Dlaczego jeszcze nie głosujemy elektronicznie?

Jakub Zadrożny

Streszczenie

Esej przybliża zagadnienie głosowania elektronicznego poprzez krótki opis wykorzystywanych obecnie technologii, dotychczasowych doświadczeń, analizę zagrożeń oraz nietypowych prób rozwiązania problemu.

1 Wstęp

W ciągu ostatnich kilkudziesięciu lat komputery zdominowały niemal wszystkie dziedziny naszego życia. Urzędy, szkoły, uniwersytety, przedsiębiorstwa, instytucje są w dużej mierze zarządzane przy użyciu zinformatyzowanych systemów. Pod kontrolą komputerów znajduje się coraz więcej skomplikowanych procesów - to właśnie one dbają o bezpieczeństwo naszego konta bankowego, sterują ruchem w naszych miastach i pilotują samoloty, którymi latamy.

Jednym z niewielu przedsięwzięć, wciąż stawiających opór informatyzacji, jest organizacja wyborów w demokratycznych państwach. W większości z nich, w tym w Polsce, głosujemy przecież zakreślając długopisem odpowiednie pola na kartkach papieru, które są następnie ręcznie zliczane przez członków komisji wyborczych. Jak to możliwe, że w czasach tak silnie zdominowanych przez komputery nie zdołaliśmy wykorzystać ich do przyspieszenia, usprawnienia i poprawienia bezpieczeństwa demokratycznych wyborów? A może taki rozwiązanie istnieje, lecz nie zostało wystarczająco spopularyzowane?

2 Technologie i wykorzystanie

Perspektywa zmechanizowanego lub skomputeryzowanego głosowania wydaje się niezwykle kusząca - bylibyśmy w stanie przyspieszyć liczenie wyniku, pozbyć się ogromnych ilości papierowych głosów, ułatwić głosowanie osobom niepełnosprawnym, a może nawet poprawić bezpieczeństwo wyborów i zmniejszyć koszty ich przeprowadzenia. Sięgając po te korzyści, mieszkańcy demokratycznych państw już od dawna starali się zmierzyć z zagadnieniem automatyzacji wyborów. Ich dotychczasowe próby możemy podzielić na dwie kategorie:

- *e-głosowanie* - wybory odbywają się w nadzorowanym przez komisję środowisku (lokalu wyborczym), a komputery wykorzystywane są do zbierania lub liczenia głosów,
- *i-głosowanie* - wybory odbywają się przez internet, komputery służą do weryfikacji wyborcy, zbierania i liczenia głosów oraz zabezpieczenia całego procesu.

Instytut Informatyki Uniwersytetu Wrocławskiego, 2016–2017
Esej przygotowany w ramach zajęć *Kultura bezpieczeństwa komputerowego*

2.1 E-głosowanie [?, ?]

Pierwsze maszyny rejestrujące głosy w komisjach wyborczych i liczące je automatycznie pojawiły się już pod koniec XIX wieku. Oczywiście były to konstrukcje czysto mechaniczne, jednak zasada ich działania jest niemal identyczna jak współczesnych rozwiązań komputerowych.

2.1.1 Lever machine

Jednym z pierwszych takich wynalazków była tzw. *lever machine*. Urządzenie to składało się z wielu dźwigni, z których każda przypisana była do konkretnego kandydata. Aby oddać głos wyborca musiał pociągnąć za jedną z nich, co skutkowało przekręceniem odpowiedniego licznika w środku maszyny. Maszyna posiadała również odpowiednie zabezpieczenia uniemożliwiające podwójne głosowanie. Została wprowadzona do użytku pod koniec XIX wieku i po pewnym czasie zyskała ogromną popularność. W 1960 roku ponad połowa głosów w Stanach Zjednoczonych była rejestrowana właśnie przy jej użyciu. Wynalazek został wycofany z użycia w USA dopiero w 2010 roku.

2.1.2 Skanowanie optyczne

Innym pomysłem na automatyzację liczenia głosów było wykorzystanie skanowania optycznego. Głosy musiały być zarejestrowane na tradycyjnych nośnikach (kartach papieru lub kartach perforowanych), które mogły być skanowane przez komputer zliczający głosy. Metodę tę stosuję się w Ameryce nieprzerwanie od 1964 roku, a szczyt jej popularności przypadł na 1996 rok, kiedy to ponad 60% głosów w Stanach Zjednoczonych zostało oddanych przy jej użyciu.

2.1.3 Direct Recording Electronics

Najnowszym rozwiązaniem są tzw. systemy DRE. Tak naprawdę są to tylko skomputeryzowane *lever machines*. Ich działanie jest następujące: urządzenie prezentuje listę kandydatów wyborcy, który używając odpowiedniej metody wprowadzania (klawiatury, przycisku lub ekranu dotykowego) może zaznaczyć swoją preferencję, tym samym oddając głos. Komputer następnie zapisuje głos na lokalnym nośniku danych lub przekazuje go do zbioru centralnego. Urządzenia te wykorzystywane są na dużą skalę m.in w Brazylii (od 1996 głosuje się tam jedynie za ich pośrednictwem), Indiach (od 2003 jedyna metoda głosowania) oraz USA (znacznie mniejsza skala niż w Brazylii i Indiach). W Holandii oraz Kazachstanie metoda ta była wykorzystywana powszechnie, ale na skutek protestów obywatelskich została porzucona na rzecz tradycyjnego głosowania papierowego [**?**].

2.2 I-głosowanie

Wraz z rozpowszechnieniem się internetu rozpoczęły się eksperymenty z głosowaniem za jego pośrednictwem. Z jednej strony stwarza to ogromne możliwości np. dla ekspatriantów i osób niepełnosprawnych, z drugiej jednak przedstawia nowe wyzwania w zakresie bezpieczeństwa. Dotychczasowe podejścia opierają się na dwóch głównych środkach komunikacji.

2.2.1 Poczta elektroniczna i fax

Najprostszą formą głosowania przez internet jest przesyłanie swoich głosów pocztą elektroniczną lub faxem do urzędników, którzy następnie weryfikują głosy i rejestrują je w systemie. Niektóre

państwa, np. Stany Zjednoczone, Francja i Szwajcaria, dopuszczają taką możliwość żołnierzom przebywającym poza granicami kraju oraz ekspatriantom [**?**].

2.2.2 Dedykowane aplikacje webowe

Nieco bardziej skomplikowane jest udostępnienie wyborcom specjalnej aplikacji webowej, która byłaby w stanie uwierzytelnić ich jako obywateli, zarejestrować ich głos i przesłać go na centralny serwer, zapewniając jednocześnie odpowiedni poziom bezpieczeństwa. Wdrożenia takiego systemu na dużą skalę podjęło się tylko jedno państwo - Estonia. Za pomocą aplikacji na swoim komputerze wyborca może uwierzytelnić się używając specjalnego e-dowodu osobistego i oddać swój głos. Ta informacja jest następnie przesyłana do centralnej bazy danych i przechowywana do czasu ostatecznego zliczania. Przed zliczaniem, z każdego głosu usuwane mają być dane pozwalające na zidentyfikowanie osoby, od której dany głos pochodzi [**?**].

Estonia, jako pierwsza na świecie, przeprowadziła legalnie wiążące wybory z możliwością głosowania przez internet w 2005. Projekt został ogłoszony sukcesem i od tego czasu możliwość głosowania przez internet jest oferowana każdemu obywatelowi Estonii w kolejnych wyborach. W 2005 niespełna 2% wyborców oddało głos *on-line*, jednak w wyborach lat 2014 i 2015 było to już ponad 30% [**?**].

3 Udokumentowane ataki

Wielu ludzi na świecie zdaje sobie sprawę, że zagadnienie komputeryzacji wyborów nie jest tak proste, jak mogłoby się wydawać. Głównym problemem nie jest przecież stworzenie systemu, który działa, a systemu, który działa i jest odporny na różnego rodzaju spiski i ataki hakerów. Z tego powodu eksperci nieustannie zadają sobie trud i starają się przedostać przez zabezpieczenia dostępnych na rynku rozwiązań i w ten sposób zwrócić uwagę władz i opinii publicznej na zagrożenia, jakie wiążą się z informatyzacją wyborów. Dzięki ich pracy dowiadujemy się, że przeprowadzenie ataku na dostępne na rynku i wykorzystywane w praktyce systemy nieraz okazuje się nie tylko możliwe, ale niestety prostsze niż można by przypuszczać...

3.1 E-głosowanie

Odpowiednie zabezpieczenie maszyny DRE przeznaczonej do użytku w lokalu wyborczym wydaje się być zadaniem możliwym do wykonania. Mimo tego znane są nam przykłady urządzeń, które uzyskały certyfikaty bezpieczeństwa w kilku stanach USA i przez lata były używane w rzeczywistych wyborach, a do których włamać mógłby się nawet komputerowy laik.

3.1.1 AVS WINVote [**?**]

Urządzenie typu DRE pochodzące od firmy *Advanced Voting Solutions* zostało dopuszczone do użytku (i było faktycznie używane) w trzech stanach USA: Pensylwanii, Missisipi i Virginii. Dopiero w roku 2015, po przeprowadzeniu kontroli bezpieczeństwa, utraciło certyfikat w ostatnim z nich. Lista luk i uchybień, które zostały podczas niej wykryte, jest skandalicznie wręcz długa, a wnioski, które z niej wyciągamy są zdecydowanie powodem do obaw. Oto niektóre błędy:

- maszyny połączone były bezprzewodową siecią LAN, zabezpieczoną przestarzałym protokołem WEP; hasło zostało ustawione na “abcde”, a jego zmiana nie była możliwa,
- system operacyjny był wersją Windowsa XP, a ostatnia łatka bezpieczeństwa została zainstalowana w 2004 roku (decertyfikacja nastąpiła w roku 2015!),

- hasło administratora systemu było ustawione na “admin”,
- opcja udostępniania plików w sieci była włączona,
- urządzenie zapisywało pliki w bazie MS Access zabezpieczonej przez krótkie hasło (“shoup”),
- system nie rejestrował zmian w bazie danych,
- fizyczne porty nie były w żaden sposób zabezpieczone.

Jak wskazuje Jeremy Epstein, ekspert od spraw bezpieczeństwa, odkrycie tych luk nie wymagało żadnych skomplikowanych narzędzi ani technik, a każda osoba, choć trochę znająca się na komputerach, byłaby w stanie wykraść bazę oddanych głosów, dowolnie ją zmienić i wgrać z powrotem na serwer, nie zostawiając żadnych śladów w systemie. Prowadzi to do wniosku, że **jeśli** żadne wybory w jednym z trzech stanów używających WINVote-ów nie zostały zmanipulowane, to tylko dlatego, że nikt nie podjął takiej próby.

3.1.2 Diebold AccuVote-TS [?]

Rozwiązanie typu DRE wyprodukowane przez firmę Diebold Election Systems było swego czasu najpowszechniej używanym systemem DRE w Stanach Zjednoczonych, a inny system od tego producenta jest jedynym środkiem rejestracji głosów w Brazylii. W wyborach w Stanach Zjednoczonych w 2006 roku ponad 10% wszystkich głosów zostało oddanych za jego pośrednictwem.

Grupa naukowców z Princeton University opublikowała raport, w którym przedstawia luki w zabezpieczeniach systemu *AccuVote*. Złamanie zabezpieczeń i zmanipulowanie wyniku było znacznie trudniejsze w wypadku tego urządzenia niż *AVS WINVote*, jednak wpływ, jaki potencjalny atak mógłby wywrzeć na wynik wyborów, był odpowiednio większy. Zgodnie z tym raportem, każda osoba, posiadająca choćby jednominutowy dostęp bez nadzoru do jednej z maszyn, mogłaby wgrać na nią złośliwe oprogramowanie. Takie oprogramowanie byłoby w stanie zmienić wszystkie oddane głosy i zmanipulować dowolnie wynik przy minimalnym ryzyku wykrycia, nawet po wnikliwej analizie ekspertów. Ponadto wspomniane oprogramowanie byłoby w stanie zainfekować również inne maszyny w chwili, gdy pracownicy komisji wykonywaliby rutynowe czynności wyborcze. Zatem instalując wirusa na jednej maszynie z odpowiednim wyprzedzeniem, atakujący byłby w stanie dotrzeć do wielu więcej, a przez to wpłynąć na znaczącą liczbę głosów.

3.1.3 Inne przypadki

Podobne problemy dotyczą znaczącej liczby innych urządzeń (DRE oraz skanerów optycznych) pochodzących od różnych producentów. Np. komputera wyborczego *Nedap ES3B*, przez który oddawano w Holadnii 90% głosów [**?**], a który okazał się podatny na atak bardzo podobny do opisanego przy maszynie *AccuVote*. W 2007 roku Sekretarz Stanu Kalifornia zarządziła kontrolę bezpieczeństwa wszystkich używanych wówczas w tamtym stanie systemów DRE. Jej przeprowadzenie powierzono grupie ekspertów pod kierownictwem Uniwersytetu Kalifornijskiego. Ekspertyza wykazała poważne uchybienia w każdym z czterech testowanych urządzeń. Błędy były na tyle poważne, że działający w pojedynkę przestępca (niekoniecznie ekspert) mógłby zagrozić bezpieczeństwu wyborów w całym stanie. Na skutek tej kontroli wszystkie urządzenia utraciły swoje certyfikaty [**?**].

Z tych doświadczeń należy wnioskować, że przeprowadzenie ataku na urządzenie wyborcze może się okazać możliwe nawet, jeśli uzyskało ono odpowiedni certyfikat.

3.2 I-głosowanie [?]

Problem zabezpieczenia wyborów internetowych jest znacznie bardziej skomplikowany niż w przypadku elektroniki wykorzystywanej w lokalach wyborczych. Mimo tego znany jest nam jeden przypadek wykorzystania takiego rozwiązania na wielką skalę - Estonia. Ich rozwiązanie nie jest wolne od kontrowersji - przeprowadzonych zostało wiele niezależnych analiz, a wyniki często wskazują jednoznacznie, że zmanipulowanie internetowego głosowania w Estonii było i nadal jest możliwe. Tamtejszy rząd dyskredytuje jednak takie badania i utrzymuje, że internetowy sytem jest w pełni bezpieczny.

Jedną z takich analiz zajął zespół złożony z naukowców Uniwersytetu Michigan oraz kilku niezależnych ekspertów. Skupili się oni na dwóch potencjalnych metodach ataku: od strony serwera oraz od strony klienta.

3.2.1 Atak od strony serwera

Ta metoda zbliżona jest do ataków, na które podatne są często systemy DRE (np. *AccuVote*). Polega ona na wgraniu złośliwego oprogramowania na serwer gromadzący lub zliczający głosy. Jest to droga trudniejsza i łatwiejsza do wykrycia niż atak na komputery klientów, ale - zdaniem analityków - wciąż możliwa, a w efekcie daje kontrolę na całościowym wynikiem wyborów internetowych, czyli w przypadku Estonii ponad 30% wszystkich głosów.

Sam serwer zliczający jest w Estonii dosyć dobrze zabezpieczony, zatem wgranie własnego kodu bezpośrednio na niego wydaje się być trudne. Istnieje jednak furtka w postaci komputera deweloperskiego, z które pochodzi oprogramowanie instalowane na serwerze. Według zespołu analityków możliwe jest przejęcie kontroli nad nim i za jego pośrednictwem odpowiednie spreparowanie systemu przeznaczonego do instalacji na serwerze. Dobrze przygotowane złośliwe oprogramowanie mogłoby ponadto unikać wykrycia np. na skutek liczenia sum kontrolnych lub ręcznych testów.

3.2.2 Atak od strony klienta

Ten sposób opiera się na najbardziej podatnym na ataki ogniwie łańcucha komunikacji - komputerze wyborcy. Według szacunków ok. 30% maszyn jest zainfekowanych różnego rodzaju wirusami, a część z nich należy również do tzw. *botnetów*. Analiza wykazała, że jeśli atakującym udałoby się wgrać złośliwe oprogramowanie na komputer wyborcy, to byłoby ono w stanie zmienić jego głos bez jego wiedzy. Takie oprogramowanie jest w stanie ominąć wszystkie zabezpieczenia w postaci estońskiego e-dowodu tożsamości, osobistego PINu wyborcy oraz mobilnej aplikacji weryfikacyjnej.

Atakując klientów, oszust może zmieniać pojedyncze głosy, co - z pozoru - może wydawać się mało efektywnym podejściem, jeśli jego zamiarem jest zmanipulowanie wyborów w całym kraju. Jednak będąc właścicielem dużego *botnetu*, atakujący jest w stanie wgrać swoje złośliwe oprogramowanie do tysięcy komputerów na raz, a to mogłoby już wywrzeć znaczący wpływ na wynik wyborów. Ponadto niektórzy atakujący mogą okazać się właścicielami wielu *botnetów*...

Podobny atak udało się zademonstrować estońskiemu studentowi Paavo Pihelglasowi, który podał działanie stworzonego przez siebie wirusa jako powód do unieważnienia wyborów. Sąd jednak nie przychylił się do jego wniosku twierdząc, że skoro student doprowadził do takiej sytuacji dobrowolnie, to jego prawa nie zostały pogwałcone [**?**].

4 Zagrożenia

Elektroniczne głosowanie jest niezwykle kuszącą perspektywą. Wydaje się przecież dawać wiele wymiernych korzyści takich jak: uproszczenie procedur, zwiększenie wydajności przez szybsze zliczanie głosów, odporność na ludzkie błędy i oszustwa oraz niższy koszt eksploatacji. Podczas gdy *e-głosowanie* ma z pewnością swoje zalety, to - przy obecnym podejściu władz większości państw i prywatnych korporacji dostarczających im rozwiązania - nie są to niestety żadne z wymienionych. Wszystkie te domniemane korzyści oparte są na jednym, prostym, lecz błędnym założeniu, że komputery się nie mylą. Rzeczywiście, same maszyny dosyć rzadko popełniają błędy, jednak z pewnością mylą się programiści tworzący systemy, które je kontrolują. W efekcie wybory czysto elektroniczne nie są tak bezpieczne, jak wybory papierowe. Bezpieczeństwo to prawdopodobnie główny (chociaż nie jedyny) powód, dla którego większość demokratycznych państw wciąż nie korzysta ze skomputeryzowanych rozwiązań wyborczych.

Taki system musiałby działać na tyle sprawnie, by cały naród skłonny był mu powierzyć przyszłość swojej demokracji. W tym celu powinien spełniać kilka absolutnie podstawowych wymagań [**?**]:

1. Rzetelność - wynik wyborów powinien dokładnie odzwierciedlać wolę narodu. Z tego powodu system nie może zgubić żadnego głosu, pominąć go przy liczeniu czy bezzasadnie unieważnić. Nie może również dodawać sztucznych głosów do puli.

2. Anonimowość - głosowanie musi być całkowicie tajne. Po pierwsze, wyborca musi mieć pewność, że nikt nie dowie się, na kogo oddał swój głos. Po drugie, wyborca nie może być w stanie udowodnić na kogo oddał swój głos, nawet jeśli taka jest jego wola. Tylko taki poziom anonimowości zapewnia ochronę przed kupowaniem i wymuszaniem głosów.

3. Dostępność - wybory muszą odbyć się w wyznaczonym przedziale czasu - nie mogą zostać przesunięte na skutek np. niedostępności serwerów.

4. Przejrzystość - metoda przeprowadzania wyborów musi być prosta, przejrzysta, możliwa do zrozumienia przez ludzi nie będących technikami. Jednocześnie musi być możliwe obserwowanie całego procesu. Jeśli system nie będzie przejrzysty, to wyborcy będą musieli ufać komuś (nie mogąc sprawdzić), że działa on poprawnie, co zwiększy szanse na powodzenie spisku.

5. Bezpieczeństwo - system musi działać poprawnie nawet w przypadku spisku, którego członkami mogą być programiści tworzący system, pracownicy komisji wyborczych, władze lub wyborcy, oraz ataku hakerskiego. Musi również istnieć metoda na wykrycie próby manipulacji i skontrolowanie poprawności wyniku.

W praktyce zbudowanie systemu informatycznego łączącego wszystkie te cechy okazuje się niezwykle trudne, jeżeli w ogóle możliwe. W sytuacji, którą rozważamy, nie chodzi już bowiem o bezpieczeństwo jednostki czy pojedynczej instytucji, jak w przypadku np. bankowości online, ale o bezpieczeństwo całego narodu [**?**]. Oczywiście, tradycyjne, papierowe głosowanie jest wciąż podatne na pewne ataki, ale w jego przypadku zmanipulowanie większej liczby głosów wymaga powiększenia rozmiaru spisku, nakładu pracy i środków oraz zwiększa ryzyko wykrycia przez służby bezpieczeństwa. Potrzebne jest zatem rozwiązanie przynajmniej tak bezpieczne jak wybory tradycyjne.

4.1 E-głosowanie

Potencjalne ataki i szkody, które mogą one spowodować, różnią się pomiędzy głosowaniem elektronicznym w lokalach wyborczych a głosowaniem przez internet. Główne problemy rozwiązań

DRE to ich brak przejrzystości i odporności na niektóre ataki. Typowe urządzenie DRE jest przecież tajemniczą elektroniczną skrzynią, która przyjmuje głosy obywateli, a po zakończeniu wyborów ogłasza ich wynik. Nie ma możliwości zaobserwowania rejestrowania głosów i ich zliczania, nie ma możliwości ponownego przeliczenia głosów - wynik oznajmiony przez maszynę jest ostateczny. Ewidentnie jest to sprzeczne z założeniem, że wybory powinny być przejrzyste.

Można wymienić kilka dokładnych problemów urządzeń DRE. Skąd wyborca może mieć pewność, że oprogramowanie dostarczone przez producenta działa tak, jak on sam zapewnia? Jednym z rozwiązań tego problemu jest upublicznienie kodu źródłowego systemu działającego na maszynach, co prywatne przedsiębiorstwa czynią niezbyt chętnie. Ale nawet po takiej publikacji, skąd wyborca może mieć pewność, że to właśnie ten dostępny kod został zainstalowany na maszynie, która znajduje się przed nim? Możliwości są dwie: albo zaufa dostawcy maszyn oraz pracownikom komisji wyborczej (którzy mogą przecież być członkami mniejszego lub większego spisku) albo w jakiś sposób sprawdzi to za pomocą sum kontrolnych, ale wtedy musiałby albo uzyskać dostęp do samej maszyny (co mogłoby dać mu możliwość wgrania własnego wirusa), albo zaufać komuś, że on zrobił to za niego. Ponieważ dawanie każdemu wyborcy dostępu do maszyny nie jest dobrym rozwiązaniem, jedyną opcją jest zaufanie producentowi, czyli utrata przejrzystości [**?**].

Zakładając jednak, że żaden spisek nie miał miejsca, nadal nie możemy być pewni, że komputer wyborczy poprawnie policzy wszystkie oddane na nim głosy. Jak pokazują przykłady z podrozdziału **??**. wiele rozwiązań DRE dostępnych obecnie na rynku podatnych jest na ataki przestępców. W przypadku gorzej zabezpieczonych systemów można dokonać ataku nie znajdując się nawet w lokalu wyborczym i nie mając dostępu do samych maszyn. Natomiast w przypadku lepiej zabezpieczonych, wystarczy znaleźć się sam na sam z komputerem wyborczym chociażby na minutę. Uzyskawszy taki dostęp, możemy zarazić maszynę wirusem, który będzie w stanie rozprzestrzenić się na inne, nawet pomimo braku połączeń sieciowych między nimi. Opisanym atakom prawdopodobnie dałoby się zapobiec stosując kryptograficzne zabezpieczenia, podpisy i weryfikacje, ale wtedy natrafiamy na dwa kolejne problemy. Po pierwsze implementacja kryptografii może być błędna, przez co atakującym uda się jednak znaleźć furtkę do maszyn. Po drugie, z każdym kolejnym zabezpieczeniem mniej i mniej ludzi będzie w stanie pojąć działanie takiego systemu, dlatego będą oni ponownie zmuszeni zaufać producentowi, co znowu powoduje, że wybory przestają być przejrzyste.

Ponadto istnieje jeszcze jedna droga ataku, podobna do metody obranej przez naukowców z Michigan w ataku opisanym w podrozdziale **??**. Atakujący zamiast celować w gotowe urządzenia wyborcze, może skierować swoje starania na proces tworzenia oprogramowania i włamać się na serwery producenta instalując w kodzie swoją furtkę, którą wykorzysta dopiero w dniu wyborów. Bezpieczeństwo wyborów narodowych zależy wtedy również od zabezpieczeń wewnętrznych producenta, nad którymi obywatele nie mają kontroli.

4.2 I-głosowanie

Głosowanie internetowe jest zdecydowanie bardziej niebezpiecznie niż wykorzystanie systemów DRE z powodu kilku czynników:

- liczba możliwych ataków jest nieporównywalnie większa niż w przypadku lokalnych maszyn,
- łańcuch komunikacyjny pomiędzy wyborcą a centralnym serwerem jest niezwykle długi, a każde jego ogniwo podatne na działanie przestępców,
- o atak na taki system może pokusić się każdy, od samotnego hakera fanatyka, aż po agencję wywiadowczą obcego rządu,

- atakujący może przeprowadzić wszystkie działania prosto ze swojego domu, znajdując się poza jurysdykcją państwa, które atakuje,

- jeden skuteczny atak może wpłynąć nie tylko na głosy tysięcy osób, a na wynik całych wyborów.

Wybory internetowe są formą wyborów elektronicznych, przez co pozostają podatne na wszystkie ataki, na które podatne są systemy DRE [**?**]. Trzeba zatem przekonać ludzi, że oprogramowanie centralnych serwerów działa dokładnie tak, jak powinno, i nie jest efektem spisku programistów. Trzeba serwery zabezpieczyć tak, by atakujący nie był w stanie w żaden sposób wgrać na nie złośliwego oprogramowania. Trzeba również zaufać dostawcy systemu, że jego serwery były odpowiednio zabezpieczone i atakującemu nie udało się stworzyć furtki w oprogramowaniu. Warto zaznaczyć, że jest to jeden z problemów, które wykazała analiza estońskiego systemu wyborów interentowych. Opisane w rodziale 3.

Zabezpieczenie serwerów centralnych to jednak dopiero początek wymogów, jakie powinien spełniać system wyborów internetowych. Dodatkowym problemem, z którym nie muszą radzić sobie systemy DRE jest autoryzacja wyborcy i upewnienie się, że nie oddał on dwóch głosów w jednych wyborach. Jeśli uda się jakoś zweryfikować tożsamość obywatela przed głosowaniem, to trzeba zapewnić mu anonimowość głosu - tak, by nikt nie wiedział jak on zagłosował, ale też tak, by on sam nie mógł tego udowodnić. Ponownie - nawet gdyby za pomocą silnej kryptografii udało się odpowiednio zabezpieczyć serwery i prywatność głosów, to cały system powinien być zrozumiały dla większości wyborców, bo w przeciwnym wypadku nie będzie przejrzysty.

Ponadto zapewniając prawidłową, nienaruszalną przez spisek, ani działalność hakerów, pracę serwera i możliwość zweryfikowania tożsamości wyborcy, wciąż pozostaje kwestia transmisji danych pomiędzy serwerem a klientem oraz wykonania pewnych operacji po stornie wyborcy. Nad żadnym z tych etapów system wyborczy nie ma praktycznie żadnej kontroli, a oba z nich mogą oczywiście znaleźć się na celowniku hakerów - transmisja danych przez sieć może zostać zakłócona na czas trwania wyborów np. poprzez atak typu *denial of service* [**?**]. Przy takim zakłóceniu niemożliwe byłoby odpowiednie rejestrowanie głosów. Natomiast sposobów zaatakowania klienta jest mnóstwo, a jeden z nich został zaprezentowany przez naukowców z Michigan podczas analizy sytemu estońskiego (opisane wyżej).

Największym zagrożeniem wspólnym dla *e-wyborów* i *i-wyborów* jest jednak niemożność przeprowadzenia jakiejkolwiek kontroli. W dowolnym elektronicznym systemie wyborczym powinniśmy mieć możliwość ręcznego wykrycia ewentualnego spisku, lub ataku hakerskiego, i skontrolowania jego skutków, ponieważ całkowite zabezpieczenie oprogramowania przed lukami i błędami po prostu nie jest możliwe [**?**]. Niestety w przypadku głosowania czysto elektronicznego nie jest to możliwe, bo jedynym śladem po głosach wyborców są liczniki w wewnętrznej pamięci komputerów podatnych na dokładnie te same spiski i ataki.

Należy zaznaczyć, że niektóre ze wspomnianych ataków mogłyby zostać przeprowadzone przez osobę pracującą w pojedynkę. Gdyby się powiodły, mogłyby wpłynąć na wyniki całych wyborów, a wykrycie nieprawidłowości i odwrócenie skutków przestępstwa byłoby w praktyce niemożliwe z powodu niemożności przeprowadzenia kontroli. Dodatkowo, przy głosowaniu internetowym, ewentualne ściganie atakującego mogłoby się okazać niemożliwe, ponieważ wszystkie operacje byłby on w stanie przeprowadzić ze swojego domu niekoniecznie znajdującego się pod jurysdykcją atakowanego państwa (co dodatkowo zachęca go do bardziej ryzykownych działań) [**?**].

5 Bezpieczniejsze metody

Czy w takim razie niemożliwe jest przeprowadzenie elektronicznych wyborów bezpiecznie? Jest to trudne pytanie, na które świat prawdopodobnie nie zna jeszcze odpowiedzi, ale pewne jest, że można przeprowadzić je znacznie bezpieczniej niż przy użyciu samych systemów DRE. W tym celu należy wykorzystać tzw. technologię VVPAT (*voter-verified paper audit trail*). Rozwiązanie to jest uzupełnieniem systemów DRE, dodającym jedno niezwykle istotne zabezpieczenie - po zarejestrowaniu głosu wyborcy, maszyna drukuje potwierdzenie, na którym wyborca może sprawdzić, czy zachowany głos zgadza się z jego wyborem. Następnie wyborca zobowiązany jest wrzucić otrzymany wydruk do urny w lokalu wyborczym. Dzięki zastosowaniu tej technologii można wyeliminować najpoważniejszy zarzut wobec elektronicznych systemów wyborczych - niemożność przeprowadzenia kontroli. Jeśli zachowamy potwierdzone przez wyborców, anonimowe wydruki, to wciąż możemy korzystać z szybkiego przeliczania pełnych wyników przy użyciu komputerów, jednak jesteśmy w stanie przeprowadzić ręczną kontrolę poprawności działania systemów na odpowiednio dobranych próbkach statystycznych, co pozwoli wykryć i ewentualnie poprawić wszystkie ataki i spiski [**?**]. Należy oczywiście pamiętać o odpowiednim zabezpieczeniu maszyn DRE - wydruki papierowe powinny być tylko formą kontroli, nie podstawowym zabezpieczeniem.

Korzystając z tego rozwiązania możemy znacząco przyspieszyć zliczanie wyników przy zachowaniu poziomu bezpieczeństwa porównywalnego z głosowaniem papierowym. Ta technologia ma jednak swoje wady. Po pierwsze, w całości zależy ona na potwierdzaniu wydruków przez wyborców - jeśli obywatele będą wrzucać wydruki do urn bez weryfikacji, lub - co gorsza - nie wrzucać ich wcale, to cały system jest bezwartościowy. Po drugie, zastosowanie tego rozwiązania wymaga dużego nakładu finansowego, prawdopodobnie nie mniejszego niż głosowanie tradycyjne (nie jest to potwierdzone analizami) oraz zwiększa ryzyko awarii sprzętowej i generuje problemy związane właściwą konserwację tych urządzeń.

Zupełnie inne niż niemal wszystkie powszechnie wykorzystywane rozwiązania są protokoły oparte na całkowitej przejrzystości wyników, zachowujące tym samym prywatność głosów. Wykorzystują one skanowanie optyczne i kryptografię, a w efekcie są w stanie przyspieszyć zliczanie głosów, jednocześnie zapewniając większe bezpieczeństwo niż standardowe wybory papierowe. Kluczem do tego bezpieczeństwa jest w ich przypadku umożliwienie każdemu zweryfikowania, czy jego głos został poprawnie zarejestrowany (nie dając mu jednak możliwości dowiedzenia na kogo głosował), oraz udostępnienie bazy głosów tak, by każdy mógł sprawdzić, czy zliczanie zostało przeprowadzone poprawnie. Przykładem takiego systemu jest opracowany przez Petera Ryana na Uniwersytecie Luksemburskim Prêt à Voter [**?**]. Jednym z wyzwań, z którymi muszą poradzić sobie twórcy tych rozwiązań jest przekonanie wyborców, że silna kryptografia zastosowana przez nich rzeczywiście działa, a innym przetestowanie go w warunkach prawdziwych wyborów.

6 Podsumowanie

Jak pisze Bruce Schneier, problem z elektronicznym głosowaniem polega na tym, że technologia dodaje kolejnych kroków do wystarczająco już złożonego procesu wyborczego. Kolejne kroki oznaczają zwiększenie szansy na wystąpienie błędu, bo żadna technologia tworzona przez człowieka nie jest idealna [**?**]. Z tego powodu należy być niezwykle ostrożnym przy rozważaniu bezpieczeństwa systemów do elektronicznego głosowania. Istotne jest też by rozpatrywać ten problem w kategorii bezpieczeństwa narodowego, znacznie ważniejszego i trudniejszego do zapewnienia niż bezpieczeństwo komercyjne. Ponadto - inaczej niż w bezpieczeństwie komercyjnym - w razie udanego spisku lub ataku, jego skutki mogą okazać się bardzo trudne do odwrócenia, bo ludzie, którzy ten spisek przeprowadzili, mogą już być u władzy.

Mając na uwadze powyższe względy, uważam, że zwykłe systemy DRE nie są wystarczająco bezpieczne by być wykorzystywane w skali wyborów narodowych, a rozwiązania DRE z właściwym użyciem VVPAT zapewniają odpowiedni poziom bezpieczeństwa, jednak uch użycie wydaje się być nieuzasadnione. Są skomplikowane, kosztowne, trudne do zastosowania i eksploatowania oraz niedostatecznie przetestowane, a ich zalety są niewspółmierne z wadami. W kategorii rozwiązań używanych w lokalach wyborczych bardzo interesujące wydają się rozwiązania kryptograficzne w stylu Prêt à Voter - być może jest to dobry sposób na poprawienie bezpieczeństwa procesu wyborczego.

Natomiast w dziedzinie wyborów internetowych, zważając na opinie i analizy ekspertów, skłonny jestem stwierdzić, że wykorzystywanie obecnej technologii na wielką skalę jest przedwczesne. Być może z pomocą znowu przyjdzie nam kryptografia, jednak opracowanie odpowiedniej metody - jeśli w ogóle możliwe - z pewnością zajmie lata, a nawet kryptografia nie będzie mogła poradzić sobie z atakami na dostępność sieci i komputer klienta.

Literatura

[1] Jeremy Epstein. *Decertifying the worst voting machine in the US.* Freedom To Tinker, 2015. https://freedom-to-tinker.com/2015/04/15/decertifying-the-worst-voting-machine-in-the-us/

[2] *OSCE findings on Estonian e-voting.* EDRi, 2011. https://edri.org/edrigramnumber9-11e-voting-osce-estonia

[3] Mary Bellis. *The History of Voting Machines.* http://inventors.about.com/library/weekly/aa111300b.htm

[4] *Electronic voting in Estonia.* Wikipedia. https://en.wikipedia.org/wiki/Electronic_voting_in_Estonia

[5] *Electronic voting by country.* Wikipedia. https://en.wikipedia.org/wiki/Electronic_voting_by_country

[6] David Bismark. *Verifiable Electronic Voting.* https://evoting.bismark.se/verifiable-electronic-voting

[7] Douglas W. Jones. *A Brief Illustrated History of Voting.* The University of Iowa, 2003. http://homepage.cs.uiowa.edu/~jones/voting/pictures

[8] David Jefferson. *What About Email and Fax?.* Verified Voting. https://www.verifiedvoting.org/resources/internet-voting/email-fax

[9] Bruce Schneier. *What's Wrong With Electronic Voting Machines?.* Schneier on Security, 2004. https://www.schneier.com/essays/archives/2004/11/whats_wrong_with_ele.html

[10] Rop Gonggrijp, Willem-Jan Hengeveld. *Nedap/Groenendaal ES3B voting computer.* Stichting "Wij vertrouwen stemcomputers niet", 2006. http://wijvertrouwenstemcomputersniet.nl/images/9/91/Es3b-en.pdf

[11] Ariel J. Feldman, J. Alex Halderman, Edward W. Felten. *Security Analysis of the Diebold AccuVote-TS Voting Machine.* Princeton University, 2006. https://www.usenix.org/legacy/events/evt07/tech/full_papers/feldman/feldman_html/index.html

[12] Drew Springall, Travis Finkenauer, Zakir Durumeric, Jason Kitcat, Harri Hursti, Margaret MacAlpine, J. Alex Halderman. *Security Analysis of the Estonian Internet Voting System*. University of Michigan, Open Rights Group, 2014. https://jhalderm.com/pub/papers/ivoting-ccs14.pdf

[13] David Jefferson. *Electronic and Internet Voting*. Lawrence Livermore National Laboratory, 2011. https://www.youtube.com/watch?v=_GjmRwfkRXY&t=2688s

[14] Barbara Simons. *California: The Top to Bottom Review*. VoteTrustUSA, 2007. http://www.votetrustusa.org/index.php?option=com_content&task=view&id=2554&Itemid=113

[15] Hagai Bar-El. *Why secure e-voting is so hard to get*. 2015. https://www.hbarel.com/analysis/cyber/secure-e-voting-is-hard-to-get