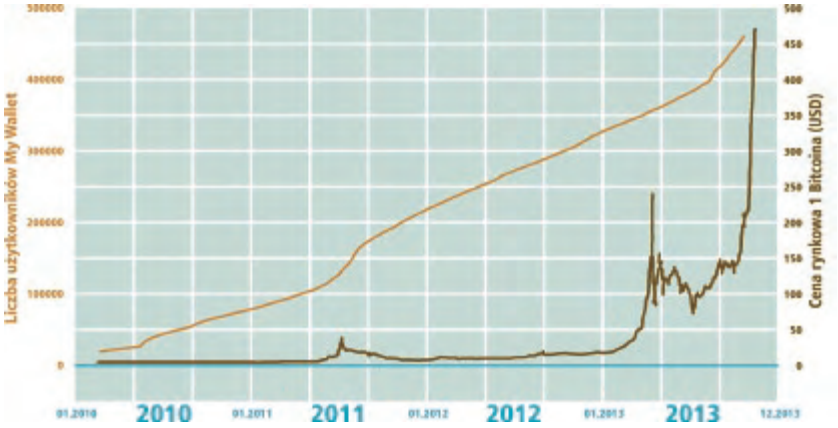
Nowe problemy kryptowaluty Bitcoin: błąd w Android i zablokowanie procesu „kopania” monet

dr inż. WOJCIECH NOWAKOWSKI, prof. nadzw.

Instytut Maszyn Matematycznych, Warszawa

Ponowny wzrost kursu kryptowaluty Bitcoin (*rys. 1*) spowodowały oczywiście poszukiwanie metod nielegalnego jej zdobycia, czyli po prostu kradzieży w sieci. Ostatnio stało się to możliwe, bowiem cybernetyczni złodzieje wykryli lukę w systemie operacyjnym Android. Twórca systemu, firma Google Inc. przyznała, że taka luka istnieje. Problem jest poważny, bo z jednej strony wpływa na zmniejszenie zaufania do cybernetycznego pieniądza Bitcoin, a z drugiej – co gorsze – generuje podejrzenia, że z wieloma innymi aplikacjami na Androida mogą pojawić się problemy.



Rys. 1. Kurs waluty Bitcoin od czasu jej powstania [1]
Fig. 1. Bitcoin exchange rate since the beginning of the currency [1]

Problem w systemie operacyjnym Android [4]

Podobnie jak większości systemów operacyjnych, w systemie Android niezbędne jest generowanie liczb losowych. Ten system wprowadzony przez firmę Google Inc. opiera się od 2008 roku na oprogramowaniu *Java Cryptography Architecture* (JCA), jeszcze w wersji API 1. Część JCA jest znana jako *SecureRandom*, która to nazwa sugeruje wyraźnie zakres jej zastosowania.

Wywołanie przez aplikację systemowej procedury *SecureRandom* jest równoważne z żądaniem, by system operacyjny wygenerował liczbę losową. Jak wiadomo, wykorzystywanie takiej liczby jest bezpieczne tylko wtedy, gdy proces jej generacji jest niedeterministyczny, przynajmniej w przybliżeniu. Jeżeli natomiast taką liczbę można byłoby przewidzieć, byłaby ona nieprzydatna. Procedura *SecureRandom* ma uruchomić w Androidzie procedurę *OpenSSL PRNG* (ang. P*seudoRandom Number Generator*) czyli chroniony plik systemowy *dev/urandom*.

Operacja ta jednak nie działa zwykle poprawnie. W większości wersji systemu Android plik *urandom* jest niedostępny, wskutek czego nie następuje poprawne generowania liczb losowych. Pseudolosowość liczb generowanych przy użyciu standardowej procedury SecureRandom jest niewystarczająca, wskutek czego liczby te stają się powtarzalne i przewidywalne.

Żeby odpowiedzieć w jaki sposób ta przewidywalność czy powtarzalność może prowadzić do kradzieży wirtualnej waluty wystarczy przypomnieć, że kody szyfrujące tym łatwiej jest złamać, im więcej jest przykładów kodowania. System Bitcoin jest oparty na kryptografii klucza publicznego i prywatnego [1, 2]. Wszystkie transakcje są publiczne i przechowywane w rozproszonej bazie danych. Klucze publiczne w transakcjach Bitcoin są łatwe do skanowania, co ma istotne znaczenie. Hakerzy poszukiwali więc powtórzeń w kluczach publicznych i wykorzystywali je do odgadnięcia kluczy prywatnych, które powinny być znane wyłącznie właścicielowi portfela Bitcoin. Potem dokonanie przelewu na własne konto było już proste.

Nie wiadomo, ile pieniędzy zostało skradzionych. Jakkolwiek ten błąd znany jest już od dość dawna, nie było dotąd doniesień o powtórzeniach w generacji liczb pseudolosowych w procedurze *SecureRandom*. Jest więc prawdopodobne, że niektóre z wcześniejszych niewyjaśnionych kradzieży pieniądza Bitcoin są wynikiem tego problemu.

Fot. http://ako-investovat.sk/clanok/489/bitcoin

Co z innymi aplikacjami Androida?

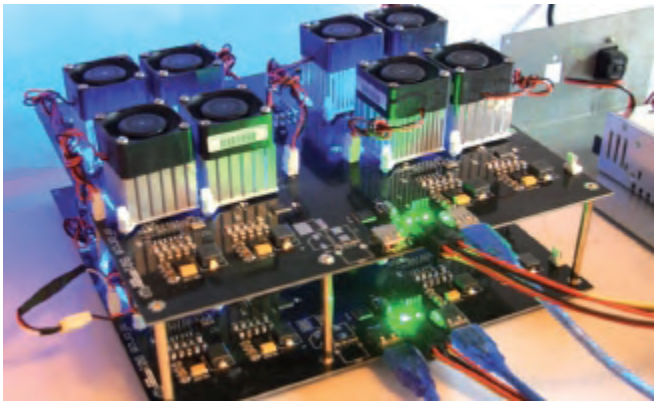
Aplikacja przelewów waluty Bitcoin została zaatakowana jako pierwsza przede wszystkim dlatego, że w wyniku takiego ataku można uzyskać natychmiastowy zysk. Wykorzystanie procedury *SecureRandom* jest jednak powszechne, co oznacza, że znacznie więcej aplikacji Androida może być niebezpiecznych, np. wskutek możliwości kopiowania danych osobowych. Problemy procedury *SecureRandom* mogą być również wykorzystywane do generowania identyfikatorów lub kluczy zabezpieczających komunikację danych. Raport firmy Symantec szacuje, jest ponad 360000 aplikacji w *Google Play*, które korzystają z *PRNG Android*. Wszystkie one, począwszy od aplikacji edukacyjnych do portali społecznościowych, mogą być zagrożone ponieważ, nie mogąc zainicjować procedury */dev/urandom* generują liczby niewystarczająco pseudolosowe.

Uważa się, że wersje 4.2 i 4.3 Androida nie są wrażliwe, ponieważ Google Inc. zmieniło ich sposób generacji liczb pseudolosowych. Jednak zmiana ta obejmuje tylko niewielką liczbę użytkowników Androida i chociaż poprawkę wykonano szybko, może ona nieprędko dotrzeć do większości użytkowników.

Problem z procedurą weryfikacji i emisji Bitcoin [3, 5]

W ostatnich miesiącach pojawiły się też doniesienia o znacznej wrażliwości procedury *kopania* monet na działania przestępcze, które utrudniają pierwotne pozyskiwanie pieniędzy waluty wszystkim uczciwym tzw. *górnikom*, a nawet przejęcie całej dostępnej emisji kryptowaluty.

Kopanie monet Bitcoin polega na pracy użytkowników systemu w specjalnie utrudnianej procedurze weryfikacji transakcji, wymagającej dużych mocy obliczeniowych, w wyspecjalizowanych stacjach roboczych skonfigurowanych z najbardziej wydajnych procesorów (CPU, graficznych CPU, FPGA itd). W tym celu każdy *górnik* zbiera wszystkie niepotwierdzone jeszcze transakcje w blok, a następnie próbuje obliczyć *hash* takiego bloku spełniający pewne z góry określone cechy. Wymaga to przewidywalnej liczby prób i błędów. Kiedy znajdzie rozwiązanie, ogłasza je reszcie sieci. Sieć sprawdza poprawność weryfikacji zastosowanych w transakcji podpisów cyfrowych oraz ilości monet, sprawdza także nowo rozwiązany blok i dodaje do łańcucha. Ostatecznie łańcuch bloków zawiera kryptograficzną historię zmian posiadania wszystkich monet, poczynając od adresu ich emitenta, aż po adres aktualnego posiadacza.



Rys. 2. 8-rdzeniowy procesor FPGA – Bitcoin Miner. 1,6 Ghash/s, 85 W (bitcointalk.org)
Fig. 2. 8 cores FPGA Bitcoin Miner, 1,6 Ghash/s, 85W total (bitcointalk.org)

Działanie przestępcze polega na zachowaniu rozwiązanego bloku i nieujawnianiu go, przez co nie zostanie on dołączony do łańcucha bloków [3]. Gdy rozwiązany blok zostałby upubliczniony i dołączony do końca łańcucha, każdy *górnik* mógłby to zauważyć i rozpocząć obliczanie następnego. Gdy jednak rozwiązany blok nie zostanie umieszczony na końcu łańcucha, lecz ukryty, inni *górnicy* nie są już w stanie odnaleźć zakończenia łańcucha, którego już nie ma.

Zagrożenia

Obecnie uważa się, że takie postępowanie jest niemożliwe, a procedura emisji systemu Bitcoin jest bezpieczna. Nie jest to prawda – możliwość zablokowania systemu istnieje, jeśli nie teraz, to w przyszłości. Stosowane obecnie łączenie mocy obliczeniowej przez wielu *górników* do pozyskiwania Bitcoinów zwiększa prawdopodobieństwo omawianego opanowania łańcucha bloków. Gdyby powstała przestępcza wspólnota, która dysponowałaby więcej niż połową całkowitej obliczeniowej mocy *górniczej*, groźba sparaliżowania oprogramowania Bitcoin stałaby się realna.

Fot. www.coindesk.com

Gavin Andresen, szef jednego z zespołów rozwijającego obecnie technologię Bitcoin powiedział, że niebezpieczeństwo skutecznego wpływu na procedurę emisji waluty Bitcoin nie jest aż tak poważne, jak sugeruje się w [3]. Musiałyby bowiem jednocześnie mieć miejsce trzy istotne zdarzenia. Po pierwsze, musiałoby się znaleźć przynajmniej jeden wyjątkowo nieuczciwy *górnik*, zdecydowany na ukrycie swojego rozwiązania bloku. Po drugie, fakt braku bloku na końcu łańcucha musiałby zostać niezauważony, a wydobycie kontynuowane. Po trzecie wreszcie, nieuczciwi *górnicy* musieliby następnie współdziałać bardzo długo.

Wydaje się, że choć teoretycznie system Bitcoin jest podatny na atak uniemożliwiający jego działanie, ale atak ten byłby bardzo kosztowny i pracochłonny, więc nieopłacalny.

Literatura

[1] Nowakowski W.: O kryptografii kwantowej. Elektronika, konstrukcje, technologie, zastosowania, nr 2/2010, str. 98–100.
[2] Nowakowski W.: Kryptograficzne aspekty technologii wirtualnej waluty BitCoin. Elektronika – konstrukcje, technologie, zastosowania, nr 5/2013, str. 58–62.
[3] Ittay Eyal, Emin Gun Sirer: Majority is not Enough: Bitcoin Mining is Vulnerable. Computer Science > Cryptography and Security. Nov 2013. http://arxiv.org/abs/1311.0243v1
[4] Whitwam R.: How Bitcoin thieves used an Android flaw to steal money, and how it affects everyone else. August 2013. http://www.extremetech.com/computing/164134-how-bitcoin-thieves-used-an-android-flaw-to-steal-money-and-how-it-affects-everyone-else
[5] Plafke J.: Bitcoin flaw allows miners to game the system, gain control of entire network. November 2013. http://www.extremetech.com/extreme/170473-bitcoin-flaw-allows-miners-to-game-the-system-gain-control-of-entire-network