

***Bankowość internetowa
vs
Malware***



SecuRing

Wojciech Dworakowski



Agenda

Wprowadzenie:

- Malware a bankowość internetowa

Stosowane funkcje bezpieczeństwa

- Wpływ na ryzyko malware, używalność, koszty:
 - Uwierzytelnienie
 - Autoryzacja transakcji
- Spotykane błędy koncepcji i implementacji

Podsumowanie



Malware a bankowość internetowa

o://www.dia.

Zagrożenie: „Użytkownik może mieć na stacji wrogie oprogramowanie”

- No dobrze – ale to przecież stacja użytkownika i jego problem.
- W praktyce – ciężko jest jednoznacznie wykazać „winę” użytkownika.
- Bank raczej stara się unikać problemów i ewentualnych sporów z klientem.



Malware a bankowość internetowa

o://www.dla.

Wpływ zagrożenia na ryzyko

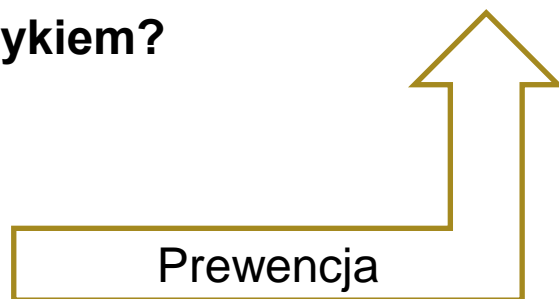
Ryzyko =	Prawdopodobieństwo wystąpienia	x	Potencjalne skutki
	Duże		Duże
	Bank ma na nie niewielki wpływ		Utrata środków Utrata zaufania

Co zrobić z tym ryzykiem?

Zaakceptować?

Delegować?

Ograniczać?





o://www.dfa.



ZABEZPIECZENIA



Uwierzytelnianie

Cel:

- Ograniczenie ryzyka kradzieży tożsamości klienta

Pożądane cechy:

- Ogranicza ryzyko podejrzenia i podsłuchania
- Utrudnia manipulację klientem w celu wyłudzenia „hasła”
- Jest wygodne w użyciu

Metody:

- hasło statyczne
- hasło maskowane
- podpis elektroniczny
- metody dwuskładnikowe



Uwierzytelnianie – Hasło statyczne

Wygoda użytkowania

- Wygodne

Koszty

- Niskie

Wpływ na ryzyko (malware)

- Praktycznie żaden



Uwierzytelnianie – Hasło maskowane

■	■	□	■	□	■	□	■	■	□	□
1	2	3	4	5	6	7	8	9	10	11

Wygoda użytkownika

- Uciążliwe, ale akceptowalne (raczej dlatego, że jest powszechnie stosowane)

Koszty

- Niskie

Wpływ na ryzyko (malware)

- Pozornie – zabezpieczenie ogranicza ryzyko, bo malware musi podsłuchać kilka prób uwierzytelnienia.
- Czy rzeczywiście tak jest?



Uwierzytelnianie – Hasło maskowane

o://www.dla

Błędy implementacji

- Hasło „pseudomaskowane”
 - Na pozycjach ukrytych – znaki hasła w `<input type="hidden"/>`
- Źle dobrane proporcje: ilość znaków w hasle / ilość znaków w masce
 - Dużo znaków „ukrytych” → rośnie prawdopodobieństwo ataku brute-force
 - Dużo znaków „odkrytych” → mniejsza ilość prób koniecznych do zebrania informacji o wszystkich znakach
- Przy kolejnej próbie uwierzytelnienia po niepowodzeniu trzeba pytać ciągle o te same znaki (ta sama maska)
 - Inaczej intruz spróbuje kilka razy, aż maska będzie „odpowiednia”

Problemy

- Ciężko jest równocześnie zastosować przechowywanie haseł użytkowników w postaci nieodwracalnej



Uwierzytelnianie – Hasło maskowane

o://www.dfa.

Największa wada

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19
M O J Ę T R U D N E H A S Ł O 1 2 7 0

Hasło:

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	
█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█	█



Uwierzytelnianie – „Podpis elektroniczny”

o://www.dfa.

Logowanie

Użytkownik Wioletta Bieniek
Data i czas logowania 2007-11-12 09:36

Podpisz

Podpisz dyspozycję

W celu zakończenia procesu logowania proszę wpisać ponownie hasło

Nazwisko i imię: Wioletta Bieniek

Data logowania: 2007-11-12 09:36

Proszę podać hasło:



Podpisz

Anuluj

Źródło: ING Bank Śląski S.A.



Uwierzytelnianie – „Podpis elektroniczny”

o://www.dla.

Wygoda użytkowania

- Wygodne, ale „początkujący” użytkownik może mieć problemy
- Zazwyczaj wymaga zainstalowania dodatkowego oprogramowania



Koszty

- Klucz z pliku – niskie
- Klucz na karcie – średnie (karty, czytniki, wsparcie)



Wpływ na ryzyko (malware)

- Klucz z pliku – praktycznie żaden
- Klucz na karcie – znaczne ograniczenie ryzyka - teoretycznie



Uwierzytelnianie – „Podpis elektroniczny”

o://www.dfa.

Mebroot (klucz w pliku)

Pobierz klucz:

Podaj hasło do klucza:



Uwierzytelnianie – Metody dwuskładnikowe

o://www.dfa.

Coś co wiesz + coś co masz

- Hasło + ? (token, sms, karta chipowa, aplikacja w telefonie...)

Wygoda użytkowania

- Zależy jakie to będą „składniki”
- Złożoność na pewno większa niż przy jednym składniku

Koszty

- Hasło + SMS: koszt sms-ów
- Hasło + token: koszt tokenów, wsparcie
- Hasło + karta: koszt czytników, kart, wsparcie

Wpływ na ryzyko (malware)

- Znaczące ograniczenie ryzyka, pod warunkiem, że:
 - dane uwierzytelniające są „jednorazowe”
 - mamy zaufanie do „drugiego składnika”



Uwierzytelnianie a malware

Stosowanie nowych zabezpieczeń → Zmiana taktyki malware

- Celem nie jest pozyskanie hasła. Celem jest wyprowadzenie środków z konta.
- Zamiast przechwytywać dane uwierzytelniające, lepiej zaczekać aż ofiara się sama uwierzytelnia i wtedy działać
- W Polsce około 2008 – ataki przy użyciu malware ZBot / ZeuS

Zmiana zagrożenia → Nowe zabezpieczenia

- Zabezpieczenie samych transakcji
- Autoryzacja transakcji



Autoryzacja transakcji

Cel:

- Ograniczenie ryzyka wykonywania transakcji bez wiedzy klienta

Pożądane cechy:

- Utrudnia manipulację w celu wyłudzenia „danych autoryzujących”
- Jest wygodne w użyciu

Metody:

- hasło jednorazowe niezwiązane z transakcją
 - kody TAN („zdrapka”, matryca)
 - token oparty na czasie/liczniku
 - kod SMS
- hasło jednorazowe związane z transakcją
 - kod SMS
 - „podpis elektroniczny”
 - tokeny challenge-response



Autoryzacja transakcji – Karty kodów jednorazowych (TAN)

o://www.dla.

Wygoda użytkowania

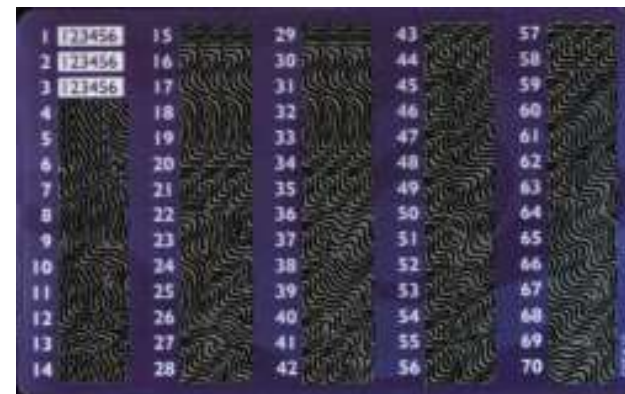
- Średnia – klient musi mieć kody zawsze przy sobie, kody kiedyś się skończą i trzeba zamówić nowe

Koszty

- Średnie – w szczególności: drukowanie i rozsyłanie kodów

Wpływ na ryzyko (malware)

- Nikły
- Typowy przykład zabezpieczenia, które działało „na teraz”
- Po wprowadzeniu kodów TAN twórcy malware szybko zmienili taktykę





Autoryzacja transakcji – Karty kodów jednorazowych (TAN)

o://www.dfa.

Wyłudzanie kodów TAN

Logowanie.

Błąd 0071631: Odnotowano niepomyślną próbę logowania! Została jedna próba!

Błąd 0071631: Odnotowano niepomyślną próbę logowania! Została jedna próba!

Aby system mógł zidentyfikować Państwo jako właściciela konta,
proszę wpisać hasła jednorazowe i zalogować się ponownie.

Drugi poziom bezpieczeństwa - Hasła jednorazowe

01	03	05	07	09	11	13	15	19	21
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
25	27	31	33	37	39	43	45	47	49
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Podaj kod nr 33 Podaj kod nr 38



Autoryzacja transakcji – Karty kodów jednorazowych (TAN)



Kod TAN nie jest związany z transakcją

- Podśluchany kod TAN może posłużyć do autoryzowania dowolnej transakcji
- Malware może pokazać w przeglądarce inną transakcję niż ta, która faktycznie się wykona.

PRZELEW ZEWNĘTRZNY	
NAZWA	GAZOWNIA
NR KONTA	67 7773 0000 0000 9999
KWOTA	152,40

WPROWADŹ KOLEJNY KOD

nr_konta=661111000000006666
kwota=1000
KOD=3872



Przykład ataku na jeden z banków przy użyciu malware Zeus:

- Modyfikacja rachunku docelowego i kwoty (czasami również opisu)
- Dane nie były zaszyte tylko były pobierane z Internetu (ciężiej zablokować konta „mułów”)
- Umiał „obsłużyć” rachunki oszczędnościowe



Autoryzacja transakcji – Token oparty na czasie lub liczniku



Wygoda użytkowania

- Token trzeba zawsze mieć przy sobie
- Czasami trzeba go wymieniać na nowy
- Może się rozsynchronizować

Koszty

- Tokeny, wsparcie

Wpływ na ryzyko (malware)

- Kod z tokena nie jest powiązany z transakcją
- Malware może podmieniać transakcję w locie (tak jak dla kodów TAN)
- W sumie – skuteczność podobna do kodów TAN
- Dodatkowo daje klientowi fałszywe poczucie bezpieczeństwa



Autoryzacja transakcji – Kody SMS – bez opisu transakcji

o://www.dla.

Wygoda użytkowania

- Trzeba mieć przy sobie komórkę
- Obecnie powszechnie akceptowane (bo powszechnie stosowane)

Koszty

- Znaczne: koszty sms-ów
- Można ograniczać przez autoryzowania tylko niektórych (ale których?) transakcji

Wpływ na ryzyko (malware)

- Jeśli razem z kodem SMS nie są przesyłane dane transakcji to skuteczność i metody ataku takie same jak dla innych metod niepowiązanych z transakcją (TAN, token)



Autoryzacja transakcji – Kody SMS – z opisem transakcji

Wpływ na ryzyko (malware)

- Skuteczne, o ile użytkownik zweryfikuje dane transakcji
- Jeśli nie → tak samo jak dla TAN, tokenów, kodów SMS bez opisu transakcji
- Użytkownicy przyzwyczajają się do „formatu” SMSa i z czasem przepisują kod co raz bardziej automatycznie
 - Zmianie kolejności (może drażnić użytkowników)
 - Dodatkowy SMS przy transakcjach „nietypowych” (czyli jakich?)





Autoryzacja transakcji – Kody SMS – z opisem transakcji

o://www.dfa.

Błędy implementacji

- Treść SMS, którą można sterować z poziomu przeglądarki (np. jest przesyłana w parametrze ukrytym)
- Zamiast nr rachunku docelowego – nazwa odbiorcy
- Ilość cyfr z nr rachunku – Ile cyfr jednoznacznie (?) identyfikuje rachunek



Autoryzacja transakcji – „Podpis elektroniczny”

- Transakcje są podpisywane przy użyciu klucza zapisanego na karcie kryptograficznej. Klucz nie opuszcza karty.
- Podczas autoryzacji, komponent podpisujący pokazuje użytkownikowi podpisywaną transakcję. Użytkownik ją weryfikuje i wpisuje PIN do karty/klucza.

Wygoda użytkownika

- Wymaga zainstalowania dodatkowego oprogramowania

Koszty

- Średnie / wysokie (karty, czytniki, wsparcie)

Wpływ na ryzyko (malware)

- Tak jak w przypadku kodu SMS – zależy od tego czy użytkownik zweryfikuje transakcję przed podpisaniem
- Malware może zmienić to co jest pokazywane użytkownikowi



Autoryzacja transakcji – Token challenge-response

- Użytkownik musi przepisać *challenge*

Wygoda użytkowania

- Wymaga dodatkowego oprogramowania na telefonie
- lub dodatkowego urządzenia
- *Challenge* musi „przenieść” informacje o transakcji do zweryfikowania
 - Nr rachunku (fragment) docelowego
 - Kwota
- Im dłuższy *challenge* tym lepiej
 - Weryfikacja parametrów transakcji
 - Unikalność



Źródło: <http://pekao.com.pl>



Źródło: <http://iss.thalesgroup.com>



Źródło: <http://emue.com>



Autoryzacja transakcji – Token challenge-response

o://www.dfa.

Koszty

- Oprogramowanie lub czytnik, wsparcie (!)

Wpływ na ryzyko (malware)

- Mniejszy wpływ ignorancji użytkownika (musi przepisać dane transakcji)
 - ale jeśli parametry transakcji będą „zakodowane” w *challenge* (kompresja)
 - rozwiązanie to ma te same wady co kod SMS z informacją o transakcji
- Czy telefon to urządzenie zaufane?
 - Wyłudzenie nowej karty SIM
 - ZeuS „Man-in-the-mobile”
 - Jak zainstalować malware na komórce?



Man in the Mobile

o://www.dia.

INFORMACIÓN IMPORTANTE ACERCA DE LA SEGURIDAD

Por favor elija la marca y el modelo de su teléfono

Nokia 5130 XpressMusic

¿Si el teléfono no existe en la lista?

Su teléfono : Nokia 5130 Xpress

El número de teléfono registrado

El link para la instalación del certificado



baje e instale la aplicación.

Źródło: <http://securityblog.s21sec.com/2010/09/zeus-mitmo-man-in-mobile-i.html>





Autoryzacja transakcji – Błędy implementacji

o://www.dfa.

Błędy implementacji – przykłady:

- Możliwość „przeskoczenia” operacji autoryzacji
- Zmianienie parametrów transakcji podczas (lub po) autoryzacji
- Nadużycie funkcji „przelewów zaufanych”

Wpływ na ryzyko

- Duży – obejście konieczności autoryzacji transakcji

Niezależne od stosowanej metody



Inne zabezpieczenia

- Klawiatura wirtualna
- Obrazek antyphishingowy

Czy to naprawdę coś daje?

Metody „tradycyjne”

- Limity
- Powiadomienia
- Fraud detection



Podsumowanie

Dalszy rozwój zabezpieczeń =
mniejsza wygoda + większe koszty

Czy ryzyko na dzień dzisiejszy jest
akceptowalne?

Problemy:

- Ignorancja użytkowników
- Błędy implementacji





Pytania?



Wojciech Dworakowski

wojciech.dworakowski@securing.pl

Tel.: 12 4252575, 506 184 550