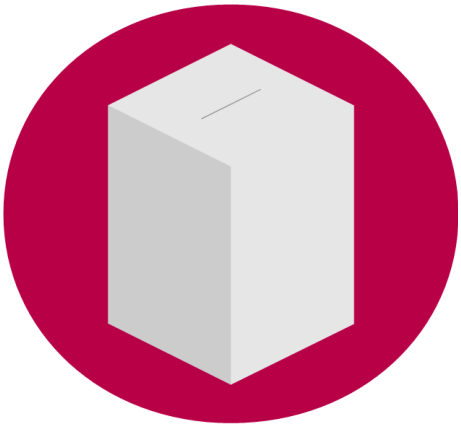


System wyborów internetowych

Tomasz Krutak
Maciej Ziarkowski

Instytut Informatyki UJ, Bezpieczeństwo Systemów Komputerowych, 2012/2013

Niniejszy dokument opisuje w skrócie strukturę i sposób działania stworzonego przez nas systemu głosowania internetowego. Po dokładny opis użytych algorytmów i protokołów odsyłamy do pierwszej części naszego projektu, będącej tutorialem przedstawiającym w szerszym zakresie zagadnienie wyborów elektronicznych (wraz z niezbędnymi podstawami kryptograficznymi i matematycznymi).

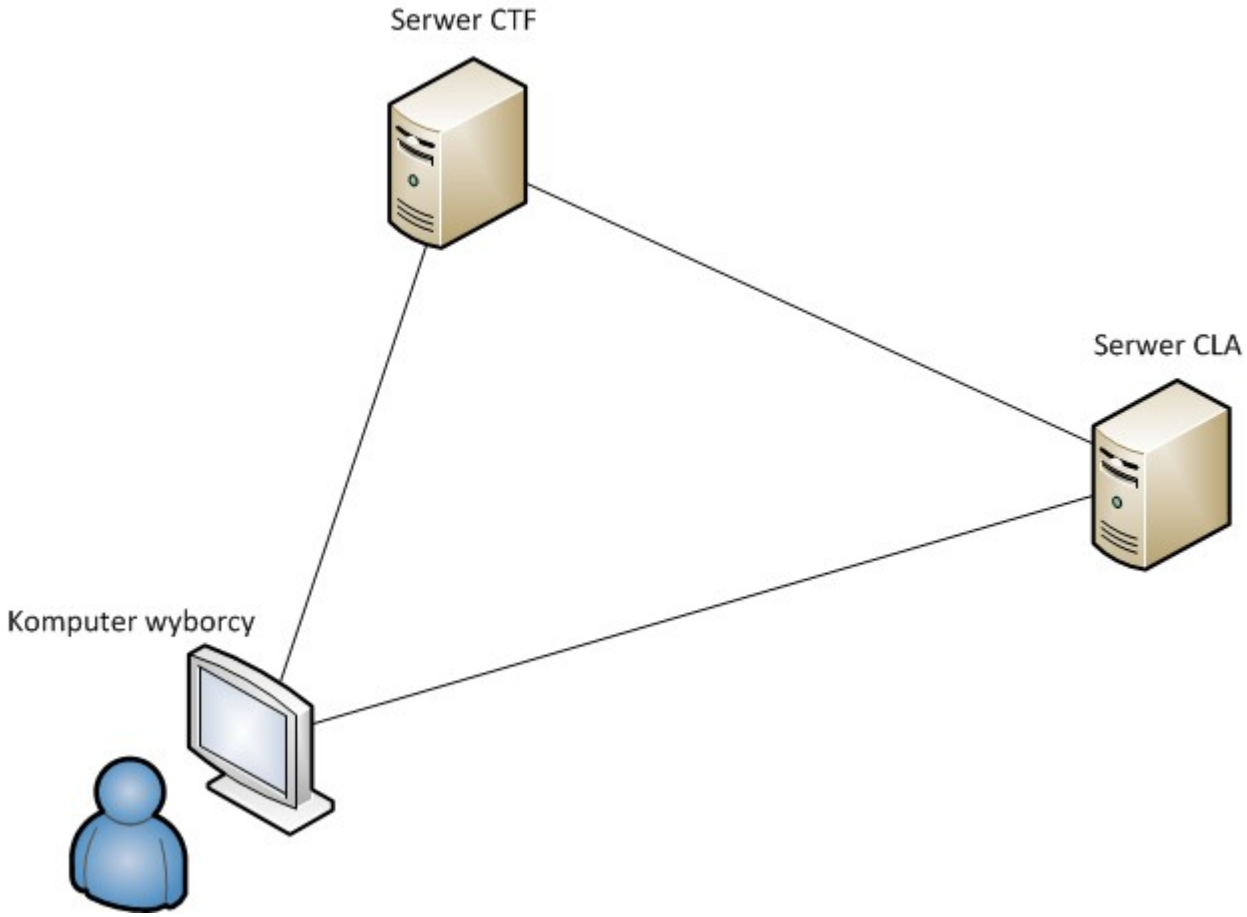
System został oparty o schemat głosowania z użyciem dwóch jednostek centralnych, opisany w książce *Applied Cryptography* autorstwa Bruce'a Schneiera.

Przy pomocy standardowych algorytmów kryptograficznych, stosunkowo łatwo zapewnić dzisiaj tajność przesyłanych informacji. W przypadku wyborów internetowych pojawiają się jednak dodatkowe wymagania dotyczące anonimowości głosującego, przede wszystkim - aby oficjalne instytucje zajmujące się odbieraniem i zliczaniem głosów nie były w stanie połączyć tożsamości głosującego z treścią oddanego przez niego głosu. Wiąże się to z pojęciem wolności wyznawanych poglądów, ma zapobiec między innymi przekładaniu się oddanego głosu na późniejszą sytuację

życiową głosującego (kandydat zwycięskiej partii, który odkryłby, kto głosował na jego przeciwnika, mógłby bowiem dyskryminować te osoby sprawując władzę).

W wielu schematach głosowania internetowego (np. w głosowaniu przy użyciu ślepych podpisów czy przy użyciu funkcji homomorficznych) wykorzystuje się prawa matematyki w celu osiągnięcia anonimowości głosujących. W schemacie z dwoma jednostkami centralnymi polega się jednak przede wszystkim na logicznym i fizycznym rozdzieleniu komisji wyborczej na dwie jednostki - pierwszą, zajmującą się weryfikacją tożsamości wyborców (CLA - z ang. *Central Legitimization Agency*) i drugą, zajmującą się zbieraniem anonimowych głosów od zweryfikowanych wyborców (CTF - z ang. *Central Tallying Facility*).

Poniżej znajduje się diagram przedstawiający strukturę systemu:



W systemie zawierają się trzy aplikacje - serwer CLA, serwer CTF oraz aplikacja kliencka (na tym poziomie rozwoju są to aplikacje konsolowe), które

realizują przedstawiony model wyborów.
Do zapewnienia bezpieczeństwa połączenia między stronami zostało użyte połączenie SSL, które używa publicznych certyfikatów, aby wygenerować i przesłać symetryczny klucz sesyjny. Jest on później używany do szyfrowania wymienianych informacji.
UWAGA: niniejszy system wymaga wydzielenia z wyborów dwóch faz - fazy zapisów na wybory, kiedy uprawnieni do głosowania obywatele uzyskują "numery walidacyjne", które pozwolą im później uwierzytelnić swój głos. Dopiero, gdy faza zapisów się kończy - rozpoczyna się faza głosowania i można wtedy wysyłać swoje głosy. Nikt nie może się już wtedy zapisywać na wybory. Rozpoczęcie i zakończenie poszczególnych faz jest przeprowadzane ręcznie przez administratorów systemu.
Uwierzytelnianie wyborców opiera się na tajnym haśle, które musi być przesłane drogą nieelektroniczną (np. pocztą) wcześniej. Może być to uniwersalne hasło, które obywatel posiada w różnych celach - ogólnie rzecz biorąc, niezbędny jest tutaj jakiś typ państwowej infrastruktury, która umożliwia elektroniczne potwierdzenie tożsamości obywatela tylko przez niego samego (w zaawansowanych technologicznie systemach mogłyby to być np. dane biometryczne, jednak takie rozwiązanie wymagałoby posiadania specjalnego skanera przez każdego, kto chciałby głosować przez internet).

Działanie systemu wygląda następująco:

I. Faza zapisów
    1. Wyborca włącza aplikację kliencką i łączy się z serwerem CLA
    2. Serwer prosi wyborcę o podanie numeru PESEL i specjalnego hasła
    3. Jeżeli dane są poprawne, serwer wysyła wyborcy unikalny numer walidacyjny (wyborca musi go zapisać w bezpiecznym miejscu)

Faza zapisów kończy się po określonym czasie. Wtedy też serwer CLA tworzy listę numerów walidacyjnych. Jest ona przenoszona na serwer CTF. W celach bezpieczeństwa można ją przenieść na fizycznych nośnikach i w

postaci chronionej hasłem.

II. Faza głosowania

1. Wyborca ponownie włącza aplikację kliencką i łączy się z serwerem CTF
2. Wyborca prosi o listę dostępnych kandydatów i otrzymuje ją w odpowiedzi (każdy może poprosić o listę kandydatów)
3. Wyborca dokonuje wyboru (można oddać głos nieważny), a następnie jest proszony o wprowadzenie numeru walidacyjnego.
4. Aplikacja kliencka generuje numer identyfikacyjny głosu i wysyła wiadomość w formacie:
   numer_identyfikacyjny | numer_walidacyjny | wybrany_kandydat
5. Serwer CTF sprawdza, czy podany numer walidacyjny znajduje się na liście otrzymanej od CLA oraz czy nie został wcześniej zużyty. Numer identyfikacyjny głosu powinien być globalnie unikatowy. Jeżeli już wcześniej ktoś oznaczył swój głos takim numerem, serwer powiadamia o tym aplikację kliencką, ta zaś generuje nowy numer i ponownie przesyła wiadomość (aż do skutku).
6. Aplikacja kliencka wyświetla wyborcy użyty ostatecznie numer identyfikacyjny głosu (wyborca powinien go zapisać)

Gdy faza głosowania się kończy, serwer CTF tworzy plik zawierający wyniki wyborów. W pliku tym znajdują się też listy wszystkich numerów identyfikacyjnych, które oznaczały głosy oddane na poszczególnych kandydatów. W niniejszym systemie plik ten sformatowany jest w języku znaczników HTML, aby łatwo go było umieścić na stronie internetowej.

Zauważmy, że w systemie pojawiają się trzy ważne elementy: tożsamość wyborcy (PESEL+hasło), numer walidacyjny wyborcy oraz numer identyfikacyjny głosu. To rozwiązanie zapewnia tajność głosowania. CLA zna powiązanie między tożsamością a numerem walidacyjnym, ale nie zna głosu wyborcy. CTF może uwierzytelnić użytkownika dzięki liście numerów walidacyjnych od CLA, ale nie zna powiązania między tożsamością

użytkownika a numerem walidacyjnym, a zatem także i głosem danego wyborcy. Tylko wyborca wie, jak zagłosował. Co więcej, dzięki znajomości numeru identyfikacyjnego własnego głosu, może w wynikach wyborów sprawdzić, czy jego głos został poprawnie podliczony.
Oczywiście w wypadku zmowy między CLA i CTF, mogłoby dojść do ujawnienia połączeń między wyborcami a ich głosami. Prawdopodobieństwo takiego zdarzenia można jednak ograniczyć przez wprowadzenie odpowiedniego systemu kontroli.

Dalsze kierunki rozwoju aplikacji:

1. Uwolnienie kodu dla społeczności Open Source za pośrednictwem platformy google code. Tymczasowo źródła dostępne są pod urlem https://internetvotingsystem.googlecode.com/svn/trunk/
2. Chcielibyśmy aby tematem zainteresowało się więcej osób gdyż implementacja jest jak najbardziej życiowa – podobna używana jest w Estonii. Celem jest taki rozwój platformy aby można ją wdrożyć we względnie różnych warunkach – tzn aby nie była powiązana na stałe z jedną infrastrukturą ale aby raczej była na tyle uniwersalna żeby niewielkim nakładem pracy można ją było dostosować dla potencjalnie wielu krajów i komisji wyborczych.
3. Nie wykluczamy, że będziemy się starali pozyskać na jej rozwój środki z Unii Europejskiej, dzięki czemu moglibyśmy podjąć się dalszego rozwoju tego dzieła.