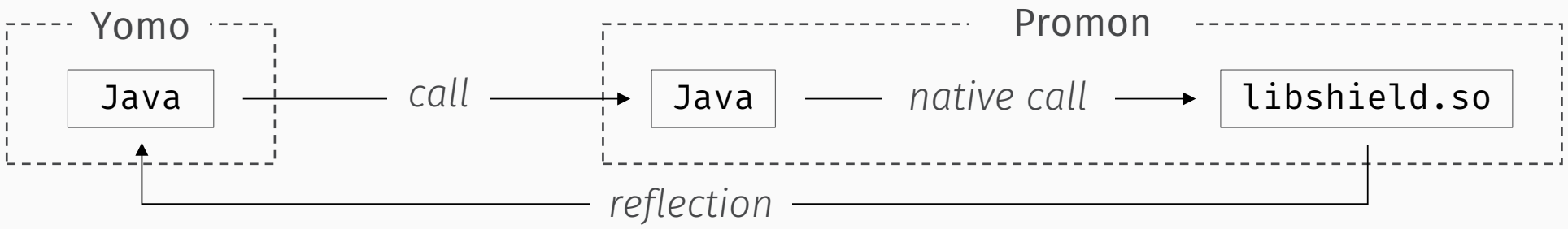
  ⇒ vermutlich auch neuste Promon-Version



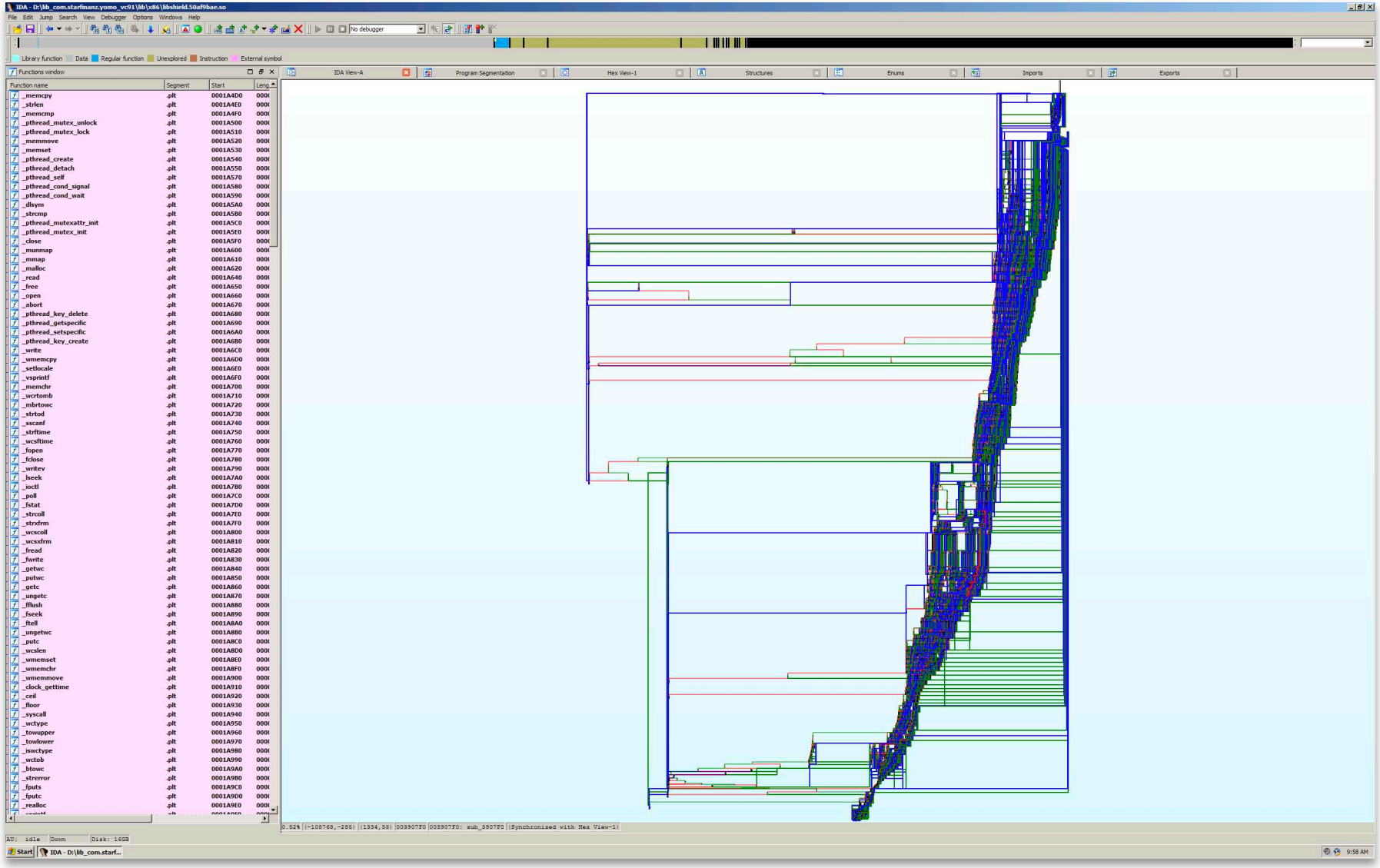
Funktionsweise Promon SHIELD

- Promon übernimmt `MainActivity`, um native Bibliothek `libshield.so` zu laden
- Fügt eigene Java-Klassen ein, die über Renaming obfuskiert sind
- Externalisiert Strings und Konstanten
- Verwendung eines Client-Zertifikats

1 Bibliothek modifizieren



Promon SHIELD am Beispiel Yomo



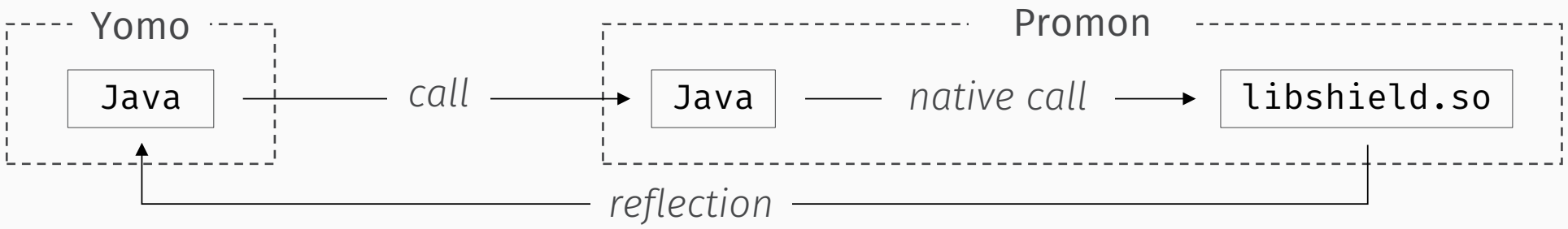
Funktionsweise Promon SHIELD

- Promon übernimmt `MainActivity`, um native Bibliothek `libshield.so` zu laden
- Fügt eigene Java-Klassen ein, die über Renaming obfuskiert sind
- Externalisiert Strings und Konstanten
- Verwendung eines Client-Zertifikats

Promon SHIELD Binding

2 Bibliothek aus App entfernen

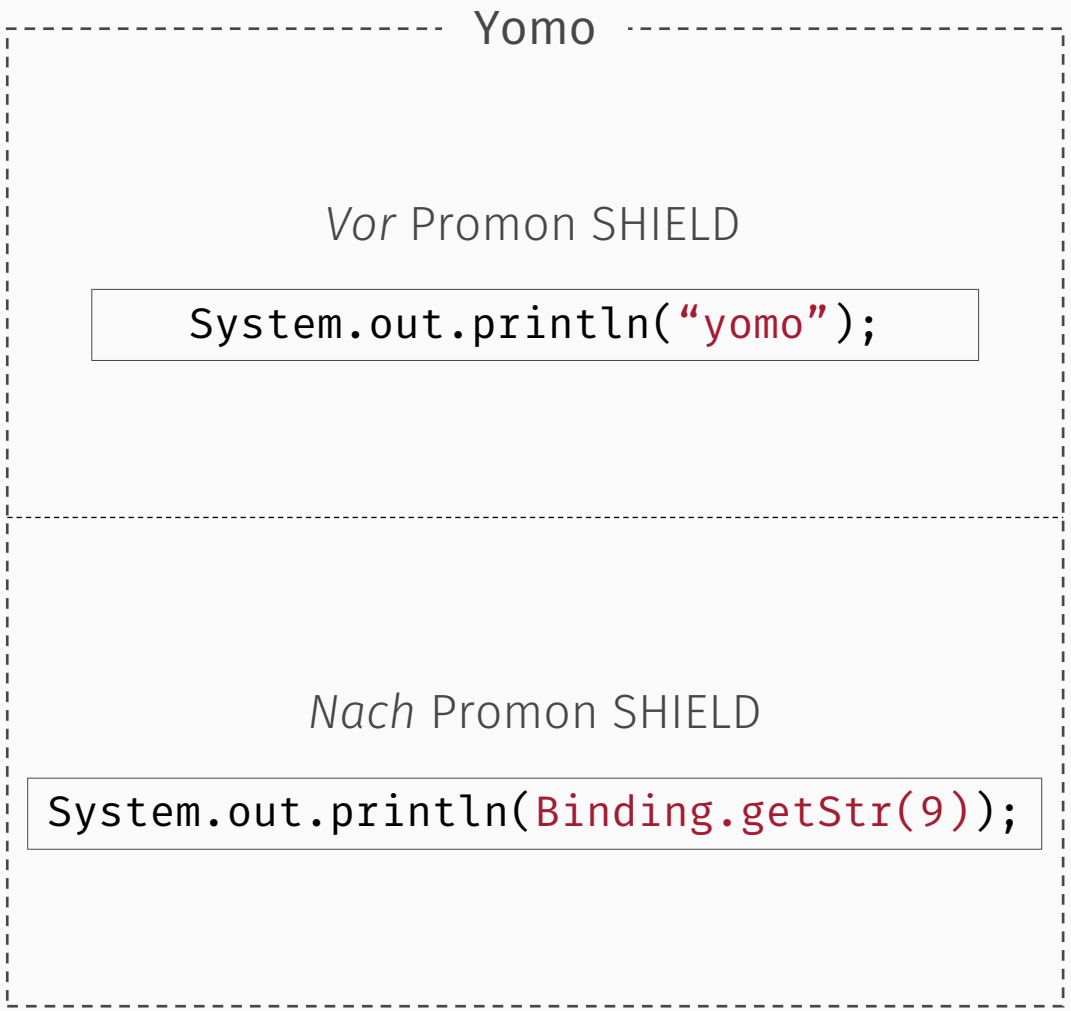
~~1 Bibliothek modifizieren~~

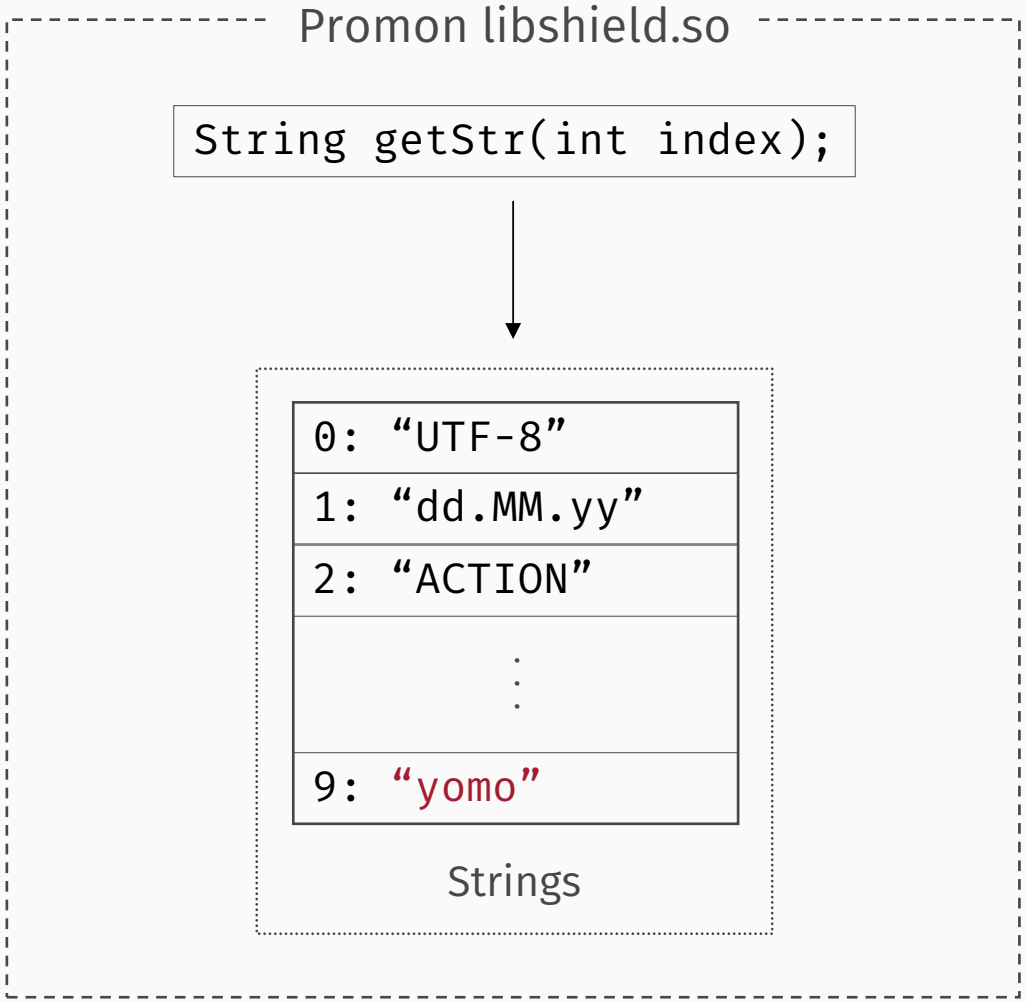


Promon SHIELD Binding

String-Externalisierung

Promon SHIELD Binding: String-Externalisierung

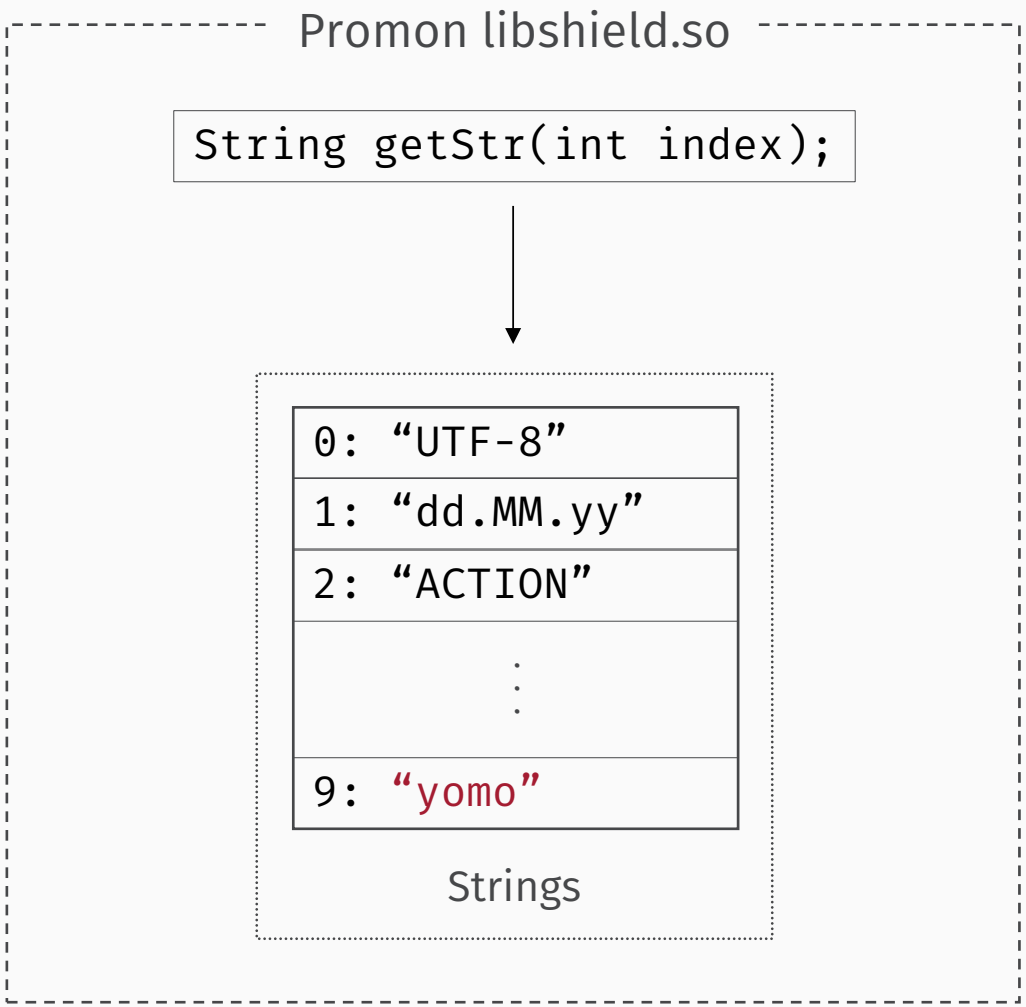




Promon SHIELD Binding: String-Externalisierung

Lösung: String-Mapping erstellen

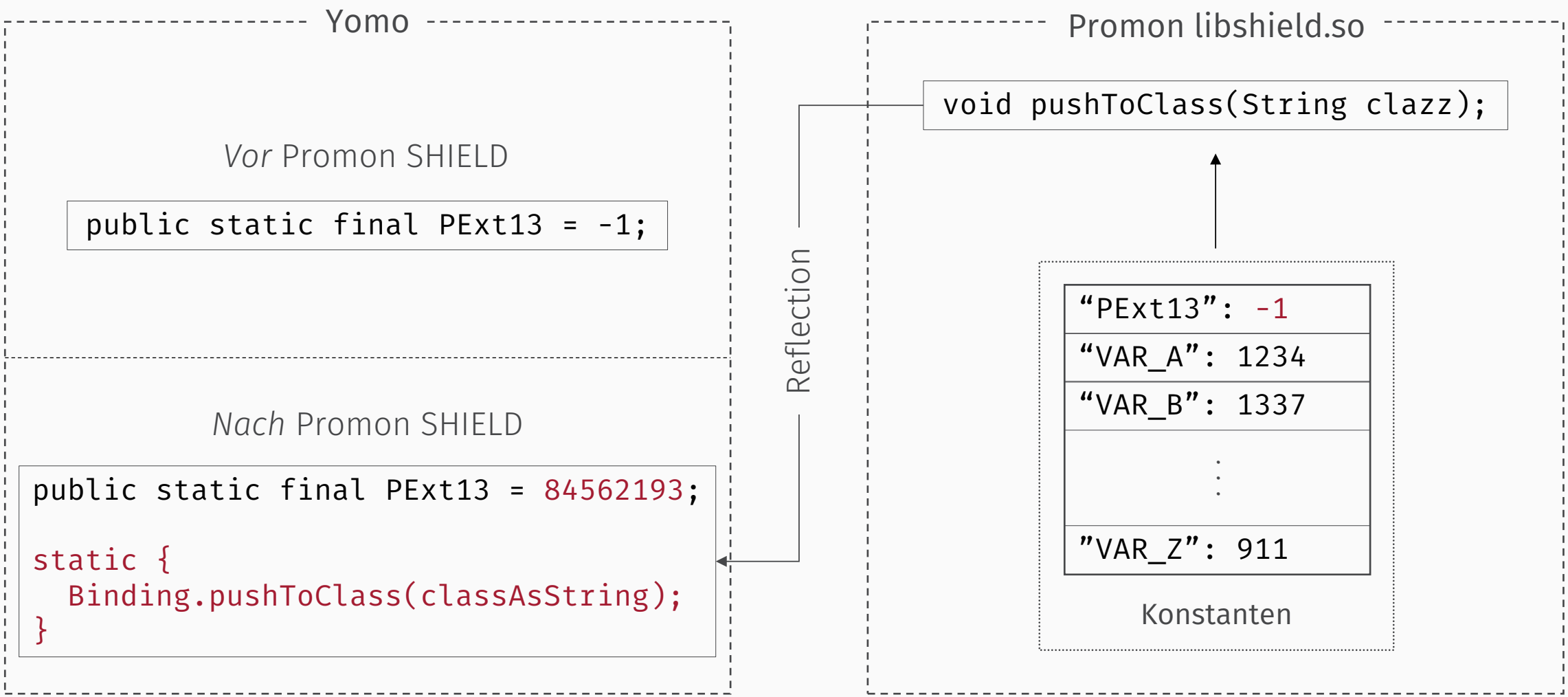
- Höchsten Index *n* von `getStr` ermitteln
- Index-String-Mapping aus *0* … *n* erstellen
- Alternativ: Solange Index *i* erhöhen, bis `getStr(i) == null`



Promon SHIELD Binding

Konstanten-Externalisierung

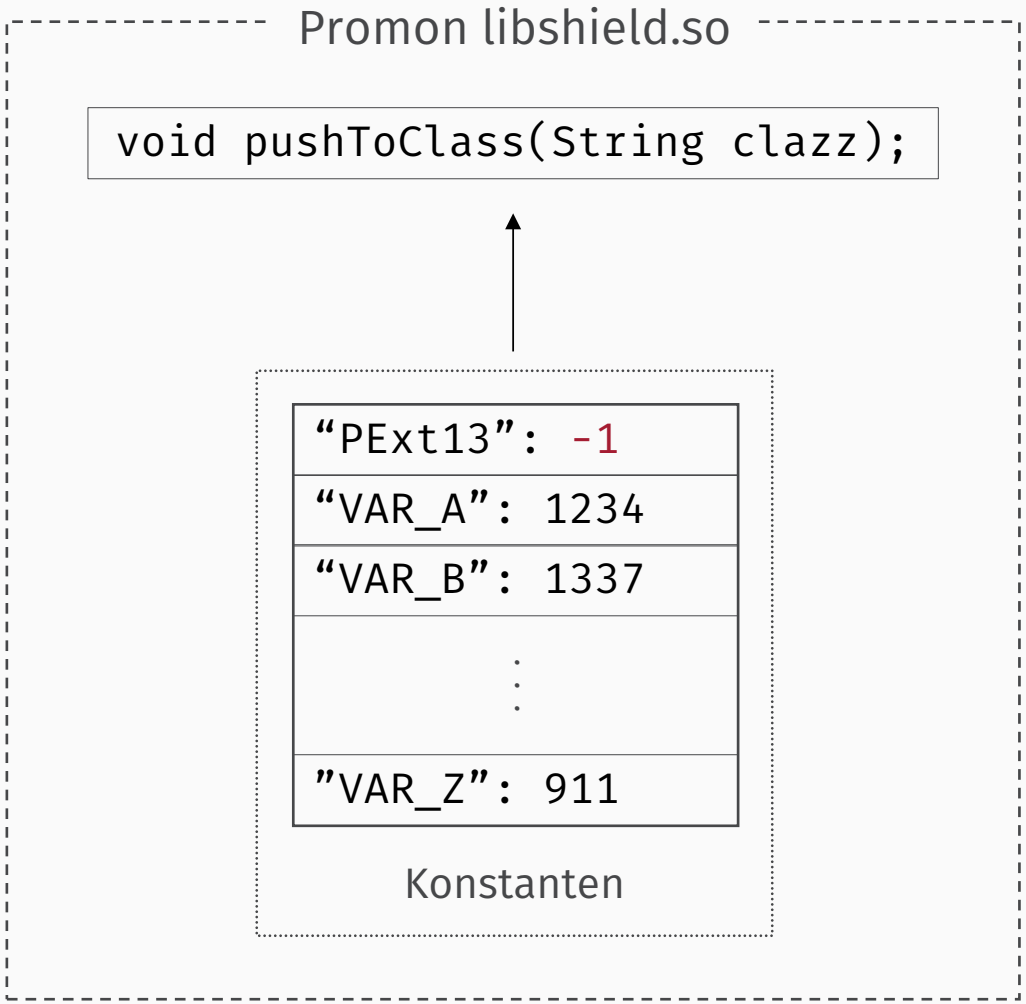
Promon SHIELD Binding: Konstanten-Externalisierung



Promon SHIELD Binding: Konstanten-Externalisierung

Lösung: Konstanten-Mapping erstellen

- Alle Klassen ermitteln, die `pushToClass` aufrufen
- `pushToClass` selbst aufrufen, neue Werte speichern



Promon SHIELD Binding

Client-Zertifikat

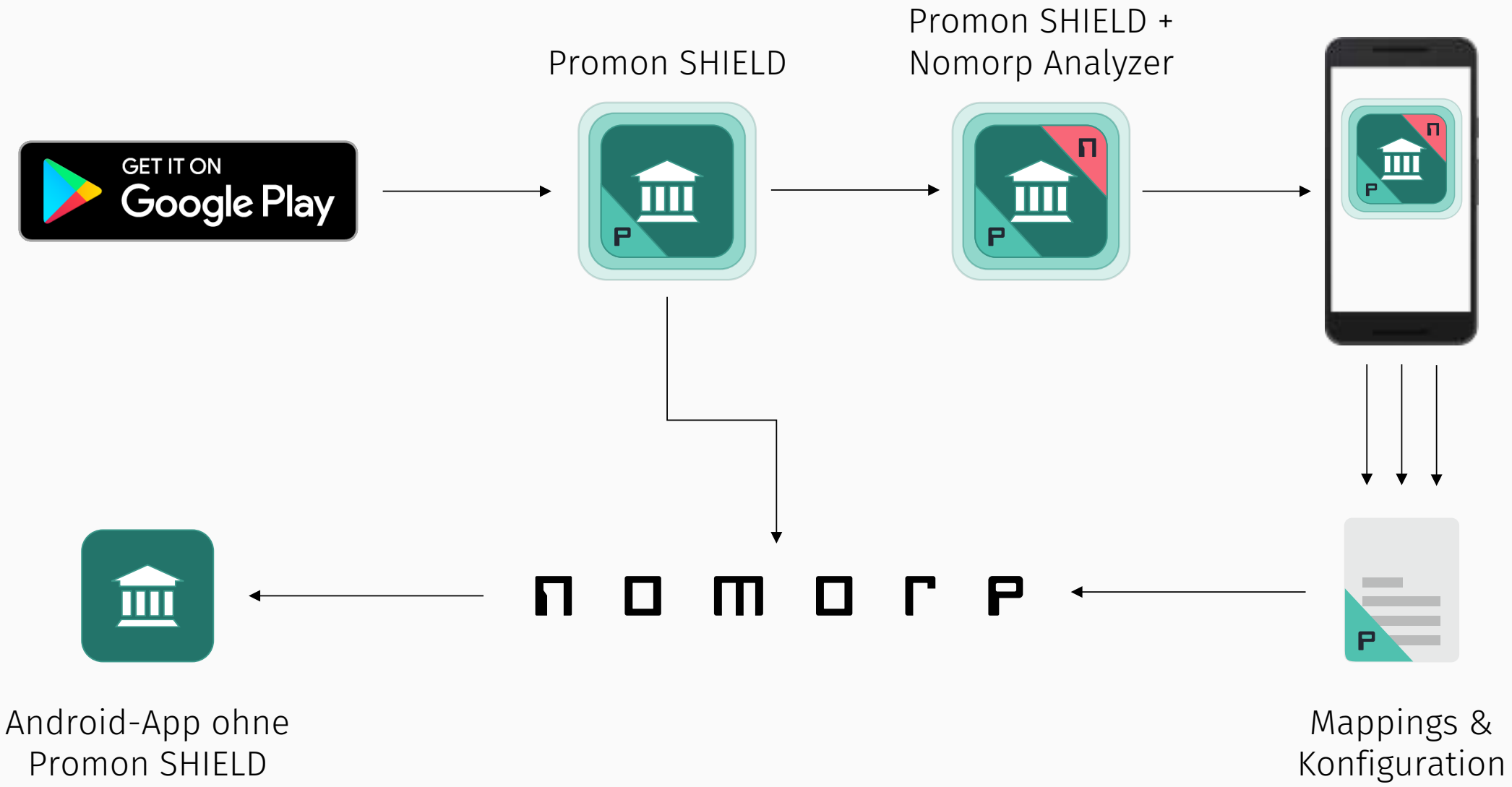
Promon SHIELD Binding: Client-Zertifikat

⇒ Zur Laufzeit Speicherallokationen und –freigaben überwachen

Promon SHIELD Binding: Client-Zertifikat

checkDebugger=1;**exitOnDebugger**=1;**exitOnDebuggerURL**=https%3A%2F%2Fwww.yomo.de%2Fdebugger;**blockJavaDebugger**=1;**checkEmulator**=1;**exitOnEmulator**=1;**exitOnEmulatorURL**=https%3A%2F%2Fwww.yomo.de%2Femulator;**checkRooting**=1;**exitOnRooting**=0;**exitOnRootingHeuristicsThreshold**=26;c**heckHookingFrameworks**=1;**exitOnHookingFrameworks**=1;**exitOnHookingFrameworksURL**=https%3A%2F%2Fwww.yomo.de%2Fexposed;**checkRepackaging**=1;**exitOnRepackaging**=1;**exitOnRepackagingURL**=https%3A%2F%2Fwww.yomo.de%2Frepackage;**applicationSignerCertificate**=MIIDpzCCAo%2Bg...;
clientCertificate=MIIHZDCCBUygAwIBAgIC...;**clientCertificateKey**=MIIJRAIBADANBgkqhkiG...;
blockScreenshots=1;**checkTrustedKeyboard**=1;**exitOnUntrustedKeyboard**=0;**secureTextFieldKeyboard**=policy;**checkTrustedScreenreaders**=1;**blockUntrustedScreenreaders**=1;**exitOnUntrustedScreenreaders**=1;**exitOnUntrustedScreenreadersURL**=https%3A%2F%2Fwww.yomo.de%2Fscreenreader;**checkNativeCodeHooks**=1;**exitOnNativeCodeHooks**=1;**exitOnNativeCodeHooksURL**=https%3A%2F%2Fwww.yomo.de%2Fexposed_nativ;**secureStorageServerRequestTimeout**=30;**oldSecureStorageEncryption**=0;**shutdownImmediately**=0;**addSecureStorageServer**=https%3A%2F%2Fyomo.starfinanz.de%2Fpss%2Fresources%2Fkey;...**addSecureStorageServer**=https%3A%2F%2Fyomo.starfinanz.de%2F;...;**addSecureStorageServerCertificate**=MIIHQjCCBiqgAwIBAgIQ;addTrustedCACertificate=MIIHQjCCBiqgAwIBAgIQ...;**addTrustedScreenreaderSigner**=df37f8d8023ce4776089...;**addTrustedScreenreaderSigner**=df37f8d8023ce4776089;**blockScreenMirroring**=0;**checkRootingDeepScan**=1;**checkScreenMirroring**=0;**deviceManagementServerRequestTimeout**=60;**encryptedLogMaxAgeInDays**=30;**sign**=a86af0fc9530985d73a8...;

Nomorp: Automatisiertes Entfernen des Promon SHIELDs

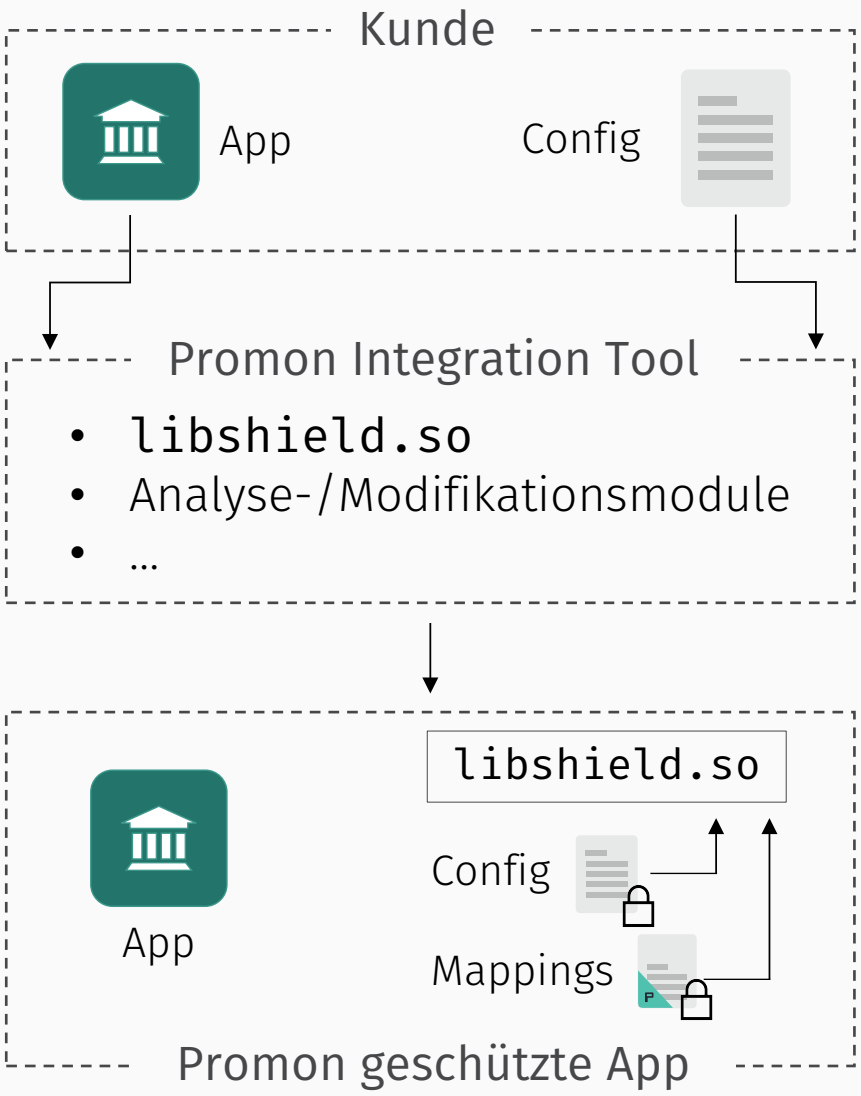


Promon SHIELD

Konfiguration und Mappings

Promon SHIELD: Konfiguration und Mappings

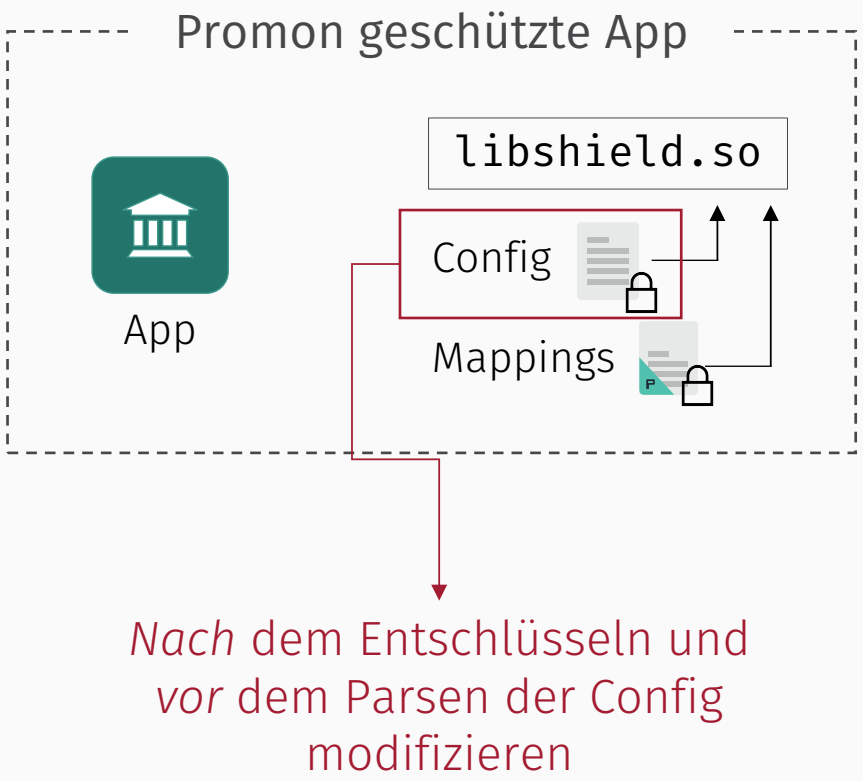
- Die `libshield.so` wird von Promon fertig ausgeliefert
- Mehrere verschlüsselte Dateien werden eingelesen
  - Konfigurationsdatei
  - Mappings, z. B. für `getStr` und `pushToClass`



Promon SHIELD: Konfiguration und Mappings

Config

```
checkDebugger                 = 1; 0;
exitOnDebugger                = 1; 0;
exitOnDebuggerURL             = URL1;

blockJavaDebugger             = 1; 0;

checkEmulator                 = 1; 0;
exitOnEmulator                = 1; 0;
exitOnEmulatorURL             = URL2;

checkRooting                  = 1; 0;
exitOnRooting                 = 0;

checkHookingFrameworks        = 1; 0;
exitOnHookingFrameworks       = 1; 0;
exitOnHookingFrameworksURL    = URL3;

checkRepackaging              = 1; 0;
exitOnRepackaging             = 1; 0;
exitOnRepackagingURL          = URL4;
```



Promon SHIELD

iOS

Promon SHIELD: iOS

Config

```
applicationDelegateClassName          = AppDelegate;
blockDebugger                         = 0;
blockExternalScreens                  = 0;
checkDebugger                         = 1; 0;
checkJailbreak                        = 1; 0;
checkRepackaging                      = 1; 0;
disableAppStoreTrust                  = 0;
disableTestFlightTrust                = 0;
exitOnDebugger                        = 0;
exitOnJailbreak                       = 0;
exitOnRepackaging                     = 0;
exitOnUserScreenshot                  = 0;
keyboardCacheMonitor                  = 1; 0;
preventRuntimeLibraryInjection        = 1; 0;
preventSystemScreenshot               = 0;
preventSystemScreenshotBGColor        = ffffff;
preventSystemScreenshotBlurStrength   = 0;
runtimeLibraryInjectionPreventionMode = policy;
sign                                  = 01959…;
userScreenshotMonitor                 = 1; 0;
```

Promon SHIELD

Zusammenfassung der Angriffe

Promon SHIELD: Zusammenfassung Angriffe

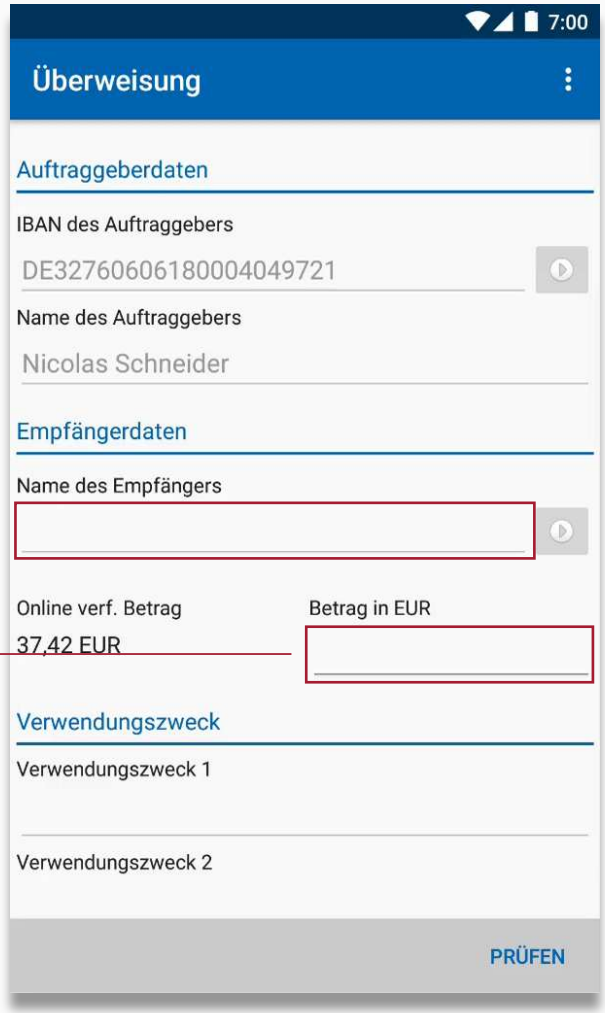
- Zwei verschiedene Angriffe
  1. Mappings und Config extrahieren

     ⇒ Promon SHIELD entfernen
  2. Config umschreiben

     ⇒ Promon SHIELD erhalten
- App danach ungeschützt

  ⇒ Beispielangriff Transaktionsmanipulation

  ⇒ Durch Nomorp fast vollständig automatisiert



VR-Banking

Demo

VR-Banking & VR-SecureGo

Szenario und Ablauf

- Nexus 5X mit Android 7.0 mit Security-Patch-Level von Nov 2016

  ⇒ DirtyCOW noch nicht gepatcht

- Nutzer lädt scheinbar gutartige App aus offiziellem PlayStore

  ⇒ App ersetzt VR-Banking und VR-SecureGo mit einer “nomorped“ Version

- Nutzer führt Transaktion über 15 Euro durch, die durch eine mit 1,23 Euro ersetzt wird

  ⇒ Transaktionsmanipulation

- Bis auf das Bestimmen der IDs für die TextViews *vollautomatisch*

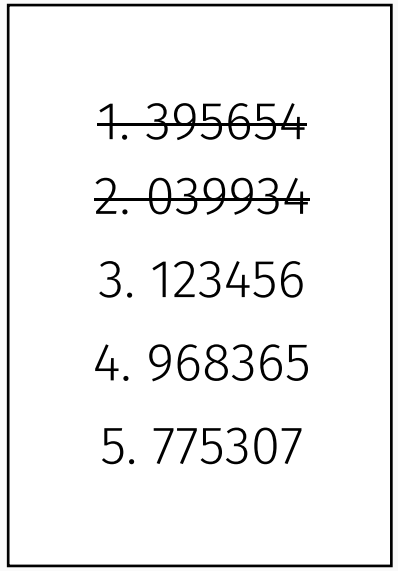
Reaktion und Fazit

Reaktion und Fazit

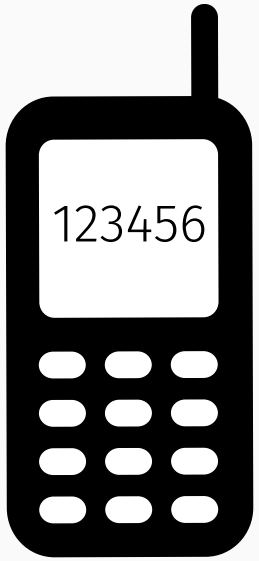
- Seit Ende November in Kontakt mit Promon
- Nette und professionell Reaktion
- Neue Version des Promon SHIELDs
  - Nomorp funktioniert ohne Anpassungen nicht mehr
  - Noch unklar, welche Maßnahmen implementiert wurden
- Um Angriffe komplexer zu machen, braucht es Individualisierung pro App

Reaktion und Fazit

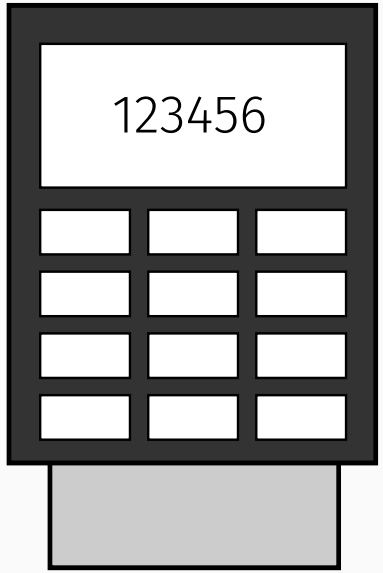
Beliebte Reaktion der Banken: „Bis heute keine Schadensfälle bekannt“



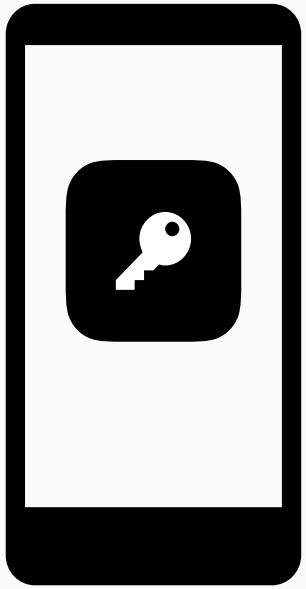
iTAN
25%



smsTAN
36%



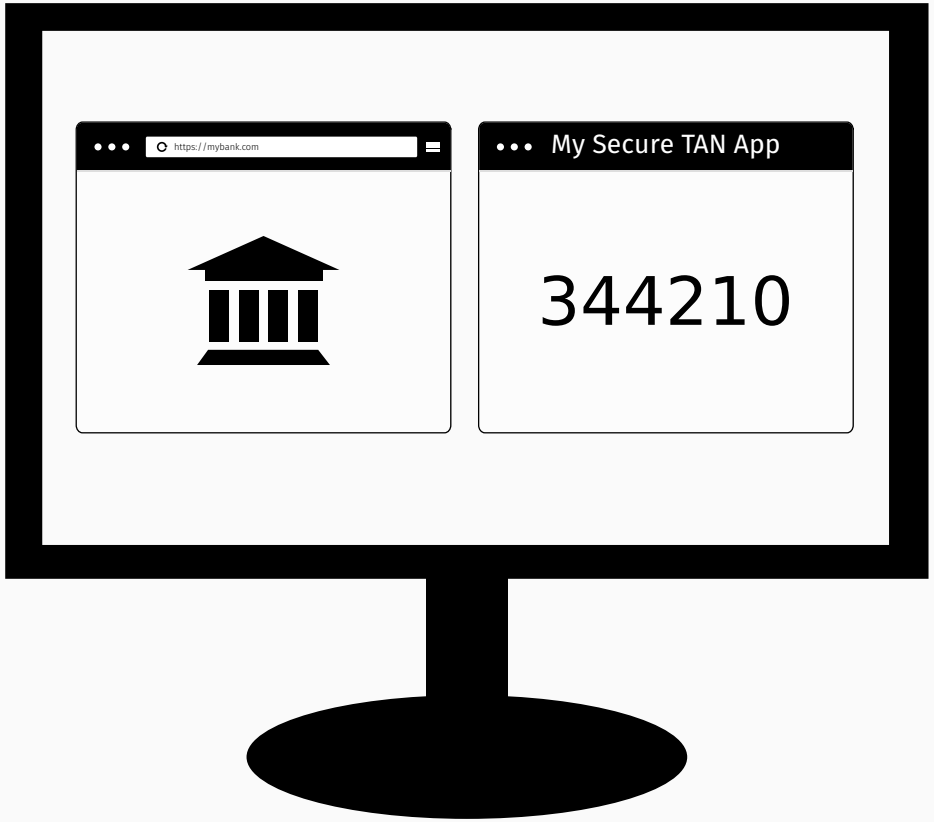
chipTAN
31%



appTAN
5-8%

Fazit

> *Im Bereich des Zahlungswesens hat sich eine besondere Kreativität in der Auslegung der Eigenschaft einer Zweifaktorauthentisierung entwickelt.*
>
> — Jens Bender, Dennis Kügler [BSI]



Ein-Computer-Authentifizierung

Fazit

Ist App-Härtung überhaupt sinnvoll?

Ja, als *zusätzlicher* Schutz

Ist App-Härtung ein Ersatz für unabhängige Zwei-Faktor-Authentifizierung?

Nein

https://www1.cs.fau.de/nomorp

Referenzen

[BSI] Jens Bender, Dennis Kügler: **Was ist starke Authentisierung?** Datenschutz und Datensicherheit 40(4): 212-216 (2016)

[DK] Die Deutsche Kreditwirtschaft: **mobileTAN**. https://die-dk.de/zahlungsverkehr/electronic-banking/mobiletan (aufgerufen am 26.12.2017)

[PS1] Promon AS: **Mobile App Security & Application Protection For Mobile Apps.** https://promon.co/solutions/mobile-app-security-application-protection (aufgerufen am 26.12.2017)

[PS2] Promon AS: **Secure any App in minutes, without affecting the user experience!** https://youtu.be/EoWLTEnddDI (aufgerufen am 26.12.2017)