OPINIA ZEWNĘTRZNA

Autorzy wskazani przez Stanisława Tyszkę, Wicemarszałka Sejmu RP

Prof. dr hab. Mirosław Kutyłowski

Dr Filip Zagórski

Politechnika Wrocławska

BAS-2158/17A **Warszawa, 22 grudnia 2017 r.**

Głosowanie przez Internet w referendum ogólnokrajowym

Analiza zmian technicznych niezbędnych dla wprowadzenia takiej możliwości w Polsce

Streszczenie: W niniejszym dokumencie omawiamy zagadnienia związane z głosowaniem zdalnym. Przedstawiamy wymagania techniczne, które mają decydujący wpływ na ocenę jakości schematów wyborczych. Prezentujemy najważniejsze własności protokołów głosowania wykorzystywanych w innych krajach. W ostatniej części prezentujemy rekomendacje dotyczące dalszych kroków procesowych jak i rozwiązań technicznych.

Spis treści

Zakres wspomagania procesów wyborczych przez systemy teleinformatyczne 2

Wymagania wpływające na stronę techniczną 3

Wymagania dotyczące poprawności zliczania głosów 3

Pozostałe wymagania techniczne 5

Założenia techniczne 6

Przykładowe rozwiązania techniczne 7

Estonia 8

Norwegia 8

Remotegrity 8

Rekomendacje 9

Rekomendacje procesowe 9

Rekomendacje techniczne 11

Krytyczne uwarunkowania techniczne 12

Bibliografia 15

Zakres wspomagania procesów wyborczych przez systemy teleinformatyczne

Głosowanie drogą elektroniczną, a w szczególności w zakresie przeprowadzenia referendum ogólnokrajowego, może obejmować różne komponenty procesu wyborczego. Podstawowymi podprocesami, jakie należy wyróżnić, są:

1. proces rejestracji (czynności techniczne i organizacyjne związane z inicjalizacją prawa wyborcy do korzystania z prawa do głosowania drogą korespondencyjną bądź elektroniczną),
2. proces informacyjny (czynności związane z przedstawieniem głosującemu informacji co do treści podejmowanej decyzji wyborczej),
3. proces dostarczenia głosującemu środków umożliwiających złożenie głosu,
4. proces złożenia głosu,
5. proces zarządzania urną elektroniczną przechowującą głosy,
6. proces obliczania wyników głosowania,
7. proces umożliwiający weryfikację prawidłowości wyników.

W zależności od przyjętej strategii droga elektroniczna dokonywania czynności może obejmować wybrane procesy. Dla przykładu proces rejestracji (związany np. z głosowaniem poza macierzystym obwodem) może być realizowany w standardowy sposób przewidziany dla kontaktów z administracją publiczną. Wyzwaniem pod względem technicznym byłoby zrealizowanie wszystkich wymienionych podprocesów na drodze elektronicznej - zwłaszcza podprocesu nr 3 i 4.

Uwagi szczegółowe:
Ad 1)
Wadliwość procesu rejestracji mogłaby umożliwić powstanie sytuacji, w której ten sam wyborca dopuszczony byłby do głosowania zarówno w trybie tradycyjnym jak i zdalnym. Z drugiej strony dokonywanie rejestracji każdorazowo w przypadku kolejnych wyborów w trybie nieelektronicznym stawia pod znakiem zapytania sensowność procesu elektronizacji - z punktu widzenia wyborcy proces staje się bardziej uciążliwy i może być tylko uzasadniony niemożnością głosowania w zwykłym trybie.
Natomiast sytuacja, w której wyborca byłby zobowiązany do jednorazowej osobistej rejestracji, która umożliwiałaby mu zdalne uczestniczenie we wszystkich kolejnych cyklach wyborczych, ma następujące zalety:

- poziom uwierzytelnienia głosującego jest na takim samym poziomie jak w głosowaniu tradycyjnym.
- zachowane są zalety głosowania zdalnego - choć rejestracja wymaga jednorazowego osobistego stawiennictwa, to nastąpić może to w dogodnym dla wyborcy momencie, w długim okresie poprzedzającym wybory.

Ad 2)
Komponent ten jest stosunkowo łatwy do zaimplementowania, lecz może stanowić bardzo istotną wartość dodaną. W obecnie ukształtowanym systemie wyborów kluczowe informacje niezbędne przy podejmowaniu decyzji wyborczych są niedostępne lub trudno dostępne dla wyborcy. Pod względem technicznym

funkcjonowanie takiego serwisu informacyjnego wymaga jedynie zapewnienia odpowiedniej przepustowości łączy i uwierzytelnienia informacji np. za pomocą podpisu elektronicznego.

Ad 3)
Proces ten jest kluczowy ze względu na trudne do jednoczesnej realizacji zasady głosowania: tajność głosu, jednokrotne składanie głosu, ograniczenie możliwości składania głosu do osób uprawnionych, prawidłowość wyników. Wynika stąd konieczność przekazania wyborcy środków (np. kodów, kluczy kryptograficznych, kart mikroprocesorowych, …) umożliwiających realizację konkretnego protokołu.

Ad 4)
Proces ten zazwyczaj jest w centrum uwagi, gdy mowa jest o głosowaniu zdalnym. Stopień elektronizacji może być różny w zależności od tego, czy obejmuje wyłącznie przesłanie (zakodowanego) głosu drogą elektroniczną, czy również całość procesu kodowania głosu na urządzeniu elektronicznym głosującego.

Ad 5)
Głos przekazywany drogą elektroniczną musi być przechowywany w systemie teleinformatycznym. W zależności od zastosowanego rozwiązania taka elektroniczna urna musi posiadać dodatkowe funkcjonalności, związane np. z możliwością sprawdzenia przez wyborcę, że jego głos faktycznie znajduje się w urnie.

Ad 6)
Proces obliczania głosów oddanych w trybie elektronicznym musi obejmować pewien zakres odkodowania głosów - w przeciwnym razie głos oddawany w jawnej postaci wraz z numerem IP nadawcy umożliwiałby ujawnienie decyzji wyborcy.

Ad 7)
Weryfikacja prawidłowości wyników pełni kluczową rolę wobec braku gwarancji o charakterze fizycznym (zapieczętowana urna i papierowe karty wyborcze). Proces ten jest kluczowy dla akceptacji głosowania elektronicznego i jego wyników przez wyborców.

Stopień trudności realizacji procesu wyborczego drogą elektroniczną zależy w znacznym stopniu od rodzaju wyborów. Referendum należy do najprostszych przypadków, ze względu na liczbę możliwych opcji do głosowania. To z kolei zwiększa liczbę relatywnie prostych technicznych rozwiązań, które mogą być zastosowane na tym etapie. Z tego względu rozpoczęcie procesu elektronizacji procesu wyborczego od referendów jest najbardziej racjonalnym kierunkiem działania.

Wymagania wpływające na stronę techniczną

Wymagania dotyczące poprawności zliczania głosów

Poprawność zliczania głosów w tradycyjnym głosowaniu osiąga się poprzez procesy kontrolne: umożliwienie obserwowania procesu liczenia bądź też aktywnego uczestniczenia w tym procesie poprzez zgłaszanie członków komisji przez

ugrupowania startujące w wyborach. W przypadku głosowania elektronicznego taka obserwacja jest niemożliwa - wszak intencja wyborcy zamieniana jest na ciąg bitów kodujący głos, który następnie jest przesyłany do komisji wyborczej przez sieć teleinformatyczną. Obserwacja zliczania głosów musiałaby objąć analizę wszystkiego, począwszy od tego, co działo się na komputerze/telefonie wyborcy, przez wszystkie routery przez które był przekazywany głos po serwery zbierające i zliczające głosy. Taka obserwacja jest niemożliwa, choćby z uwagi na fakt, że nie istnieją mechanizmy, które pozwoliłyby zapewnić, że zebrane z tych wszystkich urządzeń dane są wiarygodne. Co więcej, ingerencja w urządzenie wyborcy mogłaby doprowadzić do fikcji tajność głosowania.

Możliwym do zrealizowania i wiarygodnym sposobem rozwiązania tego problemu jest wymuszenie na systemie głosowania, aby był weryfikowalny (*end-to-end verifiable E2E-V*). Weryfikowalność osiąga się poprzez wprowadzenie mechanizmów, które pozwalają na sprawdzenie poprawności przebiegu głosowania od momentu, w którym głos jest tworzony przez wyborcę, aż do jego zliczenia.
System głosowania określamy jako weryfikowalny [PKRV10], jeżeli umożliwia sprawdzenie, że każdy z następujących etapów głosowania przebiegł poprawnie:

E1. zakodowany głos odpowiada intencji głosującego (*cast as intended*),
E2. zakodowany głos został zapisany w elektronicznej urnie wyborczej w formie odpowiadającej kodowi, który został wysłany przez głosującego (*recorded as cast*),
E3. liczenie głosów daje wynik odpowiadający zakodowanym głosom zapisanym w elektronicznej urnie wyborczej (*tallied as recorded*).

A ponadto oferuje mechanizmy umożliwiające sprawdzenie:

E4. czy zaprezentowana (wyborcy) postać głosu jest poprawna *(presented ballots are well formed)*
E5. czy głosy zapisane w urnie mają poprawną formę *(cast ballots are well-formed*).
E6. czy zbiór głosów poddanych sprawdzeniom jest spójny (*consistency check*) - w szczególności, czy zbiór podlegający sprawdzeniu E2 jest tym samym zbiorem co zbiór głosów poddanych sprawdzeniu E3.
E7. czy dla każdego zapisanego w systemie głosu istnieje wyborca, który może sprawdzić poprawność jego zapisania (*each recorded ballot is subject to the "recorded as cast" check*).
E8. czy każda procedura wpływająca na integralność może być poddana sprawdzeniu umożliwiającego wykrycie czy system zadziałał zgodnie z protokołem. Co więcej to sprawdzenie musi dostarczyć publicznie weryfikowalny dowód.

Weryfikowalne systemy głosowania spełniają własność "niezależności od implementacji" (*software independence*) [RV17]:
"System głosowania jest niezależny od implementacji, jeżeli niewykryta zmiana bądź błąd w oprogramowaniu nie może spowodować niewykrywalnej zmiany bądź błędu w wynikach wyborów."

W szczególności weryfikowalne schematy głosowania zapewniają.

W1. Niemożność zmiany głosu
Zastosowany system powinien uniemożliwiać niewykrywalną zmianę głosu (choćby w sposób losowy). Dotyczy to nie tylko komisji wyborczych, ale również sprzętu komputerowego używanego przez wyborcę oraz składników sieci teleinformatycznej pośredniczących w przekazaniu i przechowaniu złożonych głosów.

W2. Niemożność usunięcia głosu
System powinien zabezpieczać przed usunięciem głosu poprzez zagwarantowanie wykrywalności i możliwości udowodnienia, że pewne głosy zostały usunięte.

Nie można zakładać, że głosu nie można fizycznie usunąć. Dotyczy to zresztą zarówno systemów cyfrowych, jak i głosowania korespondencyjnego (np. poprzez niszczenie przesyłek podczas drogi pocztowej) czy tradycyjnego (usunięcie części głosów wyjętych z urny).

W3. Niemożność dodania głosów
System powinien zabezpieczać przed dołączeniem głosów poprzez zagwarantowanie wykrywalności i możliwości udowodnienia takiej sytuacji. Dotyczy to w szczególności sytuacji, w której wyborca zainicjował procedurę elektronicznej rejestracji lub składania głosu, lecz jej nie sfinalizował.

Pozostałe wymagania techniczne

W4. Tajność głosu
Żaden z uczestników procesu nie powinien mieć możliwości powiązania oddanego głosu z wyborcą. W idealnej sytuacji atakujący nie może wyprowadzić więcej informacji niż to wynika z informacji publikowanych w tradycyjnym trybie głosowania.
Tajność głosu powinna być zachowana zwłaszcza wobec operatora systemu, producenta urządzeń (w tym producenta sprzętu używanego przez wyborcę), wobec komisji wyborczych, czy innych wyborców.

W5. Anonimowość głosu
Zastosowany system powinien minimalizować możliwości zdobycia informacji o zachowaniu wyborcy, nie tylko w kontekście jaki głos oddał, lecz również, czy oddał głos.

W6. Wymuszenie głosowania w określony sposób
System powinien zabezpieczać przed presją wywieraną na wyborcy w celu zmuszenia go do głosowania w określony sposób. Zabezpieczenie powinno działać bez względu na brak chronionego środowiska.
W szczególności wynika stąd, że wyborca po złożeniu głosu nie powinien być w stanie wykazać osobie trzeciej, jak głosował.

W7. Efektywne rozstrzyganie sporów (*dispute-freeness*)
System musi zapewnić efektywne rozstrzyganie sporów wyborczych - w sytuacji, gdy którykolwiek z mechanizmów detekcji wykryje niezgodność z protokołem, powinna

istnieć możliwość stwierdzenia, który składnik czy też aktor systemu ponosi za to odpowiedzialność (accountability) [KTV10].

W systemach E2E-V istotnym aspektem jest to, jak zaprojektowane są mechanizmy rozstrzygania sporów. Czy w sytuacji spornej pozwalają one na stwierdzenie, kto ma rację. Jeżeli system to umożliwia, to mówimy, że ma efektywne rozstrzyganie sporów (jest *dispute-free*). Istotę problemu przedstawimy na przykładzie: wyborca chce oddać głos na kandydata A, a jego komputer zapisuje głos na kandydata B. W tej sytuacji możliwe są dwie opcje:
(a) Wyborca rzeczywiście wybrał kandydata A, a komputer (system) zmienił głos na kandydata B.
(b) Wyborca wybrał kandydata B, ale twierdzi, że to komputer (system) zmienił głos.
Jeżeli system nie jest dispute-free, to nie można rozstrzygnąć, która sytuacja miała miejsce, a więc można podważyć zaufanie do wyników wyborów nawet w sytuacji, w której przebiegły one poprawnie.

W8. Efektywne przywrócenie stanu (*recovery*)
Dobry projekt i jego implementacja oraz odpowiednie wdrożenie mogą spełniać rolę mechanizmów zapobiegających atakom (*prevention*). Weryfikowalne systemy głosowania oferują mechanizmy należące do grupy mechanizmów wykrywania (*detection*) ataków. Wdrażany na dużą skalę system powinien charakteryzować się też mechanizmami, które są w stanie w efektywny sposób zapewnić odzyskiwanie (*recovery*) stanu do tego sprzed ataku. Popularnym rozwiązaniem jest umożliwienie wyborcy oddanie ponownego głosu (nadpisującego poprzedni) w przypadku, gdy stwierdzi, że wcześniej oddany głos uległ manipulacji. Taki mechanizm był m. in. wdrożony w systemie norweskim [Gjo10], estońskim [HLW11], i w systemie Remotegrity [ZCC+13].

Założenia techniczne

Kluczowym dla bezpieczeństwa rozwiązania jest przyjęcie właściwych założeń co do środowiska, w którym będą przeprowadzane wybory. W naszej opinii absolutnym minimum jest przyjęcie następujących założeń.

Z1. Sprzęt używany przez wyborcę może być pod kontrolą wrogiego oprogramowania.
Z2. Urządzenia kryptograficzne, generatory liczb losowych mogą zawierać furtki zainstalowane przez adwersarza.
Z3. Kontrolę nad serwerami komisji wyborczej, w szczególności urną wyborczą, mogą przejąć osoby nieuprawnione, w tym osoby bezpośrednio zainteresowane wynikiem wyborów.

Ad. Z1)
Najskuteczniejszym sposobem radzenia sobie z tym założeniem jest wykorzystanie takiego schematu głosowania, który powoduje, że komputer wyborcy nie poznaje głosu oraz ma małe szanse na jego modyfikację. Stan taki można osiągnąć

wykorzystując karty do głosowania, na których każdemu kandydatowi przypisano unikalny, losowy kod. Wyborca oddając głos na wybranego kandydata wprowadza wydrukowany przy nim kod.
Jeżeli kody są wydrukowane w ten sposób, że są dodatkowo chronione tzw. zdrapką, to znacząco umożliwia to na osiągnięcie własności W7 (dispute-freeness) opisywanej w poprzednim rozdziale.

Ad. Z2)
Główne zagrożenie płynące z niewłaściwie działających generatorów liczb losowych jest w obszarze tajności głosowania. “Niewłaściwość” działania może mieć różny charakter, w tym może być celowa i trudna do wykrycia jak ataki kleptograficzne [YY97]. Problem może nie dotyczyć wyłącznie samej implementacji, ale może być zaprojektowany na poziomie standardu: np. generator Dual EC (standard: ANSI X.92, ISO/IEC 18031, NIST 800-90) realizował de facto atak kleptograficzny [CNE+14]. Sposoby przeprowadzania ataków kleptograficznych na systemy głosowania zostały opisane w [GKK+06].
Błędy w implementacji [NSS+17] mechanizmów generowania kluczy na estońskich dowodach osobistych były powodem konieczności wymiany wszystkich dowodów na nowe. Tego rodzaju błąd potencjalnie umożliwiał atakującemu oddanie głosu za wyborcę. Ponieważ mogło to mieć masowy charakter, w konsekwencji dawało to realną możliwość przejęcia władzy w kraju.

Ponownie jak w przypadku Z1), wiele można osiągnąć poprzez wykorzystanie fizycznego kanału komunikacyjnego pomiędzy komisją a wyborcą - przesłanie danych na nieelektronicznym nośniku eliminuje większość ataków.

Ad. Z3)
Wykorzystanie systemów E2E-V umożliwia szybkie wykrycie przejęcia elektronicznej urny: dzięki mechanizmom weryfikowalności wyborcy są w stanie wykryć, że ich głosy są modyfikowane bądź usuwane (w szczególności dzięki sprawdzeniu E2 - *recorded as cast*). W celu zwiększenia dostępności i minimalizacji skutków ataków typu DDOS (*distributed denial of service*), wartym rozważenia jest wykorzystanie systemów typu *distributed ledger* (w stylu kryptowaluty Ethereum) do przechowywania zakodowanych głosów.

Przykładowe rozwiązania techniczne

Systemy głosowania zdalnego były i są wykorzystywane w wiążących wyborach w wielu krajach. Najbardziej istotnymi przykładami są:

- System głosowania przez Internet w Estonii,
- System głosowania zdalnego [Gj10], wykorzystywany w wyborach samorządowych w 2011 i 2013 w Norwegii (w 2013 roku przez Internet oddało głos ok 70 tys., czyli ok 38% z 250 tys. uprawnionych - system był dostępny w 12 okręgach).
- Głosowanie w kantonach w Szwajcarii.

Estonia

System głosowania w Estonii jest całkowicie elektroniczny: uwierzytelnianie opiera się o dowód osobisty wyposażony w warstwę elektroniczną, głos oddaje się za pomocą komputera wyborcy.

Od 2015 roku, po fali krytyki m. in. w [SFD+14], wprowadzono mechanizmy weryfikacji - obecnie wyborcy, za pomocą telefonu komórkowego mogą zweryfikować poprawność zaszyfrowania głosu przez ich komputer (*recorded as cast*). Niestety, system nie zapewnia ani tajności głosu (względem komputera). jak i uniemożliwia zweryfikowania poprawności pozostałych etapów przetwarzania głosów.

Przykład estoński został przywołany z uwagi na jeden aspekt, który w ich systemie miał działać dobrze: miał on oferować silne uwierzytelnianie wyborcy, dzięki wykorzystaniu podpisu generowanego przez elektroniczny dowód osobisty (ostatecznie okazało się, że implementacja posiadała krytyczne błędy umożliwiające podrabianie podpisów). System nie gwarantuje własności: E4, E5.

Norwegia

W Norwegii komisja wyborcza posiadała adres pocztowy oraz numer telefonu komórkowego każdego zarejestrowanego wyborcy. Do głosowania wykorzystywano 3 kanały komunikacyjne. Wyborcy otrzymywali papierowe karty wyborcze przesyłane pocztą. Karty te zawierały wydrukowane kody potwierdzające. Wyborcy do oddania głosu wykorzystywali komputery, na których dokonywali wyboru (brak tajności w stosunku do komputera). Po oddaniu głosu na telefon głosującego wysyłane były kody potwierdzające - po porównaniu ich z kodami wydrukowanymi na karcie, wyborca wykonywał *de facto* dwu sprawdzeń: *cast as intended* oraz *recorded as cast*.
Wybrana grupa specjalistów mogła w imieniu społeczeństwa przeprowadzić *sprawdzenie tallied as recorded*. System norweski nie zapewniał własności: E6, E7, E8.

Remotegrity

Omówione powyżej systemy mają na celu umożliwienie głosowania przez internet. Opisany poniżej system Remotegrity [ZCC+13] ma wiele cech wspólnych z tymi opisanymi powyżej. Różni się przede wszystkim w trzech aspektach:

- Oferuje jednolitą metodę generowania i zliczania głosów zarówno dla głosowania korespondencyjnego, jak i głosowania przez Internet - dzięki czemu może stanowić opcję na płynne przejście z systemu korespondencyjnego na system głosowania internetowego.
- Zapewnia tajność głosu w stosunku do komputera, z którego jest przesyłany głos.
- Wprowadza mechanizm umożliwiający nie tylko na wykrycie niepoprawnego zapisania głosu, ale w wielu przypadkach umożliwia wyborcy na naprawienie problemu (poprzez linkowalne nadpisanie głosu).

Generowanie kart do głosowania (z kodami potwierdzającymi wydrukowanymi pod zdrapkami) może przebiegać analogicznie do np. systemu Scantegrity [CCC+10], albo do sposobu, który był wykorzystywany w Norwegii. Wyborca po otrzymaniu karty do głosowania i karty autoryzacyjnej (zawierającej jednorazowe kody, dzięki którym system przyjmie przesłany głos) może oddać głos na jeden z poniższych sposobów:

- zaznaczyć wybór na karcie do głosowania (usuwając zdrapkę przy wybranych kandydatach), zapisać odpowiadające wyborowi kody potwierdzające i odesłać kartę do komisji, albo:
- zaznaczyć wybór na karcie do głosowania (usuwając zdrapkę przy wybranych kandydatach), wprowadzić kody potwierdzające na stronie głosowania.

Rekomendacje

Rekomendacje procesowe

Rekomendacja P1: Konkurs na rozwiązania techniczne

Metoda wyboru rozwiązania technicznego oparta o specyfikację istotnych warunków zamówienia nie znajduje zastosowania w przypadku wyboru systemu do głosowania elektronicznego. Metoda ta zakłada bowiem, że

1. wszystkie istotne wymagania w stosunku do zamówienia mogą być określone z góry,
2. zamawiający posiada personel mający kompetencje merytoryczne do sformułowania specyfikacji,

Warunki te nie są spełnione:
Ad 1) bezpieczeństwo rozwiązania związane jest ze współdziałaniem wszystkich elementów systemu. Jego załamanie może być spowodowane niedostatecznie wyspecyfikowanymi detalami, które mogą być zaimplementowane w sposób zgodny z zamówieniem, jednak kreujący zagrożenie bezpieczeństwa.
Ad 2) Specjaliści posiadający odpowiednią wiedzę i doświadczenie w zakresie budowy bezpiecznych systemów informatycznych są poszukiwani na rynku pracy. Pozyskanie takich specjalistów do zaprojektowania specyfikacji może być niewykonalne, m.in. ze względu na relatywnie niski poziom wynagrodzenia i wysoki poziom ryzyka.

Rekomendowany sposób postępowania to postępowanie konkursowe na wzór konkursów przeprowadzonych przez NIST w USA (na standardowe funkcje kryptograficzne) oraz przez program ECRYPT w Europie (na metody szyfrowania strumieniowego). Tryb konkursowy musi zapewniać:

1. ocenę całości rozwiązania wraz z demonstratorami kluczowych komponentów technicznych,
2. dostęp oceniających do wszelkich detali proponowanego rozwiązania, komponenty typu “czarnej skrzynki” mogą być użyte jedynie, gdy ich opanowanie przez adwersarza nie prowadzi do załamania mechanizmu bezpieczeństwa,

3. możliwość ewaluacji propozycji przez każdą zainteresowaną stronę, w tym przez autorów konkurencyjnych rozwiązań.

Konkurs powinien być wieloetapowy, umożliwiając koncentrację w końcowej fazie na kluczowych propozycjach.

Rekomendacja P2: Proces decyzyjny

W konkursie, o którym mowa w poprzedniej rekomendacji, decyzje związane z wyborem rozwiązań do dalszego postępowania powinny być podejmowane przez:

- wyłącznie osoby niezależne od organizacji o charakterze politycznym i nieprowadzące działalności politycznej,
- specjaliści z wszystkich dziedzin kluczowych dla właściwego wyboru rozwiązania (oprócz specjalistów od bezpieczeństwa komputerowego również socjolodzy, prawnicy, politolodzy),
- zaproszone osoby o najwyższym autorytecie technicznym w tej dziedzinie na świecie.

Dokumentacja decyzji podejmowanych w trakcie konkursu powinna zawierać uzasadnienie umożliwiające wyborcy zrozumienie i zaufanie podjętym decyzjom, a także zdobycie świadomości marginesu ryzyka.

Ograniczenie grona decyzyjnego do prawników i/lub osób zaangażowanych w działalność polityczną przesądziłoby o braku wiarygodności rozwiązania (brak zaawansowanej wiedzy technicznej, konflikt interesów).

Rekomendacja P3: Transparentność

Proces decyzyjny powinien być udokumentowany, powinien również uwzględniać wysłuchania publiczne zainteresowanych stron. Informacje i uwagi zgłaszane gremium decyzyjnemu powinny mieć utrwaloną postać i być uwierzytelnione np. za pomocą podpisu elektronicznego.

Całość dokumentacji związanej z konkursem powinna być publicznie dostępna.

Rekomendacja P4: Nadzór nad całością cyklu życiowego rozwiązania

Rozwiązanie techniczne wymaga stałego nadzoru również po zakończeniu budowy systemu. Związane jest to z monitorowaniem poziomu zagrożeń na przykład ze względu na zmieniające się możliwości techniczne potencjalnych adwersarzy.

Dotychczas zadania takie wykonuje Państwowa Komisja Wyborcza. Ze względu na techniczny charakter zagrożeń PKW wymagałaby istotnego wzmocnienia o specjalistów i możliwości wykonywania specjalistycznych badań.

Rekomendacja P5: ograniczony zakres zastosowania metodologii Common Criteria

Do wyboru systemów pod kątem bezpieczeństwa często stosuje się metodologię Common Criteria. Rekomenduje się stosowanie tej techniki co najwyżej pomocniczo, do wstępnej oceny pojedynczych komponentów.

Rekomendacja wynika z filozofii Common Criteria, gdzie oprócz godnej wykorzystania metodologii opartej na ocenie wartości, ryzyk i odpowiadających formalnych "security objectives", końcowe rozwiązanie opiera się na wykorzystaniu standardowych komponentów. Wyrażamy daleko idącą wątpliwość, czy budowa bezpiecznego i godnego zaufania systemu służącego do głosowania za pomocą sieci teleinformatycznych jest możliwa za pomocą takiego podejścia.

W przypadku wykorzystania komponentów posiadających certyfikaty CC, należy poddać drobiazgowej analizie, czy Protection Profile, w oparciu o który wydano certyfikat, odpowiada potrzebom systemu.

Rekomendacja P6: etapowe wprowadzanie rozwiązania

Standardowym sposobem postępowania w przypadku dużych projektów informatycznych jest etapowanie budowy systemu. Początkowo system wdraża się w ograniczonej skali. Pozwala to na zredukowanie skutków nieuniknionych początkowo awarii/błędów/braku należytej sprawności w funkcjonowaniu systemu.

Postępowanie takie jest rekomendowane. Scenariusz wprowadzania rozwiązania powinien być integralnym elementem rozwiązania wyłonionego w ramach konkursu, o którym mowa w rekomendacji P1. Scenariusz ten powinien również uwzględniać czynniki socjologiczne - przystosowanie wyborców do korzystania z systemu.

Rekomendacje techniczne

Ze względu na trudność zadań rekomendowane jest podejście dające największe efekty w zakresie podniesienia poziomu bezpieczeństwa i dostępności, niekoniecznie kładąc nacisk na pełną elektronizację procesu głosowania.

W Estonii podjęto ryzyko prędkiego i kompleksowego wdrażania elektronizacji procesu wyborczego, co zakończyło się wdrożeniem systemu:

- z poziomem tajności uzależnionym od uczciwego trybu działania systemu weryfikacji i dekodowania głosów przy braku procedur weryfikacyjnych,
- podatności na atak na komputery wyborców (możliwość zmiany oddanych głosów na dużą skalę a w konsekwencji przejęcia władzy w państwie),
- opartym o karty kryptograficzne (estoński dowód osobisty) z wadliwie zaimplementowanym algorytmem RSA, co skutkuje możliwością oddania głosu na podstawie znajomości certyfikatu klucza publicznego ofiary.

W związku z tym rekomendowane jest w pierwszym etapie ograniczenie elektronizacji do:

- **składania głosu drogą elektroniczną,**
- **procedur weryfikacji, że głos złożony został zgodnie z intencją wyborcy i uwzględniony w wyniku końcowym.**

Wymagać to będzie zachowania procesu przekazania niezależnym kanałem informacji umożliwiających złożenie głosu.

Podejście takie pozwala na osiągnięcie:

- **gwarancji dostarczenia głosu (co jest poważnym postępem w stosunku do głosowania korespondencyjnego),**
- **gwarancji prawidłowego policzenia głosu i odporności na jego unieważnienie (co jest poważnym postępem w stosunku do głosowania tradycyjnego).**

Krytyczne uwarunkowania techniczne

Czynnik Cz1: okres realizacji projektu

Powszechne niedoszacowanie czasu potrzebnego na realizację tego typu projektów wynika z brania pod uwagę jedynie okresu czasu niezbędnego na napisanie i uruchomienie określonego kodu. W przypadku systemu tak wrażliwego na błędy w zakresie wiarygodności, bezpieczeństwa i ochrony prywatności, ciężar przesuwa się na etapy:

1. wyboru koncepcji i projektowania,
2. testowania i nadzoru,
3. udokumentowania końcowemu użytkownikowi (wyborcy) własności systemu.

Co więcej, czas potrzebny realizację faz 2 i 3 silnie zależy od rezultatów fazy pierwszej, tak więc **nie sposób z góry określić czasu potrzebnego na realizację całego procesu.**
W tym kontekście okres czasu wynikający z procedur przetargowych i realizacji kodu jest stosunkowo łatwo przewidywalny, choć doświadczenie projektów e-administracji uczy, że nawet w prostych sytuacjach dochodzi do znacznych opóźnień.

Wzorując się na analogicznych procesach wyboru standardów dla funkcji kryptograficznych, można by stwierdzić, że **sam okres potrzebny na prawidłową realizację pierwszego etapu to co najmniej rok do 3 lat (SHA-3 Competition - wybór funkcji haszującej rozpoczął się w 2008 roku, a zakończył w 2012; wybór AES - Advanced Encryption Standard trwał od 1997 do 2000 roku).** W tej sytuacji **krytycznym zagrożeniem dla projektu jest niestabilność polityki Państwa wyrażająca się w ciągłych zmianach organizacyjnych i koncepcyjnych.**

Czynnik Cz2: rejestr wyborców

Jakkolwiek wiele krajów (USA, Australia, …) realizuje system wyborczy bez wsparcia w postaci rejestru wyborców, stwarza to możliwość wielokrotnego głosowania przez tę samą osobę, lub wręcz głosowania na podstawie fikcyjnej tożsamości. W przypadku głosowania drogą elektroniczną niebezpieczeństwo takie wzrasta, ze względu na mniejsze ryzyko złapania na gorącym uczynku. Brak centralnego rejestru może również ułatwiać dokonywanie oszustw wyborczych przez komisje wyborcze.

Rejestr wyborców może/powinien być realizowany w oparciu o rejestr PESEL, jednak nie jest z nim tożsamy. W przypadku referendów państwowych stopień skomplikowania jest jednak znacząco mniejszy niż w przypadku wyborów samorządowych, ze względu na brak problemów związanych z przypisaniem wyborcy do okręgu wyborczego, czy z uczestnictwa w wyborach obywateli UE nie będących obywatelami Polski.

Rejestr wyborców jest podstawą do wydawania obywatelom środków umożliwiających głosowanie drogą elektroniczną i/lub blokowania tej możliwości (na przykład w przypadku pozbawienia praw publicznych, czy w przypadku kradzieży lub utraty środków umożliwiających takie głosowanie).

Czynnik Cz3: elektroniczna identyfikacja wyborców

Warunkiem koniecznym dla realizacji procesów wyborczych jest na którymś etapie zapewnienie, że osoba będąca w interakcji z instytucjami zaangażowanymi w systemie wyborczym jest faktycznie uprawnionym wyborcą. Pierwotny kontakt tego typu musi mieć charakter fizyczny, jednak w momencie tym wyborca może zostać wyposażony w środki służące mu później do identyfikacji w sposób elektroniczny. Środki te powinny być odporne na niebezpieczeństwa związane z kradzieżą czy sprzedażą tożsamości (m.in. sprzedaż głosów).

Narzędzia typu EPUAP w obecnym kształcie w bardzo ograniczonym stopniu odpowiadają potrzebom ze względu na uwierzytelnianie za pomocą tak słabych narzędzi jak login-hasło i weryfikacja za pomocą adresu poczty elektronicznej. W istocie EPUAP oparty jest o silne uwierzytelnianie dokumentów dokonywane nie przez obywatela, lecz przez serwer będący pod zarządem administracji rządowej, z definicji zależnej od wyników wyborów.

Dobrze zrealizowana elektroniczna identyfikacja i uwierzytelnianie wyborców powinny zapewniać jednocześnie następujące warunki:

- pełną kontrola wyborcy,
- odporność na sprzedaż tożsamości - ze względu na inne czynniki wyborca powinien być silnie zniechęcony do sprzedaży tożsamości; alternatywnie, kupujący tożsamość powinien być zniechęcony do zakupu poprzez prostą możliwość oszukania przez sprzedającego,
- silne uwierzytelnianie na poziomie zaawansowanego podpisu elektronicznego,
- silna pseudonimizacja na poziomie kryptograficznej nierozróżnialności od pseudonimów losowych.

Skądinąd budowa takiego narzędzia jest kluczowa dla cyberbezpieczeństwa Państwa, budowy e-administracji, zwalczania przestępczości (zwłaszcza w zorganizowanej postaci), czy rozwoju rynku gospodarki i usług elektronicznych.

Rozwiązania mogące podołać temu zadaniu to przede wszystkim elektroniczny dokument tożsamości z funkcjami bezpieczeństwa zrealizowanymi na drodze elektronicznej. Dokument taki (lub dokumenty) mógłby być wydawany zarówno przez instytucje państwowe oraz instytucje prywatne.

Czynnik Cz4: wsparcie informacyjne

Warunki takie jak weryfikowalność wyborów wymagają stworzenia infrastruktury bezpiecznego i uwierzytelnionego publikowania informacji. Po stronie technicznej wymaga to stworzenia repozytoriów informacji, które zapewniałyby jednocześnie weryfikowalne gwarancje dla wyborcy w zakresie:

1. pochodzenia poszczególnych informacji,
2. odporności na usuwanie informacji i zmiany ich kolejności,
3. dostępności.

Technologie pozwalające osiągnąć te cele są obecnie intensywnie rozwijane (*blockchain, distributed ledger,...*), jednak zadanie to nie jest trywialne i wymaga sporego wysiłku w realizacji.

Zaznaczyć jednak należy, że realizacja powyższych zadań i tak jest nieuchronna, choćby w kontekście zapewnienia odpowiedniego poziomu bezpieczeństwa dla rejestrów państwowych.

Czynnik Cz5: niezależny kanał komunikacji z wyborcą

Obecnie nie jest znane bezpieczne rozwiązanie oparte wyłącznie na komunikacji przez komputer wyborcy bez udziału niezależnego od niego kanału komunikacyjnego. W związku z tym należy się liczyć z koniecznością budowy takiego kanału. Obecnie dostępne możliwości to:

1. przesyłanie informacji drogą pocztową,
2. komunikacja za pomocą telefonu wyborcy - poprzez sieć telefoniczną,
3. komunikacja za pomocą telefonu wyborcy - poprzez komputer wyborcy, odczyt zaszyfrowanej wiadomości optycznie przez telefon wyborcy,
4. komunikacja za pomocą zaufanej strony trzeciej,
5. komunikacja za pomocą elektronicznego dokumentu tożsamości.

Każde z tych rozwiązań jest obarczone pewnymi wadami:
Ad 1) W przypadku tego kanału atak może polegać na fizycznym niszczeniu kopert wyborczych pochodzących z okręgów, gdzie preferencje wyborcze nie odpowiadają preferencjom strony atakującej. Schemat korzystający z tego kanału powinien uwzględniać sytuacje, w których do zaginięcia przesyłek jednak dochodzi. Pod uwagę musi być brana pod uwagę niska jakość usług pocztowych (problemy z terminowością, zaginięcia przesyłek). Uwzględnić też trzeba niskie zaufanie części wyborców do Poczty Polskiej jako organizacji zależnej od administracji rządowej.
W związku z tym preferowane rozwiązanie to przesłanie karty wyborczej drogą pocztową, jednak odesłanie głosu odpowiednim kanałem elektronicznym.
Ad 2) Opcja ta wymaga zarejestrowania numeru telefonicznego obywatela do celów wyborczych. Jakikolwiek schemat wyborczy musi brać pod uwagę realia poziomu bezpieczeństwa przesyłania wiadomości SMS.
Ad 3) Opcja ta wymaga zaimplementowania na telefonie wyborcy asymetrycznego algorytmu szyfrowania nie wymaga natomiast kontaktu za pomocą wiadomości SMS od operatora telefonicznego. Może to być szczególnie atrakcyjna opcja ze względu na wyborców znajdujących się za granicą, gdzie usługi SMS mogą być zawodne lub

niedostępne. Zasadniczą trudnością jest budowa infrastruktury klucza publicznego i implementacja kluczy prywatnych na urządzeniach wyborców.
Ad 4) Instytucje takie jak banki, są w stanie pod względem technicznym zapewnić kanał komunikacyjny zapewniający komunikację ze stosunkowo silnie uwierzytelnionym odbiorcą. Budowa takiego kanału w sposób zapewniający anonimowość i poufność jest jednak wyzwaniem.
Ad 5) Elektroniczny dokument tożsamości mógłby być doskonałym środkiem do budowy uwierzytelnionego i zanonimizowanego kanału pomiędzy wyborcą a komisjami wyborczymi, wykorzystując takie na przykład narzędzia jak podpis domenowy. Z drugiej strony implementacja takiego projektu trwa wiele lat (wliczając w szczególności okres wymiany dokumentów tożsamości), a obecnie prowadzone w Polsce prace nie odpowiadają reżimom niezbędnym do wykorzystania w procesach wyborczych (brak otwartości procesu projektowego, brak wsparcia anonimowej komunikacji, …).

Z drugiej strony, budowa kanału komunikacyjnego o odpowiednio wysokich parametrach pod kątem pseudonimizacji, uwierzytelniania i niezaprzeczalności, stanowi jeden z podstawowych warunków dla zapewnienia cyber-bezpieczeństwa Państwa w e-administracji oraz faktycznego wdrożenia zasad ochrony danych osobowych.

Bibliografia

[Adi08] Adida, B., 2008, July. Helios: Web-based Open-Audit Voting. In *USENIX security symposium* (Vol. 17, pp. 335-348).

[CCC+10] Carback, R., Chaum, D., Clark, J., Conway, J., Essex, A., Herrnson, P.S., Mayberry, T., Popoveniuc, S., Rivest, R.L., Shen, E. and Sherman, A.T., 2010. Scantegrity II municipal election at Takoma Park: the first E2E binding governmental election with ballot privacy.

[CNE+14] Checkoway, S., Niederhagen, R., Everspaugh, A., Green, M., Lange, T., Ristenpart, T., Bernstein, D.J., Maskiewicz, J., Shacham, H. and Fredrikson, M., 2014, August. On the Practical Exploitability of Dual EC in TLS Implementations. In *USENIX security symposium* (pp. 319-335).

[GKV+16] Gaweł, D., Kosarzecki, M., Vora, P.L., Wu, H. and Zagorski, F., 2016, October. Apollo–End-to-End Verifiable Internet Voting with Recovery from Vote Manipulation. In *International Joint Conference on Electronic Voting* (pp. 125-143). Springer.

[GKK+06] Gogolewski, M., Klonowski, M., Kubiak, P., Kutyłowski, M., Lauks, A. and Zagórski, F., 2006. Kleptographic attacks on e-voting schemes. In *Emerging Trends in Information and Communication Security* (pp. 494-508). Springer, Berlin, Heidelberg.

[Gjo10] Gjøsteen, K., 2011, September. The Norwegian internet voting protocol. In *International Conference on E-Voting and Identity*(pp. 1-18). Springer, Berlin, Heidelberg.

[HLW11] Heiberg, S., Laud, P. and Willemson, J., 2011, September. The application of i-voting for Estonian parliamentary elections of 2011. In *International Conference on E-Voting and Identity*(pp. 208-223). Springer, Berlin, Heidelberg.

[KTV10] Küsters, R., Truderung, T. and Vogt, A., 2010, October. Accountability: definition and relationship to verifiability. In *Proceedings of the 17th ACM conference on Computer and communications security* (pp. 526-535). ACM.

[NSS+17] Nemec, M., Sys, M., Svenda, P., Klinec, D. and Matyas, V., 2017, October. The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1631-1648). ACM.

[PKRV10] Popoveniuc, S., Kelsey, J., Regenscheid, A. and Vora, P., 2010, August. Performance requirements for end-to-end verifiable elections. In *Proceedings of the 2010 international conference on Electronic voting technology/workshop on trustworthy elections* (pp. 1-16). USENIX Association.

[RV17] Rivest, R.L. and Virza, M., 2017. Software independence revisited. *Real-World Electronic Voting: Design, Analysis and Deployment. CRC Press, Boca Raton*.

[SFD+14] Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M. and Halderman, J.A., 2014, November. Security analysis of the Estonian internet voting system. In *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (pp. 703-715). ACM.

[YY97] Young, A. and Yung, M., 1997, May. Kleptography: Using cryptography against cryptography. In *Eurocrypt* (Vol. 97, pp. 62-74).

[ZCC+13] Zagórski, F., Carback, R.T., Chaum, D., Clark, J., Essex, A. and Vora, P.L., 2013, June. Remotegrity: Design and use of an end-to-end verifiable remote voting system. In *International Conference on Applied Cryptography and Network Security*(pp. 441-457). Springer, Berlin, Heidelberg.