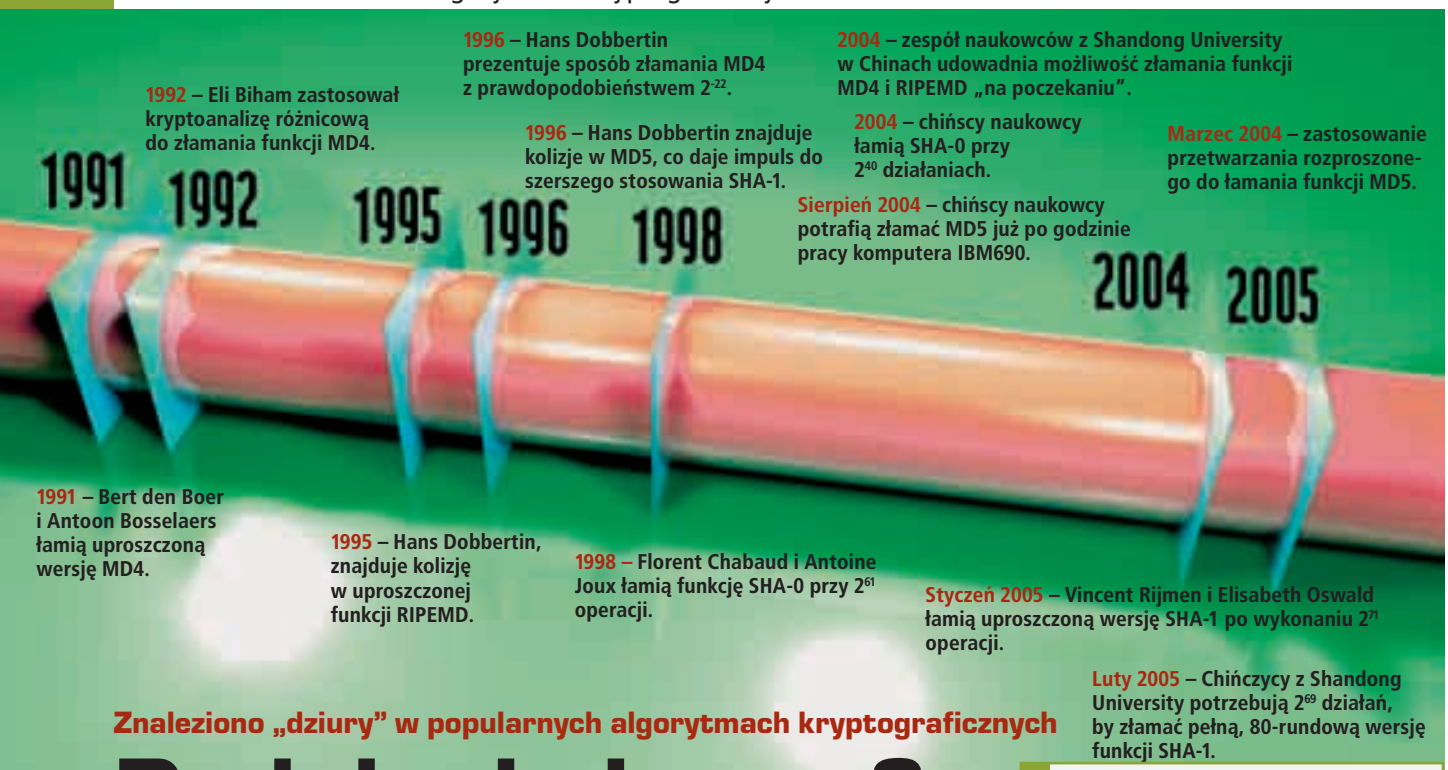


Znaleziono „dziury" w popularnych algorytmach kryptograficznych

Podpis do kosza?

Chińscy naukowcy zaprezentowali metody, dzięki którym można złamać funkcje skrótu MD5 i SHA-1. Co prawda potrzeba do tego potężnej mocy obliczeniowej, ale czy ulepszenie tych metod nie jest tylko kwestią czasu, tak jak to było w przypadku MD4?

Bartosz Żółtak

W ciągu ostatnich kilku miesięcy świat obiegły informacje o złamaniu popularnych w kryptografii algorytmów SHA-0, MD5 i SHA-1. Wydarzenia te nie nastąpiły co prawda po sobie lawinowo, ale i tak pokazują pewną niepokojącą tendencję do znajdowania luk w metodach uznawanych do tej pory za bezpieczne. Czy to oznacza, że przeciętny użytkownik komputera powinien zacząć się obawiać korzystania z bankowości elektronicznej lub poufnej poczty? Na szczęście nie jest aż tak źle, ale przyjrzyjmy się sprawie bliżej.

Odcisk palca

MD5 i SHA-1 to popularne algorytmy kryptograficzne, używane m.in. do tworzenia powszechnie stosowanych w Sieci podpisów cyfrowych. Korzystamy z nich na co dzień, na przykład podczas przeglądania stron zabezpieczonych protokołem SSL (Secure Sockets Layer) czy odczytywania e-maili kodowanych za pomocą PGP (Pretty Good Privacy). Zwykle jednak nie zdajemy sobie sprawy z istnienia tych funkcji ani też z istotnej roli, jaką pełnią one przy potwierdzaniu autentyczności informacji (patrz: ramka 901). Wartości przez nie obliczane stanowią rodzaj cyfrowego odcisku palca i powinny być unikatowe dla dowolnych danych (np. plików).

Podpisując cyfrowo dokument czy też nawiązując bezpieczne połączenie SSL, korzystamy zatem z tzw. funkcji hashujących (nazywanych też często funkcjami skrótu), które obliczają wartość cyfrowego odcisku palca dla naszego dokumentu lub dla danych stwierdzających naszą tożsamość. Ostatecznie to właśnie na przykład 20-bajtowy ciąg danych decyduje o tym, czy dokument przesyłany przez Sieć jest autentyczny. O ile sprawa dotyczy rzeczy błahych, nie ma o co kruszyć kopii. Wyobraźmy sobie jednak, że mówimy o autentyczności umowy kupna-sprzedaży, gdzie w grę wchodzą prawdziwe pieniądze. Oczywiście powyższy tok rozumowania jest dość uproszczony, ale pokazuje kluczową rolę algorytmów takich jak SHA-1 w weryfikowaniu autentyczności informacji.

Jak szóstkę w totka

Jeśli przyjmiemy, że dane wejściowe mogą być dowolnie długie, a obliczona wartość funkcji hashującej ma wielkość 160 bitów (czyli 20 bajtów, jak w przypadku SHA-1), to wynika z tego, że – przynajmniej w teorii – zawsze będą istnieć różne informacje, które po przetworzeniu przez algorytm zwrócą tę samą wartość. Wynika to wprost z faktu, że liczba wszystkich możliwych kombinacji 160-bitowego odcisku palca jest skończona w odróżnieniu od otwartego zbioru podpisywanych plików. Nie ma w tym nic złego, dopóki prawdopodobieństwo znalezienia dwóch różnych danych wejściowych, które zwrócą tę samą wartość funkcji skrótu, jest bardzo niskie. W przypadku SHA-1 powinno ono wynosić 2^{-80}, czyli tyle samo co szansa trafienia szóstki w Dużego Lotka 80 trylionów razy z rzędu (1 trylion to milion miliardów). Według specjalistów takie ryzyko można bez obaw zaakceptować i uznać algorytm za bezpieczny.

Kryptografia okazuje się jednak dziedziną płatającą figle i taką właśnie niespodziankę zafundował ostatnio światu zespół chińskich naukowców (Xiaoyun Wang, Yiqun Lisa Yin oraz Hongbo Yu) z Shandong University. Przedstawili oni sposób na uzyskanie dwóch wiadomości, które dadzą tę samą wartość funkcji SHA-1, ale w znacznie łatwiejszy sposób. Wymaga to wykonania „tylko" 2^{69} operacji. Tym samym, jeśli mamy dokument podpisany cyfrowo, to musimy się liczyć z ryzykiem, że ktoś, stosując opracowaną przez

O autorze

Bartosz Żółtak jest absolwentem Wydziału Informatyki i Zarządzania Politechniki Wrocławskiej oraz autorem jednokierunkowej funkcji szyfrującej VMPC. Była ona prezentowana m.in. na międzynarodowej konferencji kryptograficznej FSE 2004 w Indiach, gdzie spotkała się z uznaniem specjalistów. Na funkcji VMPC bazuje także stworzona przez autora aplikacja VMPC Data Security. Więcej informacji o Bartoszu Żółtaku i VMPC można znaleźć pod adresem www.VMPCfunction.com.

Zastosowania funkcji skrótu

Funkcja	Zastosowanie
MD5	PGP, GPG, TLS/SSL, Kerberos, podpisy cyfrowe
SHA-1	PGP, SSL, HMAC, S/MIME, IPSec, SSH, TCPA, podpisy cyfrowe[1)]

1) oficjalny standard w USA

OPIS	BRIEF	KATEGORIA
Luki w algorytmach kryptograficznych.	Z szyfrowania bazującego na funkcjach MD5 i SHA-1 korzystamy niemal codziennie, przeglądając na przykład zabezpieczone strony WWW. Czy odkrycie luk w tych algorytmach oznacza, że nasze elektroniczne bezpieczeństwo jest zagrożone?	Software | Bezpieczeństwo danych | Szyfrowanie danych

Funkcja hashująca a podpis cyfrowy

Do stworzenia podpisu cyfrowego potrzebne są dwa podstawowe narzędzia: asymetryczny algorytm szyfrujący z kluczami prywatnym i publicznym (np. RSA) oraz funkcja hashująca. Dane zakodowane za pomocą klucza publicznego mogą być odczytane tylko przez osoby mające przechowywany bezpiecznie klucz prywatny (i odwrotnie – wiadomości zaszyfrowane kluczem prywatnym odczyta tylko ten, kto ma dostęp do klucza publicznego).

Załóżmy, że Ala chce podpisać cyfrowo swoją wiadomość do Oli. Zaczyna więc od obliczenia tzw. wartości funkcji hashującej HASH0 np. za pomocą algorytmu MD5. Następnie Ala szyfruje tę wielkość swoim kluczem prywatnym, uzyskując HASH0', które staje się w tym momencie podpisem cyfrowym.

Ola, chcąc potwierdzić autentyczność informacji, oblicza wartość HASH1 dla otrzymanej wiadomości, korzystając z tej samej metody co Ala (MD5), i deszyfruje za pomocą klucza publicznego wielkość HASH0' z podpisu. Jeśli uzyskana w ten sposób wartość HASH0 jest taka sama jak obliczona HASH1, Ola może uznać, że to na pewno wiadomość od Ali.

Załóżmy jednak, że Bartek chce podrobić podpis Ali i przesłać Oli spreparowaną wiadomość. Musiałby zatem tak przygotować swoją informację, by obliczona dla niej wartość funkcji hashującej była taka sama jak w wypadku oryginalnych danych. Jeśli więc Ala zastosuje słaby, umożliwiający złamanie algorytm do wygenerowania HASH0, otworzy to Bartkowi drogę do oszukania Oli.

Bez paniki

Krystian Matusiewicz, doktorant Division of Information and Communication Sciences na australijskim Macquarie University, zajmujący się kryptoanalizą funkcji skrótu.

➔ Ostatnie ataki zespołu pani X. Wang na MD5, SHA-1 oraz kilka innych funkcji skrótu wywodzących się z rodziny MD spowodowały zrozumiałe poruszenie w świecie kryptoanalityków. Zapewne też wielu użytkowników komputerów i Internetu zadaje sobie pytanie, jak rezultaty tych badań wpłynęły lub wpłyną na ich bezpieczeństwo.

W obecnej chwili nie ma powodu do paniki (większymi zagrożeniami są np. kradzież tożsamości czy phishing), jednak sytuacja funkcji MD5 i SHA-1 zmieniła się zdecydowanie. Teoretyczne ataki na MD5 pojawiły się już pod koniec lat 90. i były to pierwsze sygnały podważające bezpieczeństwo tego algorytmu. Obecny atak jest na tyle praktyczny, że możliwe staje się np. konstruowanie dwóch różnych programów mających taki sam skrót. Z pewnością jest to ostatni dzwonek, by wyeliminować MD5 z zastosowań wymagających odporności na kolizje.

W przypadku SHA-1 do tej pory nie znamy żadnych szczegółów ataku, ale złożoność 2^{69} pokazuje, że mamy jeszcze trochę czasu, zanim będzie on ulepszony na tyle, by zagrozić jakimkolwiek praktycznym zastosowaniom tej funkcji.

nich metodę i dysponując odpowiednią mocą obliczeniową, może nasz podpis po prostu sfałszować. Sfałszować, a więc spreparować inny dokument, który wygeneruje tę samą wartość funkcji hashującej SHA-1 i zostanie przez odbiorcę uznany za autentyczny.

Niebezpieczne funkcje

Inna popularna funkcja hashująca – MD5 – stwarza jeszcze większe zagrożenie. Jest ona stosowana m.in. w protokole SSL oraz w wielu innych aplikacjach i tak samo jak SHA-1 może być podstawą budowania podpisów cyfrowych. Już w 1996 roku pojawiły się pierwsze obawy związane z bezpieczeństwem tego algorytmu, w 2004 roku natomiast dzięki rzeszy ochotników i przetwarzaniu rozproszonemu znaleziono realną kolizję (czyli dwie wiadomości o tej samej wartości funkcji skrótu). MD5 została zaprojektowana w 1991 roku przez Rona Rivesta jako recepta na szczególnie atakowany MD4. Ten sam kryptolog jest także autorem popularnego szyfru RC4, powszechnie wykorzystywanego np. przez pakiet Microsoft Office. Przy okazji warto wspomnieć, że implementacja ta została spektakularnie złamana przez Hongjun Wu w styczniu tego roku.

Najgroźniejszy atak na funkcję Rivesta miał miejsce w sierpniu zeszłego roku, a dokonał go... zespół chińskich naukowców z Shandong University (w składzie Xiaoyun Wang, Dengguo Feng, Xuejia Lai, Hongbo Yu). Pokazali oni, jak można w godzinę pracy komputera IBM p690 podrobić podpisy stworzone z użyciem MD5. Ataki na tę funkcję stały się zatem praktycznie wykonalne!

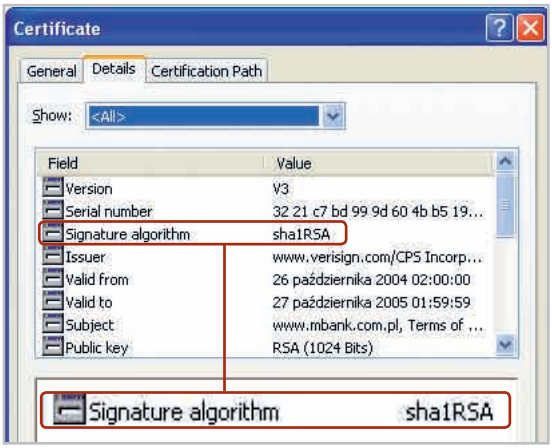
Spokojnie

Nie ma jednak, przynajmniej na razie, powodów do paniki. Dla najczęściej dziś stosowanej funkcji SHA-1, nawet z wykorzystaniem metody Chińczyków, przeprowadzenie ataku wymagałoby wykonania co najmniej 2^{69} operacji. A to jest wciąż bardzo dużo liczba! Dysponując tysiącem komputerów zdolnych obliczyć wartość funkcji SHA-1 miliard razy na sekundę, musielibyśmy czekać ok. 10 lat, aby uzyskać kolizję i podrobić podpis! Nie jest więc realne, by dzisiaj taką operację skutecznie przeprowadzić. Trzeba jednak pamiętać, że moc obliczeniowa stale rośnie, a badacze szyfrów nieustannie odnajdują nowe metody łamania algorytmów.

Sprawdź certyfikat

Użytkownicy komputerów mogą niewiele zrobić wobec słabości zastosowanych algorytmów. Funkcje hashujące są bowiem wbudowane wewnątrz aplikacji bądź protokołów i to ich producenci powinni dbać, by były bezpieczne. Prawdopodobnie w niedalekiej przyszłości zastąpią oni SHA-1 jej silniejszymi odmianami: SHA-256, SHA-384 lub SHA-512, które charakteryzują się większymi długościami cyfrowych odcisków palców (odpowiednio 32, 48 i 64 bajty).

Na pewno jednak warto zwrócić uwagę, jaki algorytm stosują używane przez nas aplikacje i strony WWW do obliczania funkcji skrótu – czy wciąż MD5 lub SHA-1, czy też już nowsze metody. Wydaje się także, że wykorzystywanie starych wersji algorytmów przy podpisywaniu mało istotnych informacji niesie za sobą małe ryzyko. Powtórzenie wyniku chińskich naukowców wymaga jednak sporej mocy obliczeniowej, a więc i nakładów finansowych na jej uzyskanie. Trudno się zatem spodziewać, że ktoś zainwestuje miliony, by ukraść tysiąc złotych z naszego konta bankowego.



Powszechnym zastosowaniem funkcji MD5 i SHA-1 jest podpisywanie certyfikatów cyfrowych zabezpieczających transmisję w Sieci (poprzez SSL). Mimo znalezienia w nich luk przynajmniej na razie możemy jednak spać spokojnie.

Za Wielkim Murem

Prawdopodobnie ostatnie odkrycia naukowców zachęcą rzesze ekspertów do opracowania nowych funkcji hashujących. Jak widzimy na przykładzie SHA-1, nawet bardzo powszechne i uważane za szeroko przeanalizowane algorytmy kryptograficzne mogą nas niemile zaskoczyć. Oznacza to, że w dziedzinie bezpieczeństwa stale coś się dzieje i nie można spocząć na laurach. Trzeba śledzić prace badawcze oraz analizować ich wyniki pod kątem realnych niebezpieczeństw, a wymyślona przez ze mnie funkcja VMPC jest tylko jednym z przykładów nowych sposobów zabezpieczania informacji, z jakimi nie raz przyjdzie się nam zetknąć. ■

Więcej informacji

Polski serwis kryptograficzny
http://www.kryptografia.com/
Międzynarodowe Stowarzyszenie Badań Kryptologicznych
http://www.iacr.org/
Funkcja VMPC
http://www.vmpcfunction.com/