ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO
NR 852 EKONOMICZNE PROBLEMY USŁUG NR 117 2015

MARCIN GOGOLEWSKI
Uniwersytet im. Adama Mickiewicza w Poznaniu

ROZPROSZONE ZNACZNIKI CZASU

Streszczenie

Potrzeba wiarygodnego ustalenia czasu niektórych zdarzeń nie jest nowa, jednak do niedawna była ograniczona do stosunkowo niewielu zastosowań. Wraz ze wzrostem ilości danych przechowywanych wyłącznie w postaci cyfrowej pojawiła się konieczność łatwego sprawdzania ich wiarygodności. W artykule wskazano na kierunki możliwego rozwoju i przeanalizowano bezpieczeństwo rozwiązań rozproszonych, oferujących większą skalowalność i mogących zapewnić wyższy poziom anonimowości.
Słowa kluczowe: rozproszone znakowanie czasem, znacznik czasu.

Wprowadzenie

W ostatnich latach widać tendencję do ulepszania i optymalizacji istniejących narzędzi z wykorzystaniem nowych, czasami znanych z zupełnie innych dziedzin, sposobów. Priorytetem wielu nowych projektów jest zapewnienie innowacyjności. Pośrednio jest to spowodowane wymaganiami finansowania, jednak bezpośrednim powodem takiego podejścia jest zapewne to, że większość rozwiązań została już znaleziona i często jedynym problemem jest efekt skali. To, co działało w przypadku niewielkich grup użytkowników, może mieć ograniczone zastosowanie w przypadku próby wykorzystania w skali całego kraju. Dobrym przykładem jest tu choćby problem wyborów elektronicznych (Gogolewski 2014, s. 311), który ostatnio w skali kraju okazał się przedsięwzięciem trudnym, nawet bez wprowadzania jakichkolwiek możliwości oferowanych przez formę elektroniczną i bez dodatkowych zabezpieczeń. Podobny problem może wystąpić w przypadku usług znakowania czasem. Nie jest to zauważalne obecnie, ponieważ samo *znakowanie czasem*

jest cały czas usługą mało popularną, działającą jedynie jako część większych systemów.

Systemy znakowania czasem, w odróżnieniu od systemów głosowania elektronicznego, mają stosunkowo proste wymagania. Podstawową ich własnością powinna być wiarygodność (rozumiana tu także jako bezpieczeństwo). Drugą cechą, uwzględnioną niejako przy okazji, choć często nie mniej ważną, jest problem zapewnienia anonimowości.

1. Opis problemu

Na początku krótko przypomnijmy, na czym polega usługa znakowania czasem i dlaczego powinna być niezbędnym składnikiem systemów obrotu dokumentami, zarówno tradycyjnymi, jak i elektronicznymi.

W tym miejscu należy wyraźnie oddzielić usługę polegającą na wiarygodnym ustaleniu aktualnego czasu *zegarowego* od usługi polegającej na poświadczeniu konkretnej sekwencji zdarzeń (czy podpis był złożony przed wygaśnięciem certyfikatu, czy czynność prawna została wykonana po wejściu w życie ustawy, czy pojazd wjechał na skrzyżowanie przed zmianą świateł, etc.). Oczywiście posługiwanie się datą i godziną jest dla człowieka znacznie bardziej wygodne niż sekwencją zdarzeń, dlatego też w większości tradycyjnych rozwiązań występuje jakieś odniesienie do czasu tzw. *zegarowego*[1]. Nastręcza to jednak sporych problemów w przypadku analizy po fakcie (czy zegary były dokładnie zsynchronizowane, na ile dokładnie, czy można to udowodnić). Sytuację dodatkowo komplikuje fakt, że samo określenie *czasu zegarowego* oparte jest zwykle na pewnych umownych założeniach (strefy czasowe, średnia długość doby, sygnał synchronizacji nie zawsze jest wiarygodny i w niektórych rozwiązaniach może zostać skutecznie zakłócony).

Jako przykład użyteczności usługi *znakowania czasem* posłuży nam przypadek osoby chcącej zapewnić sobie pierwszeństwo w zgłoszeniu wniosku o patent. Będzie to spore uproszczenie rzeczywistej sytuacji, oparte bardziej na historycznych metodach, jednak szczegółowy opis procedury nie jest związany z tematem naszych rozważań i nie wniósłby nic nowego do dalszych rozważań.

W przypadku tradycyjnym – „papierowym" – osoba chcąca uzyskać stosowny znacznik czasu sporządzała dokładny opis proponowanego przez siebie rozwiązania (aby wykazać w razie potrzeby, że w danym momencie posiadała kompletną z punktu widzenia postępowania patentowego wiedzę) na papierze, zamykała w kopercie, a kopertę dawała do podpisu, opieczętowania, itp. notariuszowi. Histo-

[1] *Czas zegarowy* jest często nazywany *czasem rzeczywistym*, jako bezpośrednie tłumaczenie ang. *Real Time Clock* (RTC) – zegar czasu rzeczywistego, jednak podobne określenie *real-time* ma zdecydowanie odmienne znaczenie, dlatego też pozostaniemy przy określeniu *czas zegarowy*.

rycznie toczyło się wiele postępowań sądowych o przyznanie patentu, z których niektóre były rozstrzygane po wielu latach[2]. Dodatkowo, aby poświadczyć aktualny czas, notariusz wpisywał pod kolejnym numerem opis sprawy do swojego rejestru. Księgi wpisów były przechowywane wyłącznie w kancelarii notarialnej, a klientom wydawane były jedynie „odpisy" (prawnie równoważne oryginałowi)[3].

Opisane powyżej datowanie jest bardzo trudne do podważenia od strony prawnej, jednak jak łatwo zauważyć, opiera się w dużej części na zaufaniu do osoby notariusza (a ciężko uwierzyć, że nie znajdzie się ani jeden nieuczciwy!). Podmiana wpisu jest niewątpliwie trudna i ryzykowna, ale nie niewykonalna.

2. Wersja elektroniczna

W przypadku tradycyjnego podejścia problemem jest zarówno skalowalność, jak i możliwość weryfikacji. Co by się stało, gdyby wszystkie dane, które mogą choć potencjalnie zostać wykorzystane jako materiał dowodowy, zaopatrywać w znacznik czasu (np. zapis zmian świateł na skrzyżowaniach, operacji finansowych, przesyłanych informacji – bez ujawniania treści, itp.)? Problemem okazuje się także „weryfikowalność" tradycyjnych znaczników. Zgodnie z prawem dokument wydany przez uprawnionego urzędnika/notariusza może mieć własność tzw. „daty pewnej"[4]. Nie od dziś jednak wiadomo, że nawet groźba utraty pozycji, czy wysokich kar, nie gwarantuje uczciwości.

Od dłuższego czasu istnieją wersje elektroniczne usług znakowania czasem, działające na podobnej zasadzie jak wersja tradycyjna (czasami z dodatkowym zabezpieczeniem polegającym na „łączeniu", opisanym w dalszej części), jednak w niektórych przypadkach rozwiązania te mogą okazać się niewystarczające zarówno ze względu na poziom bezpieczeństwa (np. w przypadku spraw, w których wartość skutecznego oszustwa jest właściwie nieograniczona), jak i ze względu na dostępność (ang. *availability*) usługi w przypadku upowszechnienia się danego rozwiązania (np. oparcia o nie wszystkich obecnych i nowych systemów finansowych, komunikacyjnych, etc.).

---

[2] Jak choćby w przypadku *N. Tesli*, którego odwołanie w sprawie patentu na wynalazek radia zostało rozpatrzone pozytywnie dopiero po wielu latach, po śmierci wynalazcy.

[3] DzU 2014 poz. 164 – Prawo o notariacie, tekst jednolity.

[4] Art. 81. Kodeksu Cywilnego.

3. Postać dokumentu

Aby nasze rozważania nadawały się do stworzenia działającego zastosowania, konieczne jest ustalenie, w jakiej postaci będą dokumenty, które chcemy opatrywać znacznikiem czasu.

W praktyce, podobnie jak w przypadku podpisu elektronicznego[5] czy np. certyfikatów protokołu SSL/TLS, wykorzystywany jest zwykle skrót dokumentu (kilkadziesiąt bajtów, niezależnie od długości oryginalnego dokumentu). Bezpieczeństwo takiego rozwiązania jest zwykle akceptowalne, w razie konieczności można stosować kilka skrótów różnego rodzaju jednocześnie. Dodatkowo zapewnia ono zarówno oszczędność miejsca (znacznik czasu nie musi zawierać kopii dokumentu, „notariusz" potwierdza tylko, że w danym momencie widział taki skrót), jak i w pewnym stopniu tajność znakowanego dokumentu, gdyż na podstawie znacznika praktycznie niemożliwe jest poznanie treści dokumentu, a przy drobnej modyfikacji – np. dodaniu na końcu kilkudziesięciu losowych znaków – nawet stwierdzenia, czy jest to konkretny, znany nam, dokument, co może być istotne w przypadku np. zgłoszeń patentowych. Nie bez znaczenia jest też fakt, że czas potrzebny do uzyskania znacznika jest wielokrotnie krótszy niż w przypadku rozwiązań tradycyjnych (wynalazca może tworzyć znacznik czasu po każdej modyfikacji dokumentu).

4. Problem z implementacją

Wąskim gardłem całego systemu jest sprzęt (i łącza komunikacyjne) organizacji świadczących takie usługi, a problem z zaufaniem wiąże się nie tyle ze sposobem tworzenia znaczników, ile z zależnością bezpieczeństwa od pojedynczych osób (może wystarczyć jeden nieuczciwy pracownik jednej z organizacji). Oba problemy mogą zostać rozwiązane poprzez implementację systemu rozproszonego, którego działanie będzie oparte na sprzęcie wielu osób i organizacji. W ten sposób działa między innymi BitCoin[6], w którym bezpieczeństwo opiera się na tzw. *proof of work*, w skrócie: ostatecznie rację ma zawsze (tzn. z bardzo wysokim prawdopodobieństwem) większość liczona jako suma poświęconej mocy obliczeniowej („notariuszem" danej rundy jest osoba, która znajdzie ciąg bajtów spełniający daną zależność, uwzględniającą wszystkie transakcje przeprowadzone w danej rundzie, na co statystycznie musi poświęcić określoną liczbę operacji procesora dobraną tak, by nowa wartość była znajdowana średnio raz na 10 minut przez któregoś spośród wszystkich aktywnych użytkowników systemu). W przypadku znakowania czasem

[5] Chodzi o ang. *digital signature*. Polskie tłumaczenie nie jest może zbyt dokładne, ale jest powszechnie używane m.in. w aktach prawnych i innych opracowaniach, dlatego też będzie stosowane w niniejszej pracy.

[6] https://bitcoin.org/bitcoin.pdf.

nie ma konieczności znajdowania za każdym razem „jedynego słusznego" ciągu zdarzeń, dlatego też system byłby wielokrotnie tańszy w implementacji[7].

Zmiana formy znaczników czasu na elektroniczną niewątpliwie pomaga, gdyż przy odpowiedniej konstrukcji audyt można przeprowadzić stosunkowo szybko bez długotrwałych obliczeń, jednak problemem pozostaje skalowalność.

W przypadku znakowania czasem niepotrzebne są kosztowne (pod względem czasu i poświęconej energii) obliczenia, gdyż praktycznie każdemu uczestnikowi zależałoby na poprawności działania systemu i każdy mógłby sprawdzić poprawność jego systemu, a w przypadku próby nadużyć nie korzystać z usług nieuczciwych uczestników (co jednocześnie wpłynęłoby na ich dochody). Ponieważ koszt liczenia funkcji hashującej jest pomijalny – na współczesnych procesorach kilkanaście milionów hashy w ciągu sekundy – jedynym istotnym kosztem jest wygenerowanie podpisu, ale podpis nie jest konieczny w przypadku rozwiązań rozproszonych! Sam łańcuch zależności jest wystarczająco wiarygodnym dowodem, gdyż jego „podrobienie" jest praktycznie tak samo trudne jak „podrobienie" podpisu elektronicznego (w którym podpisywany jest właśnie skrót). W dodatku, przy założeniu rozsądnych parametrów, bezpieczeństwo systemu opierałoby się na większości użytkowników. Praktycznie żadne współczesne systemy nie są odporne na to, że większość użytkowników będzie „nieuczciwa" i „w zmowie", więc takiej sytuacji nie zakładamy. Problem dotyczy oczywiście nie tylko systemów informatycznych, ale także całych systemów prawnych.

5. Szczegóły techniczne rozwiązania

W jaki sposób skonstruować cyfrową wersję znacznika czasu tak, by zapewnić *niezmienność*, a dokładniej tak, by każda próba zmiany była łatwa do wykrycia?

Najłatwiej będzie to opisać korzystając z zależności rekurencyjnej. Na początku funkcjonowania serwisu znakowania czasem wybieramy dowolną wartość h_0 i publikujemy ją, najlepiej podpisaną przez nas. Dla każdej kolejnej wiadomości M_i obliczamy

$$h_i = H(h_{i-1}, M_i),$$

gdzie H jest kryptograficzną funkcją skrótu (np. SHA-2), a następnie podpisujemy wartość h_i i udostępniamy autorowi wiadomości jako znacznik czasu. Oczywi-

[7] Mógłby oczywiście zostać dodatkowo łączony w każdej rundzie z istniejącą sekwencją BitCoin, co dodatkowo zwiększyłoby wiarygodność, praktycznie bez generowania dodatkowych kosztów.

ście zamiast podpisu można przechowywać znaczniki czasu w postaci drzewa binarnego tak, by do rekonstrukcji (i sprawdzenia poprawności) znacznika wystarczał jeden znacznik z każdego poziomu. Rozmiar powstałego *dowodu* rósłby co prawda wraz ze wzrostem liczby znaczników, ale np. dla 2^{64} = 18446744073709551616 znaczników i rozmiaru znacznika 64B nie przekraczałby 4KB = 4096B, a do sprawdzenia wystarczyłoby policzenie 64 wartości hashy.

Z własności funkcji skrótu wynika, że „praktycznie niemożliwe" jest znalezienie innej wiadomości generującej identyczny skrót, dlatego też po podpisaniu i udostępnieniu wartości h_i podmiana wcześniejszych elementów łańcucha nie jest możliwa (tzn. będzie łatwa do wykrycia). Podpis nie dodaje tu wiarygodności, ale może być użyty jako dowód winy podpisującego – w innym przypadku mógłby twierdzić, że co prawda *znacznik czasu* jest poprawny, ale nie on go wygenerował.

Wykorzystując tę samą metodę, możemy „zsynchronizować" dwa lub więcej łańcuchów (generując jeden wspólny węzeł, np. $h_x = H(h_i, h_j)$, gdzie każdy element był wartością łączącą innego łańcucha). W ten sposób można stwierdzić, że wszystkie znaczniki czasu sprzed połączenia powstały przed znacznikami po momencie połączenia. Otrzymujemy w ten sposób relację częściowego porządku.

Korzystając z opisanej metody, możemy otrzymać całą sieć zależności, w której albo można udowodnić, które zdarzenie było pierwsze, albo (w przypadku różnych łańcuchów i niewielkich różnic czasowych) dwa zdarzenia będą „nieporównywalne", co w praktyce może być bardziej uczciwe niż faworyzowanie wynalazcy mieszkającego bliżej notariusza, czy mającego o kilka promili szybsze łącze. Na rysunku 1 „momenty" 1 i 2 są *nieporównywalne*, podobnie 3 i 4 (nie istnieje skierowana ścieżka). Najważniejsze jest to, że nigdy nie ma potrzeby odwoływania się do *czasu zegarowego*, który, choć możliwy do określenia z dużo większą dokładnością, jednocześnie jest w wyższym stopniu podatny na manipulację.

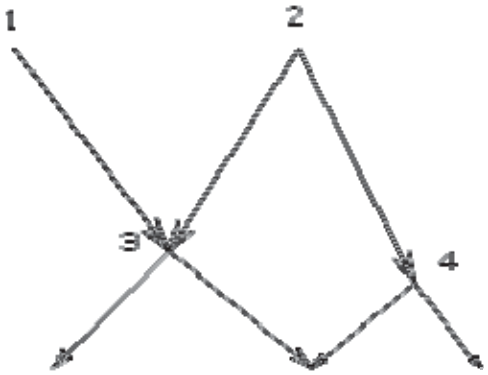
6. Problem anonimowości

Czasami wskazane jest zachowanie anonimowości w przypadku uzyskiwania znacznika czasu (np. żeby konkurencja nie wiedziała, czy wynalazcy udało się stworzyć coś nowego). W takim przypadku tajność dokumentu nie wystarczy, gdyż namierzony może zostać fakt samej komunikacji z notariuszem.

W najprostszym przypadku można by skorzystać z protokołu TOR[8]. Rozwiązanie to wymaga jednak działającej sieci rozległej, a jego dodatkowy nakład komunikacyjny jest niewspółmiernie wysoki. W praktyce, w przypadku urządzeń mobilnych lepsza mogłaby się okazać metoda przedstawiona w pozycji *Distributed Time-*

[8] The Onion Router – www.torproject.org.

Stamping with Boomerang Onion (Gogolewski 2004), oparta na dedykowanej wersji protokołu cebulkowego.



Rys. 1. Sieć zależności

Źródło: szkic autora.

We wspomnianej pracy opisane zostały niektóre szczegóły techniczne konieczne do implementacji. Praca zawiera wnikliwą analizę matematyczną problemu (od strony teoretycznej), choć skupia się na zagadnieniu anonimowości, pomijając praktyczny aspekt problemu. Opisując metodę w wielkim skrócie, użytkownik tworzy ścieżkę przez sieć stworzoną w sposób podobny jak w przypadku sieci TOR, gdzie samo przejście jest poświadczeniem, że dany pakiet pojawił się na routerze (konieczny jest klucz prywatny routera). Zapis takiego przejścia może służyć jako znacznik czasu.

Podsumowanie

Łatwo zauważyć, że sposobów optymalizacji istniejących usług jest wiele. Niektóre z nich zyskałyby w ten sposób nową jakość, oferując nowe możliwości, inne stałyby się po prostu łatwiej dostępne. Wprowadzenie nowych rozwiązań mogłoby wymagać zmian w istniejącym prawie, ale rewolucja nie jest potrzebna. W zupełności wystarczy podejście ewolucyjne, uwzględniające bieżące trendy i pojawiające się potrzeby.

Literatura

1. Dingledine R., Syverson N., Mathewson P. (2004), *Tor: The Second-Generation Onion Router*, Proc. 13th USENIX Security Symposium.
2. DzU 2014, poz. 164 – Prawo o notariacie, tekst jednolity.
3. Gogolewski M., Kutyłowski M., Łuczak T. (2004), *Distributed Time-Stamping with Boomerang Onions*, WartaCrypt 04, Tatra Mountains Mathematical Publications 33, s. 31–40.
4. Gogolewski M., Kutyłowski M., Łuczak T. (2004), *Mobile Mixing*, ICISC 04, Lecture Notes in Computer Science 3506.
5. Gogolewski M., Ren M. (2014), *Bezpieczeństwo wyborów elektronicznych*, Zeszyty Naukowe Uniwersytetu Szczecińskiego nr 808, Ekonomiczne Problemy Usług nr 112, s. 311–320.
6. Specyfikacja BitCoin – https://bitcoin.org/bitcoin.pdf.

DISTRIBUTED TIMESTAMPS

Summary

The need for a reliable determination of the time of certain events is not new, but until recently has been limited to relatively few applications. With increasing amount of data stored only in digital form, it become necessary to easily check their credibility. In this article we would like to point out the direction of possible developments and present a distributed security solutions, offering greater scalability and able to provide anonymity.

Keywords: time-stamping.

Translated by Marcin Gogolewski