

Bezpieczeństwo aplikacji typu software token

Mariusz Burdach, Prevenity

Agenda

1. Bezpieczeństwo bankowości internetowej w Polsce
2. Główne funkcje aplikacji typu software token
3. Na co zwrócić uwagę przy wyborze rozwiązania
 - ✓ Parametry
 - ✓ Wpływ na bezpieczeństwo
4. Rekomendacje zespołu Prevenity

Bankowość internetowa w Polsce

- Typowy model:
 1. Dostęp do systemu transakcyjnego (uwierzytelnianie)
 2. Operacje w systemie transakcyjnym (autoryzacja)
- Realizacja punktu 1
 - Hasło statyczne / karta zdrapka
 - Token (hardware/software) + PIN – hasła OTP
 - Certyfikat + PIN
- Realizacja punktu 2
 - Lista haseł jednorazowych / karta zdrapka
 - Token (hardware/software) + PIN – hasła OTP
 - SMS TAN
 - Token (hardware/software) + PIN – „Challenge-Response” - MAC/MDS/TDS

Główne funkcje

1. Dwuskładnikowe uwierzytelnianie (*ang. 2 Factor Authentication*) oparte o hasła jednorazowe (*tzw. OTP*)
2. Zapewnienie drugiego, niezależnego kanału autoryzacji transakcji (*tzw. Out Of Band*)
3. Autoryzacja konkretnej transakcji

Istotne parametry

- Algorytmy i standardy
- Ilość i długość parametrów
- Bezpieczeństwo klucza (shared key)
- Licznik / znacznik czasu
- „Challenge”
- Dystrybucja/Zarządzanie

Algorytmy i standardy

- Generacja haseł jednorazowych (OTP):
 - RFC 4226 – HMAC-Based One-Time Password Algorithm
 - Inne ale oparta o HMAC
 - Szyfrowanie kluczem danych (np. Znacznik czasu)
- Autoryzacja transakcji:
 - OCRA: OATH Challenge-Response Algorithms (draft)
 - Inne ale oparte o HMAC
 - Szyfrowanie kluczem danych (np. rachunek docelowy)
- Najbardziej prawdopodobny atak: brute force
 - Prawdopodobieństwo udanego ataku = $sv/10^d$
 - s – rozmiar okna do synchronizacji
 - v – ilość nieudanych prób po których dostęp jest blokowany
 - d – długość znaków w wartości OTP

HMAC

- Keyed Hash Message Authentication Code (RFC 2104)
 - Weryfikacja integralności
 - Weryfikacja autentyczności
- Parametry:
 - Dane podlegające ochronie
 - Klucz (współdzielony pomiędzy klienta banku i bank)

Results	
Original text	1210100000000000000000003823
MDS	6d7b1da7d886b567d6df18ed470a6143
SHA-1	9c02d2f520069d61bad2974772480dba06f51be4
SHA-256	202cf0ac6a56237ecba339b4d7362c5471f1ce5fcd0cc3bce5ce48977ac07793
SHA-512	2008232a0d392f246b9d2c128bcd0655dbcc2f54ad1cff77ee264c94c991d776ed7a013bee935dcc7db54b5dadf24503ef641760339ec345de71887647782a1

Parametry

- Klucz – długość powinna wynosić co najmniej 32 bajty
- Metoda generowania kluczy

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
00000000	6D	69	64	70	2D	72	6D	73	00	00	00	01	00	00	00	00	midp-rms
00000010	00	00	00	03	00	00	00	02	00	00	00	30	00	00	00	00	0
00000020	00	00	01	2C	D0	04	C3	BE	00	00	00	30	00	00	00	60	,D ĄI 0`
00000030	00	00	00	01	00	00	00	00	00	00	00	30	00	00	00	1B	0
00000040	01	79	8F	6C	B0	C7	D0	F1	AA	95	21	C6	47	69	21	14	y l°CBAŞ*!ÓGi!
00000050	B5	7E	80	1A	97	00	00	00	3C	00	00						u-c <

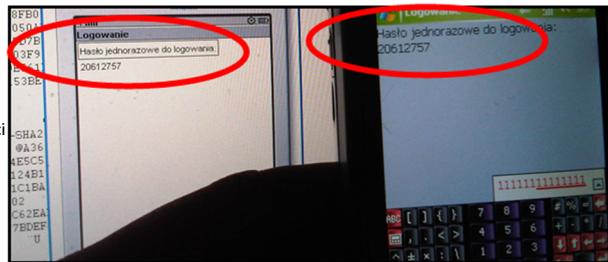
- OCRA = CryptoFunction(K, {[C] | Q | [P | S | T]}) gdzie
 - K – klucz, **wymagany**
 - C - licznik, **opcjonalny**.
 - Q - Challenge question, wymagany, dostarczany przez stronę weryfikującą,
 - P – skrót od PINu lub hasła, **opcjonalny**,
 - S – informacje na temat sesji, **opcjonalne**,
 - T – znacznik czasu, **opcjonalny**.
- Dokument „OATH Challenge-Response Algorithms” oraz RFC 4226 zawiera wytyczne na temat długości niektórych parametrów oraz inne wytyczne na temat implementacji.

Bezpieczeństwo klucza

- Klucz jest przechowywany po stronie banku i klienta
- Ochrona kodem PIN
 - PIN
 - PIN + IMEI
- Podpowiedzi do PIN
 - Algorytm podpowiedzi
 - Ilość podpowiedzi / 10^{\wedge} (długość kodu PIN)

- **Możliwe ataki:**

- Keylogger w urządzeniu mobilnym
- Przechwycenie jednej poprawnie wygenerowanej wartości oraz „zaszyfrowanego klucza” – atak brute force
- Klonowanie aplikacji



Licznik czy Znacznik czasu?

	Licznik	Znacznik czasu
Wymagana synchronizacja	NIE	TAK
Określenie aktualnej wartości	NIE*	TAK
Przewidzenie następnej wartości	NIE*	NIE
Możliwość użycia wygenerowanych uprzednio OTP	TAK	NIE
Ograniczenie „czasu życia” wygenerowanej wartości	NIE	TAK

* Dotyczy scenariusza, gdy intruz nie ma dostępu do telefonu ofiary. Innym istotnym parametrem jest długość licznika.

„Challenge”

- Nie bazuje na funkcjach kryptograficznych
- Opracowany przez producenta oprogramowania
- Nośnik wybranych informacji o szczegółach autoryzowanej transakcji
- Ograniczenia:
 - Nie nadaje się do autoryzacji niektórych transakcji niefinansowych – dotyczy to generalnie aplikacji tego typu
 - Nie nadaje się do autoryzacji transakcji zbiorczych
 - Kolizje
 - 1:10000 (dla 4 cyfr)
 - 1:100000 (dla 5 cyfr)

```
C:\Python26>python.exe kolizje.py
PI12101000000000000000000003: 23
PI12101000000000000000000013: 23
PI12101000000000000000000023: 23
PI12101000000000000000000032: 23
PI12101000000000000000000042: 23
PI12101000000000000000000052: 23
PI12101000000000000000000062: 23
PI12101000000000000000000071: 23
```

© 2011 Prevenity Sp. z o.o. Wszelkie prawa zastrzeżone.

prevenity

Dystrybucja / Zarządzanie

- Aplikacja J2ME czy natywna?
- Podpis cyfrowy
- Aktywacja
 - Proces personalizacji
 - Przekazanie kodu aktywacyjnego do klienta
 - Długość kodu aktywacyjnego i jego budowa
- Zarządzanie
 - Instalacja nowej wersji / poprawki / aplikacji na nowym telefonie
 - Zmiana kodu PIN

© 2011 Prevenity Sp. z o.o. Wszelkie prawa zastrzeżone.

prevenity

Możliwe ataki - podsumowanie

Wektor ataku	Możliwość wystąpienia ataku
Błędy implementacyjne	?
Infekcja urządzenia mobilnego <ul style="list-style-type: none">Nadpisanie aplikacjiInstalacja oprogramowania typu keylogger lub koń trojańskiRekonfiguracja telefonu	średnie
Ataki typu brute force	małe
Ataki na kod PIN	małe
Kolizje	małe
Phishing haseł OTP	małe
Klonowanie aplikacji	małe

Rekomendacja

- Szczegółowe testy rozwiązania (włączając przegląd kodu) i identyfikacja ryzyka
- Szczegółowe testy wdrożonego systemu (po stronie klienta i banku)
- Monitorowanie transakcji po stronie banku

Dziękuję z uwagę

Mariusz.Burdach@prevenity.com