Marcin Gogolewski, Michał Ren

Bezpieczeństwo wyborów elektronicznych

Ekonomiczne Problemy Usług nr 112, 311-319

2014

ZESZYTY NAUKOWE UNIWERSYTETU SZCZECIŃSKIEGO
NR 808 EKONOMICZNE PROBLEMY USŁUG NR 112 2014

MARCIN GOGOLEWSKI, MICHAŁ REN
Uniwersytet im. Adama Mickiewicza w Poznaniu[1]

BEZPIECZEŃSTWO WYBORÓW ELEKTRONICZNYCH

Streszczenie

Wybory w swojej tradycyjnej formie są zwykle związane ze sporymi wydatkami i nakładami organizacyjnymi. Implementacja nie wymagająca takich nakładów mogłaby być stosowana w sytuacjach, w których, choć większość zainteresowanych uważa, że istotne jest, by sam proces był uczciwy, anonimowy, weryfikowalny i odporny na naciski, to godzi się na pewne „uproszczenia" (np. oddawanie głosów przez telefon w przypadku wyboru przewodniczącego związków zawodowych czy partii politycznej) ze względu na brak uznanych rozwiązań (np. system posiadający uznany certyfikat bezpieczeństwa). Chcemy pokazać, że rozwiązania techniczne oferujące akceptowalny poziom bezpieczeństwa już istnieją, a głównym problemem jest bariera natury psychologicznej.
Słowa kluczowe: wybory elektroniczne.

Wprowadzenie

Wybory elektroniczne kojarzą się najczęściej z systemami podobnymi do ankiet internetowych lub z systemem, w którym zbieranie głosów polega na wypełnieniu formularza na ekranie certyfikowanej maszyny głosującej w lokalu wyborczym (tak jak np. w USA). W rzeczywistości nie chodzi jednak wyłącznie o usprawnienie procesu zbierania i zliczania głosów, oczekujemy znacznie więcej. Chcemy, by posiadały cechy niemożliwe bądź niezwykle trudne do osiągnięcia w przypadku wyborów tradycyjnych. Systemy wyborów elektronicznych mogą być

[1] Zakład Teorii Algorytmów i Bezpieczeństwa Danych, Wydział Matematyki i Informatyki.

w łatwy sposób dostosowywane do różnego rodzaju zastosowań nie związanych z wyborem przedstawicieli do władz państwowych. Uważamy, że mogą być skutecznie wykorzystane jako narzędzie do dowodliwie anonimowych ankiet na temat produktów czy do przeprowadzania sondaży w sposób niepodatny na manipulację (np. wynajmowanie firm do pisania pozytywnych opinii o produktach sklepu). W dalszej części przedstawimy krótko możliwe do uzyskania cechy, przykładowe systemy oraz zwrócimy uwagę na pewne zagrożenia, które, choć mniej poważne niż w przypadku wyborów tradycyjnych, nadal mogą stanowić problem, z którego istnienia należy zdawać sobie sprawę.

1. Cechy wyborów elektronicznych

Wymienione cechy to tylko przegląd możliwych wymagań. Konkretny system należy dostosować do przyzwyczajeń ludzi oraz prawa ustanowionego w danym kraju bądź organizacji.

Systemy można oceniać pod kątem różnych kryteriów takich, jak (Report 2001):

1. Autentykacja (czasem: legalność) – tylko uprawnieni głosujący powinni być w stanie zagłosować.
2. Unikalność – żaden głosujący nie powinien być w stanie głosować więcej niż raz (a dokładniej: nie więcej razy, niż zezwalają na to jego uprawnienia).
3. Precyzyjność – system głosowania powinien prawidłowo zliczać głosy.
4. Integralność – głosy nie mogą być modyfikowane, fałszowane ani usuwane bez wykrycia tego faktu (czasem mianem integralności określa się wszystkie powyższe własności).
5. Weryfikowalność – powinno być możliwe sprawdzenie, że wszystkie głosy zostały uwzględnione w ostatecznym rozrachunku.
6. Audytowalność – powinna być możliwość przedstawienia dowodów poprawności przebiegu głosowania.
7. Tajność – nikt (ani też żadna grupa osób w koalicji) nie powinien być w stanie ustalić, jak głosował którykolwiek z głosujących.
8. Uczciwość (ang. *fairness*) – żadna zaufana trzecia strona nie jest w stanie poznać wyników cząstkowych w trakcie głosowania.
9. Niemożność sprzedawania głosów i odporność na naciski – uniemożliwia głosującemu udowodnienie, na kogo głosował, a nawet umożliwia oszukanie osoby wywierającej nacisk co do osoby, na którą głosowano, nawet jeśli wywierający nacisk wykonywał za głosującego pewne (ale nie wszystkie) kroki protokołu.

10. Certyfikowalność – system głosowania powinien poddawać się certyfikacji, tak żeby każdy mógł przekonać się, że założone kryteria bezpieczeństwa są spełnione.
11. Niezawodność – system wyborów powinien działać bez utraty jakichkolwiek głosów, nawet w obliczu licznych awarii, w tym awarii maszyn do głosowania i całkowitej utraty łączności przez Internet.
12. Wszechstronność – system i sprzęt do głosowania powinny umożliwiać różne rodzaje głosowania, m.in. głosowania większościowe, głosowania przez uszeregowanie, dopisywanie dowolnych kandydatów, etc.
13. Dostępność – głosowanie powinno być możliwe do przeprowadzenia także przez osoby o różnym stopniu niepełnosprawności.
14. Wygoda – głosujący powinni być w stanie szybko i wygodnie oddawać głosy, bez posiadania specjalnych umiejętności czy wykonywania trudnych operacji.
15. Przejrzystość – system wyborów powinien być tak prosty, by każdy głosujący go rozumiał.
16. Efektywność – stosowanie systemu głosowania powinno być tanie w stosunku do możliwości, które system oferuje (w szczególności nie droższe niż porównywalne rozwiązania „tradycyjne").

2. Przykładowe systemy głosowania

Systemy głosowania różnią się pod względem modelu bezpieczeństwa. Wyróżnić można:

1. Systemy z głosowaniem w lokalach wyborczych – dobrze znany, powszechnie używany system, w którym wyborca musi stawić się osobiście w lokalu wyborczym, oddając głos przy użyciu maszyn do głosowania. Pewne kroki protokołu głosowania (np. potwierdzenie tożsamości i autoryzacja głosującego) mogą zostać wykonane przez obecnych na miejscu, upoważnionych urzędników. Zakłada się, że maszyny do głosowania i środowisko, w którym odbywa się głosowanie, są kontrolowane.
2. Systemy głosowania za pomocą terminali publicznych – wykorzystują publicznie dostępne maszyny, takie jak bankomaty albo inne dedykowane komputery. Środowisko głosowania nie jest więc kontrolowane, ani nie ma możliwości wykonywania kroków protokołu przez mężów zaufania. Zakłada się, że jedynie maszyny mogą być kontrolowane.
3. Głosowanie internetowe – każdy głosujący oddaje głos za pomocą komputera osobistego, z domowego zacisza. Ani komputer głosującego (tzn. ani sprzęt, ani oprogramowanie), ani środowisko, w którym się znajduje, nie mogą być kontrolowane. Istnieje jednak infrastruktura systemu głosowania złożona z serwerów i ich oprogramowania, która działa pod kontrolą zaufanej strony trzeciej

i może być kontrolowana. Ten rodzaj systemu głosowania jest najbardziej wymagający pod względem bezpieczeństwa. w praktyce stosuje się więc mechanizmy takie jak specjalne karty do głosowania, zawierające zakodowane informacje, tak żeby komputer głosującego nie był w stanie poznać informacji, na jakiego kandydata został oddany głos (Chaum 2001), albo karty chipowe, będące w istocie zaufanymi, choć bardzo ograniczonymi, urządzeniami; w niektórych rozwiązaniach mogą to być nawet karty chipowe z wyświetlaczem (Nitschke 2008).

Na przykład system ThreeBallot (Rivest 2006) jest próbą stworzenia systemu głosowania, który nie opiera się na zaawansowanej kryptografii, a mimo to ma więcej pożądanych własności niż wybory tradycyjne.

Wyborcy udają się do lokalu wyborczego, gdzie zostają autoryzowani w tradycyjny sposób. Każdy z nich otrzymuje następnie specjalną kartę do głosowania. Różni się ona tym od tradycyjnej karty do głosowania, że dzieli się na trzy kolumny, przy czym nazwiska kandydatów są powtórzone trzy razy i występują obok siebie jeden raz w każdej kolumnie. Każda kolumna może zostać oderwana (karta zawiera perforację) i każda zawiera unikalny identyfikator, jak numer na tradycyjnej karcie do głosowania.

Głosujący, aby zagłosować na jakiegoś kandydata, zaznacza jego nazwisko w dokładnie dwóch kolumnach. Jeśli nie chce głosować na danego kandydata – zaznacza jego nazwisko w dokładnie jednej kolumnie. Karty do głosowania, na których znajdą się nazwiska nie zaznaczone ani razu lub zaznaczone trzy razy, nie są ważne.

Po zaznaczeniu kandydatów głosujący sprawdza kartę do głosowania w specjalnej maszynie, która weryfikuje, że karta została wypełniona poprawnie (każde nazwisko zostało zaznaczone dokładnie raz lub dwa razy, jeśli możliwe jest głosowanie na ograniczoną liczbę kandydatów, to, że liczby tej nie przekroczono, etc.). Następnie karta zostaje rozerwana na trzy części, a głosujący ma możliwość wyboru jednej z nich i otrzymania jej kopii w celu weryfikacji. Trzy części karty są mieszane w urnie z głosami oddanymi przez innych wyborców. Każda część będzie od tej chwili traktowana jako oddzielny głos.

Po zakończeniu głosowania wszystkie karty do głosowania są skanowane, a następnie publikowane na tablicy ogłoszeń. Tablica ogłoszeń (ang. *bulletin board*) to mechanizm często wykorzystywany w systemach głosowania jako tzw. uwierzytelniony kanał publiczny. Umożliwia on publiczne rozprowadzanie wiadomości komitetowi wyborczemu w taki sposób, żeby wszyscy mieli pewność, że wiadomości w istocie pochodzą od komitetu i że nie zostały przez nikogo zmienione. Na tablicy ogłoszeń publikuje się również nazwiska głosujących.

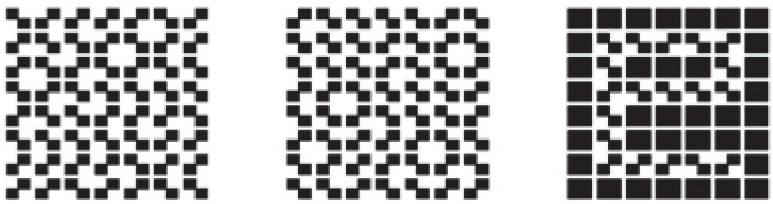
Dzięki publikacji wszystkich głosów wyborca może zweryfikować, że jego głos został policzony – kopia głosu, którą posiada, powinna się znajdować na tablicy ogłoszeń. Jeśli tak jest (nikt nie zgłosił protestów), można policzyć głosy. W konsekwencji przyjętych reguł głosowania, aby otrzymać prawdziwą liczbę gło-

sów na danego kandydata, należy policzyć, ile razy był zaznaczany na wszystkich kartach, i od tej liczby zaznaczeń odjąć liczbę wszystkich głosujących.

Warto zauważyć, że pomimo braku skomplikowanej kryptografii protokół ten pod wieloma względami ma przewagę nad standardowym głosowaniem. Głosujący może bowiem sprawdzić, czy jego głos został uwzględniony, ponieważ posiada kopię, której identyfikator może znaleźć na tablicy ogłoszeń i porównać zaznaczone nazwiska. Mimo to kopia głosu w istocie nie zdradza żadnej informacji o prawdziwych preferencjach głosującego (do tego trzeba by trzech kawałków karty do głosowania), nie może więc być użyta do udowodnienia, że głosowało się w konkretny sposób (czyli kupowania głosów).

Jednym z powszechnie wykorzystywanych mechanizmów systemów głosowania są tzw. sieci mieszające (ang. *mix networks*). Opiera się na nim m.in. system wyborczy opracowany przez Chauma (Chaum 2004, s. 38–47), który warto omówić ze względu na jego prostotę.

System ten wykorzystuje również wart uwagi mechanizm kryptografii wizualnej (ang. *visual cryptography*), także zaproponowany przez Chauma, który umożliwia tworzenie wzorców graficznych składających się z losowo rozrzuconych kropek (na tyle gęstych, że powierzchnia nimi pokryta wydaje się z pewnej odległości jednolicie szara), które dają wyraźnie widoczny rysunek bądź napis po nałożeniu na siebie i obejrzeniu pod światło. Ponieważ tworzenie wzorów kropek opiera się na zasadzie analogicznej do funkcji XOR, to żadna pojedyncza warstwa nie zawiera możliwej do odzyskania informacji o ukrytym rysunku, niezależnie od posiadanej mocy obliczeniowej (Shannon 1949, s. 656–715). Poniżej przykład dwóch takich warstw i ich złożenie.



Wyborca w tym systemie głosuje w lokalu wyborczym, przy użyciu maszyny do głosowania, podobnie jak jest to obecnie stosowane w większości głosowań w USA. Jednak maszyna, zamiast jedynie rejestrować głosy na kartce papieru, drukuje dla głosującego potwierdzenie składające się z czytelnego napisu zawierającego głos, numer seryjny głosu, oraz „cebulę" (ang. *onion*) – elektroniczny kod (Rackoff 1993), który będzie wykorzystany do zliczenia głosu. Potwierdzenie jest drukowane na dwóch warstwach, tak że jest widoczne po ich złożeniu; głosujący po wydrukowaniu wybiera, którą połówkę (warstwę) chce zatrzymać jako potwierdzenie, a maszyna dodrukowuje do obu warstw podpis elektroniczny oraz „cebulę" – informację pozwalającą później odtworzyć połówkę zabraną przez głosującego.

Przy wyjściu głosujący oddaje jedną warstwę karty do głosowania, zatrzymując wybraną przez siebie uprzednio. Dzięki podpisowi elektronicznemu głosujący może później sprawdzić, że maszyna nie oszukiwała przy generowaniu głosu, a dzięki użyciu tablicy ogłoszeń – że system odpowiednio policzył głos.

Zastosowanie bardziej skomplikowanych mechanizmów kryptograficznych, w szczególności szyfrowania homomorficznego, pozwala ograniczyć zapotrzebowanie na mężów zaufania i specjalne karty do głosowania. Przykładem systemu wykorzystującego tę technikę jest Scratch & Vote (Adida 2006).

W tym systemie głosowania wykorzystuje się technologię „zdrapek". Każda karta do głosowania jest podzielona na prawą i lewą połówkę – na prawej znajdują się pola do zaznaczenia wyboru, a po lewej – nazwiska kandydatów, koniecznie w losowym porządku. Prawa połówka zawiera też zdrapkę, pod którą jest umieszczony specjalny kod oraz dwuwymiarowy kod kreskowy. Karty są złożone tak, żeby urzędnik je wydający nie widział tego porządku. Każdy wyborca otrzymuje dwie karty, z czego jedną, losowo wybraną, wykorzystuje do sprawdzenia przez zdrapanie zdrapki i kontrolę kodu paskowego znajdującego się pod nią.

Głosujący dokonuje wyboru, zakreślając odpowiednie pole, a następnie odrywa połówkę karty z nazwiskami i może ją wyrzucić. Drugą połówkę karty oddaje urzędnikowi, który sprawdza, czy zdrapka nie została naruszona, a następnie odrywa ją i niszczy, a kartę z wyborem skanuje. Skan pojawia się na tablicy ogłoszeń, co wyborca może zweryfikować.

3. Kwestie bezpieczeństwa

W przypadku wyborów elektronicznych stosowane są takie same narzędzia kryptograficzne jak w przypadku usług finansowych, czy potwierdzania dokumentów mających moc prawną, a niektóre elementy są wręcz bezwarunkowo bezpieczne (Shannon 1949, s. 656–715) przy rozsądnych i weryfikowalnych założeniach. Systemy są cały czas badane pod kątem nowych zagrożeń (np. zagrożeń kleptograficznych, czyli polegających na niewykrywalnym kopiowaniu danych, takich jak np. klucze prywatne, na zewnątrz systemu (Gogolewski 2006).

Przyjrzyjmy się bardziej szczegółowo niektórym ze stosowanych metod. W systemie zaproponowanym przez Chauma poza kryptografią wizualną, służącą do ochrony tajności głosowania i odebrania możliwości sprzedaży głosów (potwierdzenie oddania głosu nie niesie informacji o dokonanym wyborze), został zastosowany tzw. protokół cebulkowy oraz RPC (ang. *Randomized Partial Checking*). Bez zagłębiania się w szczegóły matematyczne, tworzenie każdej z „cebulek" polega po prostu na wielokrotnym szyfrowaniu danych za pomocą kolejnych kluczy publicznych należących do różnych osób (organizacji). Dzięki temu każda taka zaufana osoba (i nikt inny) może „zedrzeć swoją warstwę" z każdej cebulki za po-

mocą swojego klucza prywatnego, a następnie (np. po losowej zamianie kolejności, by nie zdradzać, które wnętrze odpowiadało której cebulce przed operacją „zdzierania", przesłać wszystkie cebulki dalej. Czy istnieje jednak metoda sprawdzenia, że osoba ta nie dokonuje przy tym niedozwolonych manipulacji (np. podmienia część cebul lub wysyła je w ustalonej kolejności)?

Standardowym sposobem kontroli jest RPC (Jakobsson 2002) – od każdego męża zaufania wymaga się zdradzenia rozszyfrowanej postaci losowo wybranej połowy deszyfrowanych przez niego cebul[2]. Następnie od kolejnego męża zaufania, który otrzymał te zdeszyfrowane cebule, wymaga się zdradzenia rozszyfrowanej postaci cebul, których zaszyfrowana postać nie została zdradzona poprzednio. W ten sposób połowa operacji dokonywana przez każdego z nich zostaje sprawdzona, ale nikt nie jest w stanie prześledzić drogi żadnej z cebul przez sprawdzaną parę osób, ponieważ jeśli wiemy, co z daną cebulą robiła pierwsza osoba z pary, to nie wiemy, co robiła z nią druga i *vice versa*. Dzięki takiemu mechanizmowi całkowicie zostaje zatarty związek między głosem oddanym przez głosującego (który można do niego przypisać) a ostateczną, rozszyfrowaną postacią głosu, który zlicza się na końcu głosowania.

W systemie Scratch & Vote przygotowanie i sprawdzanie cyfrowych kodów wykorzystuje homomorficzne szyfrowanie asymetryczne systemem Pailliera (Paillier 1999). Kryptosystem ten ma bardzo ciekawą własność homomorfizmu – mnożąc dwa szyfrogramy, otrzymujemy wartość, która po zdeszyfrowaniu daje sumę zdeszyfrowanych wartości początkowych. Możemy więc skutecznie dodawać do siebie wiadomości, nie mając możliwości ich rozszyfrowania (mnożąc ich zaszyfrowane postaci). Bez wchodzenia w szczegóły teorii liczb wystarczy zauważyć, że umożliwia to implementację liczników homomorficznych, czyli użycia zaszyfrowanych wiadomości do inkrementacji któregoś z liczników bez wiedzy o tym, który licznik powiększyliśmy. Co więcej, poprawność przeprowadzenia tej operacji można prosto, publicznie (ponieważ prywatny klucz jest potrzebny jedynie na końcu, do odkrycia wartości licznika) zweryfikować.

System głosowania Scratch & Vote korzysta właśnie z tego mechanizmu w celu zapewnienia tajności i weryfikowalności.

Podsumowanie

Uważamy, że systemy projektowane do stosowania w przypadku wyborów elektronicznych w skali całego kraju są z jednej strony wystarczająco bezpieczne do stosowania w znacznie mniej wymagających i łatwiejszych do kontroli środowi-

[2] Każde oszustwo zostanie wykryte wtedy niezależnie, z prawdopodobieństwem ½, czyli prawdopodobieństwo niewykrycia zamiany k cebul wynosi $(½)^k$, dla porównania szansa trafienia „szóstki" w lotto przy jednym losowaniu jest większa niż prawdopodobieństwo niewykrycia manipulacji 24 cebul.

skach (głosowania w radach nadzorczych, zbieranie opinii etc.), z drugiej zaś – przynajmniej niektóre z proponowanych nie wymagają wysokich nakładów ani w trakcie wdrożenia, ani w czasie eksploatacji (w porównaniu z oferowanymi możliwościami). Niektóre z nich mogą wręcz korzystać z istniejących zasobów (komputery, drukarki) i wymagają tylko niewielkich nakładów na przeszkolenie pracowników obsługujących samo głosowanie. Nawet jeżeli wymagana jest wcześniej instalacja stosownego oprogramowania czy sprzętu, to czas ten zwróci się zwykle w fazie zliczania głosów i publikacji wyników[3]. Dla głosujących poziom trudności związany z głosowaniem jest porównywalny do wyborów przeprowadzanych w formie tradycyjnej, a przy odpowiedniej konstrukcji systemu pewne pomyłki głosujący może „wycofać", dopóki nie zatwierdzi głosu, co niemożliwe jest w przypadku błędnego zaznaczenia swojego wyboru na karcie papierowej (bez naruszania bezpieczeństwa wyborów). Dodatkowo nie bez znaczenia jest większa dostępność głosowania (możliwe jest głosowanie zdalne i przez osoby o ograniczonej możliwości ruchu) bez utraty anonimowości czy uczciwości całego procesu.

Literatura

Adida B., Rivest R. (2006), *Scratch and vote: Self-contained paper-based cryptographic voting*, in: *ACM Workshop on Privacy in the Electronic Society*, edited by R. Dingledine, T. Yu, ACM.

Chaum D. (2001), *SureVote: Technical Overview*, Proceedings of the Workshop on Trustworthy Elections (WOTE '01).

Chaum D. (2004), *Secret-ballot: True voter verifiable elections*, „IEEE Security and Privacy", Vol. 2(1).

Gogolewski M., Klonowski M., Kubiak P., Kutyłowski M., Lauks A., Zagórski F. (2006), *Kleptographic attacks on e-voting schemes*, Proceedings ETRICS '06, Springer-Verlag Berlin.

Jakobsson M., Ari Juels A., Rivest R.L. (2002), *Making mix nets robust for electronic voting by randomized partial checking*, Proceedings of the 11th USENIX Security Symposium, August 2002.

Nitschke Ł. (2008), *Remote voting using smart cards with display*, Tatra Mt. Math. Publ., Vol. 41.

Paillier P. (1999), *Public-key cryptosystems based on composite degree residuosity classes*, in: EUROCRYPT, volume 1592 of LNCS, edited by Jacques Stern, Springer.

[3] Zakładamy, że wybrany system nie wymaga ręcznej analizy i zliczania kart, a drukowane potwierdzenia stanowią jedynie dodatkowe zabezpieczenie (głosujący może np. sprawdzić, czy jego głos został uwzględniony).

Rackoff C., Simon D.R. (1993), *Cryptographic defense against traffic analysis*, in the Proceedings of ACM Symposium on Theory of Computing.
Report of the National Workshop on Internet Voting: Issues and Research Agenda (2001), Internet Policy Institute.
Rivest R. (2006), *The ThreeBallot voting system*.
Shannon C. (1949), *Communication Theory of Secrecy Systems*, „Bell System Technical Journal", Vol. 28(4).
www.uke.gov.pl (2013).

ELECTRONIC VOTING SECURITY

Summary

Traditional elections are usually associated with considerable expenditures and organizational overhead. Implementations not requiring such expenditures could be used in situations where the majority of stakeholders, while believing that it is important for the process to be fair, anonymous, verifiable and coercion-resistant, also agree for certain "simplifications" (e.g. casting of votes by phone in political party or trade union chairman elections) due to lack of recognized solutions (e.g. systems with a recognized security certification). We show that the technical solutions already exist, and the only problem is the psychological barrier.
Keywords: electronic voting.

Translated by Michał Ren