WYDZIAŁ ELEKTRONIKI
I TECHNIK INFORMACYJNYCH

Temat projektu: *Elektroniczne głosowanie*

Przedmiot: Protokoły kryptograficzne

Skład grupy projektowej:

- *Marcin Skwarek*
- *Krystian Powójski*
- *Anh Tuan Nguyen*

Prowadzący projekt: *mgr inż. Marcin Tunia*

Semestr: *14Z*

1. Wprowadzenie – opis projektu

Projekt ma na celu zaimplementowanie systemy umożliwiającego przeprowadzenie e-głosowania. Aplikacja spełnia podstawowe wymagania bezpieczeństwa i gwarancji poprawności przebiegu głosowania w tym celu wykorzystany zostanie ślepy podpis. Realizując projekt bazujemy na pomyśle zatytułowanym *„Scratch, Click & Vote: E2E voting over the Internet", autorzy Mirosław Kutyłowski, Filip Zagórski, Institute of Mathematics and Computer Science Wrocław University of Technology.*

Aplikacja składa się z czterech modułów (podprogramów):

- Election Authority (ozn EA) - odpowiada za przygotowanie list kandydatów (każda z list charakteryzuje się unikatową permutacją, wymieszaniem, kandydatów). Ponadto dba o liczenie głosów i zapewnienie głosującemu specjalny token przy pomocy którego może sprawdzić czy jego głos nie został zmieniony.
- Proxy - odpowiada za przygotowanie kart do głosowania oraz pośredniczy w przekazywaniu głosu między Voter'em a Election Authority
- Voter - odpowiada za prezentację danych otrzymanych od EA (lista kandydatów) oraz Proxy (karta do głosowania) oraz oddanie głosy przez wyborcę.
- Auditor - pełni rolę nadzorcy, sprawdza czy w toku głosowania nie doszło do fałszerstwa.

2. Opracowanie teoretyczne

Projekt zostanie opracowany przy wykorzystaniu języka C# rozszerzonego o bibliotekę kryptograficzną B*ouncy Castle* przy wykorzystaniu środowiska Microsoft Visual Studio 2010. Całość będzie składać się z oddzielnych 4 aplikacji okienkowych i wykorzystywać architekturę klient-serwer TCP do wzajemnej komunikacji.

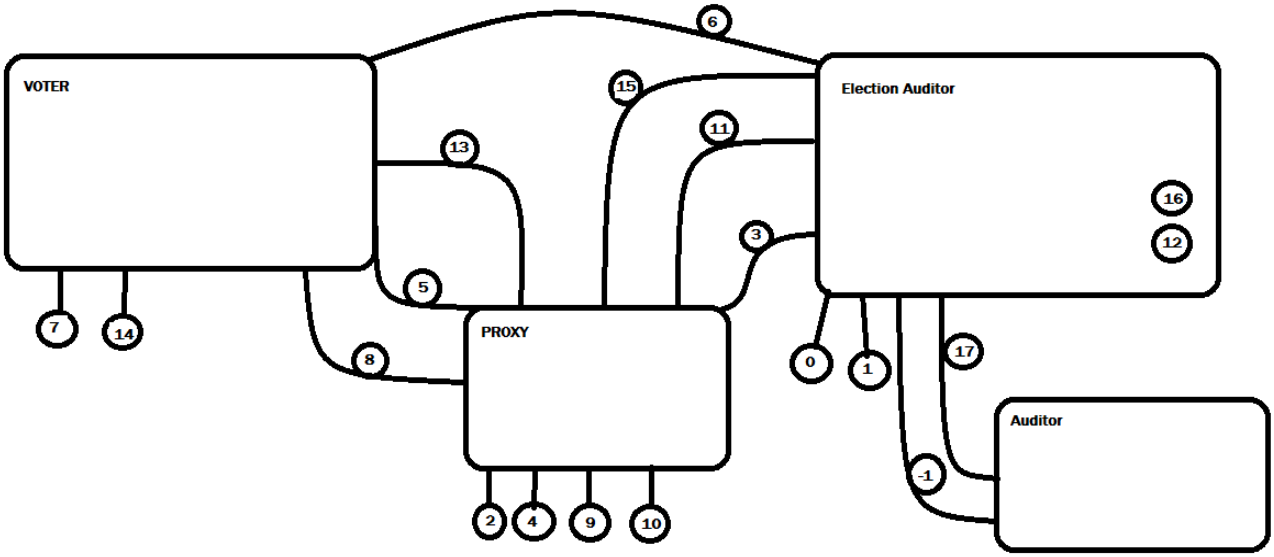
Wykorzystane rozwiązania z dziedziny kryptografii:

- Bitcommitment, pl zobowiązanie bitowe – jest to schemat pozwalający jednej stronie udowodnić niezmienność pewnego sekretu (danych, informacji) bez potrzeby ujawniania. Stron zobowiązująca nie może zmienić podanej wartości po

dokonaniu zobowiązania. Po ujawnieniu sekretu strona przyjmująca zobowiązanie ma możliwość wykrycia ewentualnych nieprawidłowości wynikających z działania drugiej strony.

- Blind signature, pl ślepy podpis - rodzaj podpisu cyfrowego w którym zawartość wiadomości jest zaślepiana przed podpisaniem. Ślepy podpis może być potem zweryfikowany z wiadomością. Są na ogół wykorzystywane w protokołach opartych na prywatności, w których autor wiadomości i podpisujący to różne osoby. Wykorzystywany jest w celu zapewnienia uczciwości jednej ze stron przy jednoczesnym zachowaniu tajności informacji.

3. Koncepcja rozwiązania problemu



SL – numer identyfikujący listę kandydatów

SR – numer karty do głosowania

π – permutacja listy kandydatów

tokeny – służą do podpisania kolumn w macierzy głosów

Opis schematu:

-1 : Przed rozpoczęciem głosowanie EA przesyła listę SL i bitcommitment od π do Auditora

0 : EA wczytuje standardową listę kandydatów

1: EA generuje dla każdej karty z osobna: SL, π oraz tokeny (A,B,C,D)

2: Proxy generuje dla każdej karty do głosowania SR

3: EA przekazuje do Proxy: SL oraz tokeny

4: Proxy paruje SL oraz odpowiadający mu SR

5: Proxy przekazuje pary SL i SR do Votera

6: Voter pobiera kartę z kandydatami na podstawie numeru SL

7: Voter dokonuje głosu

8: Głos (jako zero-jedynkowa tablica dwuwymiarowa) przekazywany jest do Proxy

9: Proxy przekształca głos na tzw. „ballot matrix", czyli zaznacza wszystkie te pola "nie", które nie zostały kliknięte przez Voter

10: Proxy zaślepia „ballot matrix" (para kluczy generowana losowo)

11: Proxy przesyła: SL, tokeny oraz zaślepiony „ballot matrix"

12: EA podpisuje zaślepioną „ballot matrix" następnie zwraca SL, tokeny i zaślepioną, podpisaną ballot matrix

13: Proxy wysyła podpisaną całość do Votera

14: Voter wybiera kolumnę którą chce stosować jako potwierdzenie - token, kolumna, podpis od EA

15: Proxy przesyła odślepioną, podpisaną „ballot matrix" i odpowiadający jej SL do Election Auditora

16: EA odpermutowuje i liczy głosy

17: Auditor dostaje odślepione π od EA i dokonuje sprawdzenie czy nie uległo ono zmianie

4. Bibliografia

- *Wykłady z przedmotu Protokoły Kryptograficzne autorstwa prof. dr hab. inż Zbigniewa Kotulskiego,*
- *Scratch, Click & Vote: E2E voting over the Internet Mirosław Kutyłowski, Filip Zagórski*
- *http://www.cs.berkeley.edu/~daw/teaching/cs276-s04/19a.ps*
- *http://wwwf.imperial.ac.uk/~rbellovi/writings/chaum.pdf*
- *http://www.bouncycastle.org/*