

# Dlaczego jeszcze nie głosujemy elektronicznie?

Jakub Zadrożny

Instytut Informatyki UWr.

3 stycznia 2017

# Czy to w ogóle potrzebne?

# Czy to w ogóle potrzebne?

- Informatyka jest wszędzie: urzędy, szkoły, uniwersytety, przedsiębiorstwa, maszyny.

# Czy to w ogóle potrzebne?

- Informatyka jest wszędzie: urzędy, szkoły, uniwersytety, przedsiębiorstwa, maszyny.
- Tylko nie na wyborach (przynajmniej nie wszędzie).

# Czy to w ogóle potrzebne?

- Informatyka jest wszędzie: urzędy, szkoły, uniwersytety, przedsiębiorstwa, maszyny.
- Tylko nie na wyborach (przynajmniej nie wszędzie).
- Co moglibyśmy zyskać?

# Czy to w ogóle potrzebne?

- Informatyka jest wszędzie: urzędy, szkoły, uniwersytety, przedsiębiorstwa, maszyny.
- Tylko nie na wyborach (przynajmniej nie wszędzie).
- Co moglibyśmy zyskać?
  - Przyspieszyć liczenie wyników.

# Czy to w ogóle potrzebne?

- Informatyka jest wszędzie: urzędy, szkoły, uniwersytety, przedsiębiorstwa, maszyny.
- Tylko nie na wyborach (przynajmniej nie wszędzie).
- Co moglibyśmy zyskać?
  - Przyspieszyć liczenie wyników.
  - Wyeliminować ludzkie błędy (przecież komputery się nie mylą).

# Czy to w ogóle potrzebne?

- Informatyka jest wszędzie: urzędy, szkoły, uniwersytety, przedsiębiorstwa, maszyny.
- Tylko nie na wyborach (przynajmniej nie wszędzie).
- Co moglibyśmy zyskać?
  - Przyspieszyć liczenie wyników.
  - Wyeliminować ludzkie błędy (przecież komputery się nie mylą).
  - Ułatwić głosowanie osobom niepełnosprawnym.

# Czy to w ogóle potrzebne?

- Informatyka jest wszędzie: urzędy, szkoły, uniwersytety, przedsiębiorstwa, maszyny.
- Tylko nie na wyborach (przynajmniej nie wszędzie).
- Co moglibyśmy zyskać?
  - Przyspieszyć liczenie wyników.
  - Wyeliminować ludzkie błędy (przecież komputery się nie mylą).
  - Ułatwić głosowanie osobom niepełnosprawnym.
  - Zmniejszyć koszty (np. pozbywając się ogromnych ilości papierowych głosów).

# Czy to w ogóle potrzebne?

- Informatyka jest wszędzie: urzędy, szkoły, uniwersytety, przedsiębiorstwa, maszyny.
- Tylko nie na wyborach (przynajmniej nie wszędzie).
- Co moglibyśmy zyskać?
  - Przyspieszyć liczenie wyników.
  - Wyeliminować ludzkie błędy (przecież komputery się nie mylą).
  - Ułatwić głosowanie osobom niepełnosprawnym.
  - Zmniejszyć koszty (np. pozbywając się ogromnych ilości papierowych głosów).
  - Poprawić bezpieczeństwo?

# Podział

Głosowanie elektroniczne można podzielić na dwie kategorie:

# Podział

Głosowanie elektroniczne można podzielić na dwie kategorie:

- e-voting - głosowanie odbywa się w lokalu wyborczym,

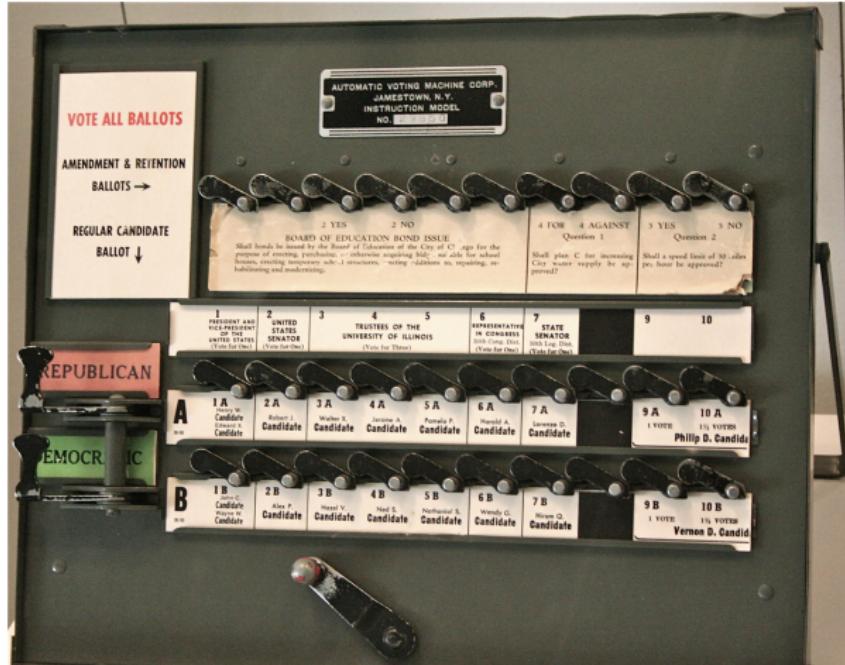
Głosowanie elektroniczne można podzielić na dwie kategorie:

- e-voting - głosowanie odbywa się w lokalu wyborczym,
- i-voting - głosowanie odbywa się przez internet.

# Lever machines

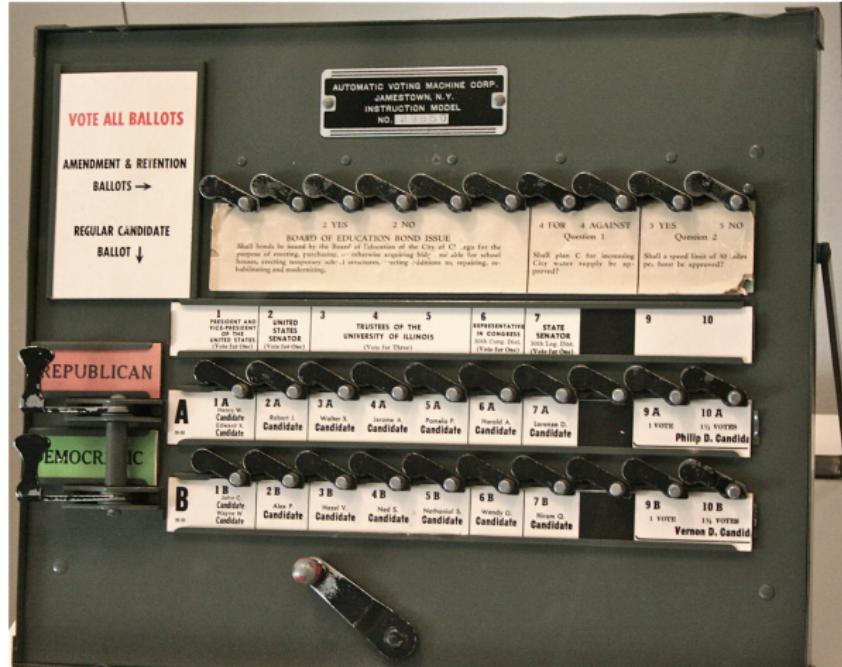


# Lever machines



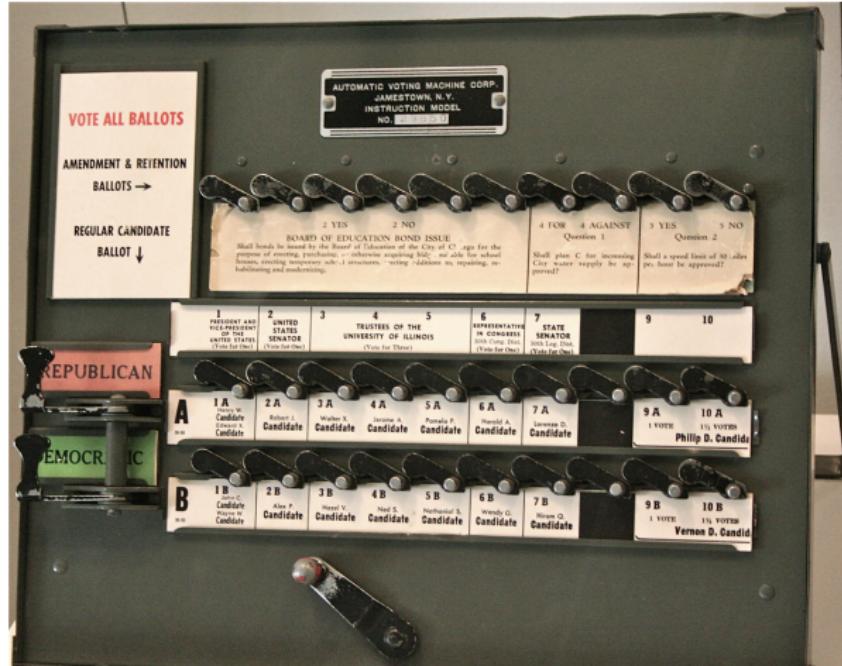
Zostały wprowadzone do użytku pod koniec XIX wieku i szybko zyskały popularność.

# Lever machines



Zostały wprowadzone do użytku pod koniec XIX wieku i szybko zyskały popularność. W 1960 ponad połowa głosów w USA była rejestrowana przy ich użyciu.

# Lever machines



Zostały wprowadzone do użytku pod koniec XIX wieku i szybko zyskały popularność. W 1960 ponad połowa głosów w USA była rejestrowana przy ich użyciu. Ze Stanów wycofano je dopiero w 2010.

# Skanowanie optyczne



# Skanowanie optyczne



W USA stosowane nieprzerwanie od 1964.

# Skanowanie optyczne



W USA stosowane nieprzerwanie od 1964. W 1996 wykorzystano je przy zliczaniu 60% głosów w Stanach.

# Direct Recording Electronics



**Ballot marking device**

*Demo device and receipt printer*

# Direct Recording Electronics



Na dużą skalę wykorzystywane m.in. w Brazylii (od 1996), Indiach (od 2003) oraz USA.

# Direct Recording Electronics

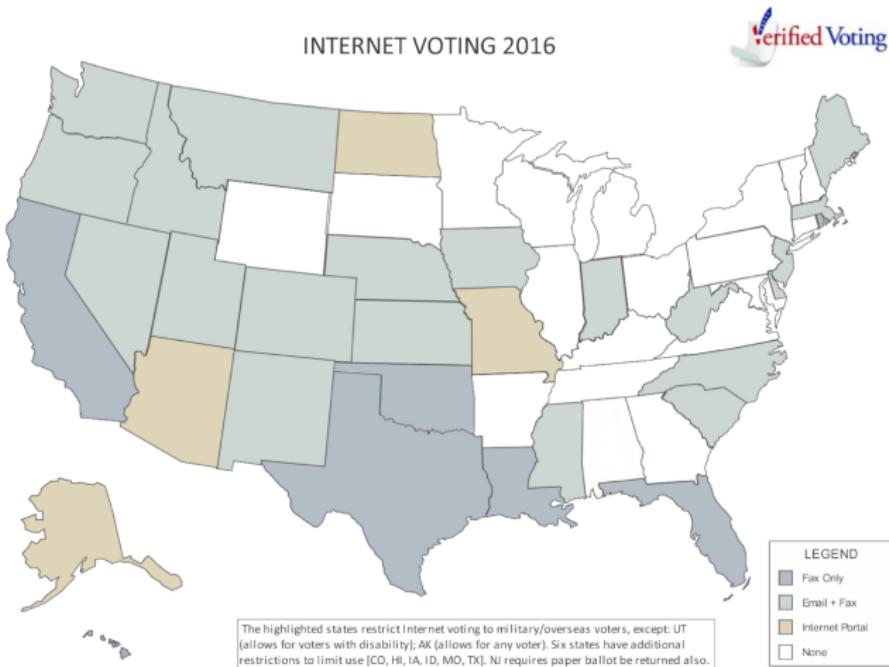


## Ballot marking device

*Demo device and receipt printer*

Na dużą skalę wykorzystywane m.in. w Brazylii (od 1996), Indiach (od 2003) oraz USA. Próbowano wprowadzić je w Holandii oraz Kazachstanie, ale na skutek protestów społecznych pomysł porzucono.

# Poczta elektroniczna i fax



Ta metoda dopuszczana jest m.in. w USA, Francji i Szwajcarii dla żołnierzy przebywających poza granicami kraju oraz ekspatriantów.

# Aplikacje webowe



# Aplikacje webowe



Wdrożenia takiego systemu na dużą skalę podjęła się tylko Estonia.

# Aplikacje webowe



Wdrożenia takiego systemu na dużą skalę podjęła się tylko Estonia. Po raz pierwszy przetestowano rozwiążanie w 2005. Wtedy głos przez internet oddało tylko 2% obywateli.

# Aplikacje webowe

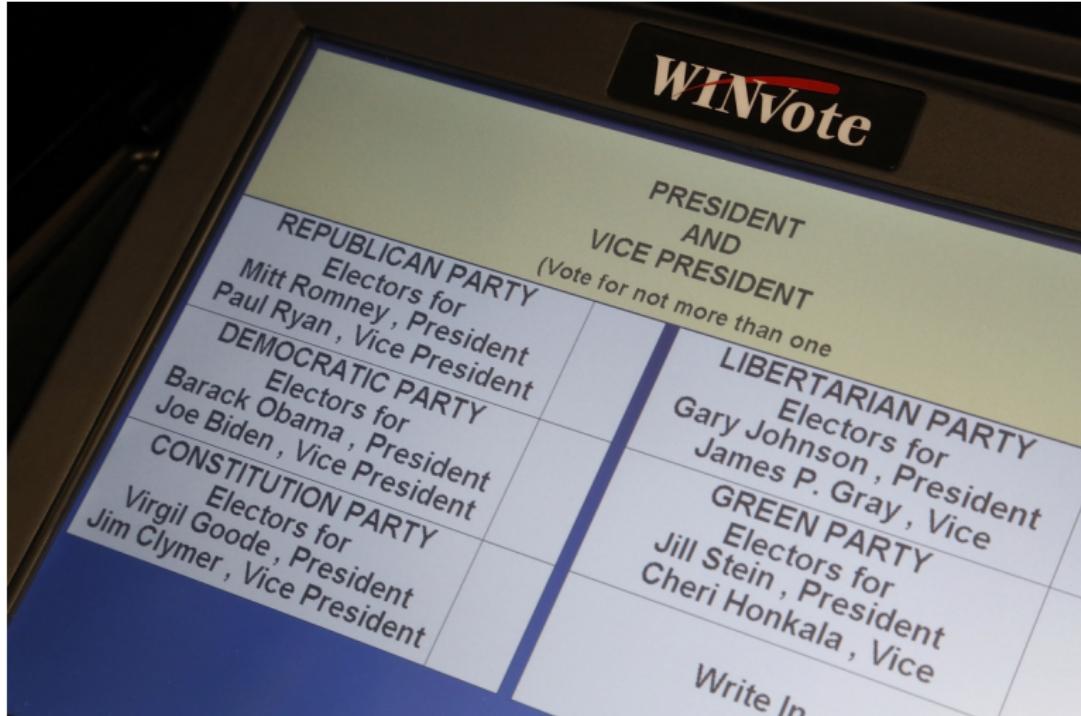


Wdrożenia takiego systemu na dużą skalę podjęła się tylko Estonia. Po raz pierwszy przetestowano rozwiążanie w 2005. Wtedy głos przez internet oddało tylko 2% obywateli. W 2014 i 2015 było to już ponad 30%.

# Udokumentowane ataki

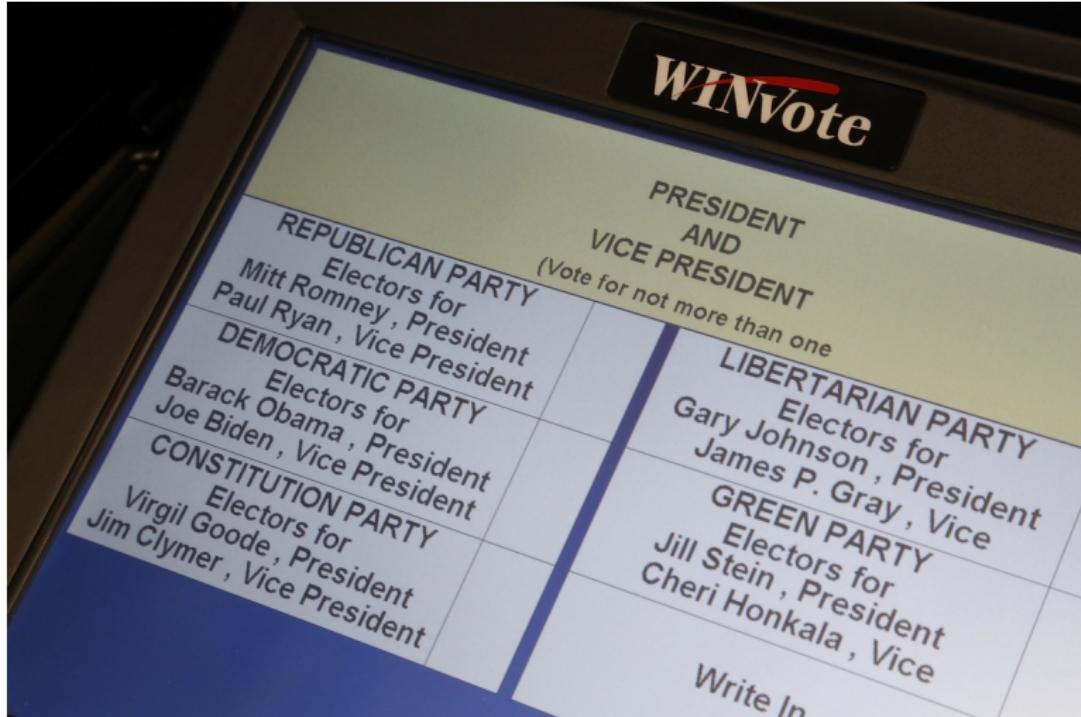


# AVS WINVote (1)



Urządzenia DRE produkowane przez firmę *Advanced Voting Solutions*.

# AVS WINVote (1)



Urządzenia DRE produkowane przez firmę *Advanced Voting Solutions*. Używane w 3 stanach USA: Pensylwanii, Missisipi i Virginii.

## AVS WINVote (2)

W 2015 roku zlecono kontrolę bezpieczeństwa. Lista znalezionych luk jest imponująco wręcz długa. Oto ona:

## AVS WINVote (2)

W 2015 roku zlecono kontrolę bezpieczeństwa. Lista znalezionych luk jest imponująco wręcz długa. Oto ona:

- maszyny połączone były bezprzewodową siecią LAN, zabezpiezoną przestarzałym protokołem WEP; hasło zostało ustawione na “abcde”, a jego zmiana nie była możliwa,

## AVS WINVote (2)

W 2015 roku zlecono kontrolę bezpieczeństwa. Lista znalezionych luk jest imponująco wręcz długa. Oto ona:

- maszyny połączone były bezprzewodową siecią LAN, zabezpiezoną 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,

## AVS WINVote (2)

W 2015 roku zlecono kontrolę bezpieczeństwa. Lista znalezionych luk jest imponująco wręcz długa. Oto ona:

- maszyny połączone były bezprzewodową siecią LAN, zabezpiezoną 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,
- hasło administratora systemu było ustawione na “admin”,

## AVS WINVote (2)

W 2015 roku zlecono kontrolę bezpieczeństwa. Lista znalezionych luk jest imponująco wręcz długa. Oto ona:

- maszyny połączone były bezprzewodową siecią LAN, zabezpiezoną 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,
- hasło administratora systemu było ustawione na “admin”,
- opcja udostępniania plików w sieci była włączona,

## AVS WINVote (2)

W 2015 roku zlecono kontrolę bezpieczeństwa. Lista znalezionych luk jest imponująco wręcz długa. Oto ona:

- maszyny połączone były bezprzewodową siecią LAN, zabezpiezoną 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,
- 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”),

## AVS WINVote (2)

W 2015 roku zlecono kontrolę bezpieczeństwa. Lista znalezionych luk jest imponująco wręcz długa. Oto ona:

- maszyny połączone były bezprzewodową siecią LAN, zabezpiezoną 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,
- 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,

## AVS WINVote (2)

W 2015 roku zlecono kontrolę bezpieczeństwa. Lista znalezionych luk jest imponująco wręcz długa. Oto ona:

- maszyny połączone były bezprzewodową siecią LAN, zabezpiezoną 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,
- 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 zaatakować wybory? (1)

# Jak zaatakować wybory? (1)

- ① Weź laptopa do lokalu wyborczego i usiądź na parkingu.

# Jak zaatakować wybory? (1)

- ① Weź laptopa do lokalu wyborczego i usiądź na parkingu.
- ② Złam proste hasło WEP.

# Jak zaatakować wybory? (1)

- ① Weź laptopa do lokalu wyborczego i usiądź na parkingu.
- ② Złam proste hasło WEP.
- ③ Podłącz się do sieci WiFi.

# Jak zaatakować wybory? (1)

- ① Weź laptopa do lokalu wyborczego i usiądź na parkingu.
- ② Złam proste hasło WEP.
- ③ Podłącz się do sieci WiFi.
- ④ Jeśli zostaniesz poproszony o hasło administratora, wpisz "admin".

# Jak zaatakować wybory? (1)

- ① Weź laptopa do lokalu wyborczego i usiądź na parkingu.
- ② Złam proste hasło WEP.
- ③ Podłącz się do sieci WiFi.
- ④ Jeśli zostaniesz poproszony o hasło administratora, wpisz "admin".
- ⑤ Przez opcję udostępniania plików ściągnij bazę danych z głosami.

# Jak zaatakować wybory? (1)

- ① Weź laptopa do lokalu wyborczego i usiądź na parkingu.
- ② Złam proste hasło WEP.
- ③ Podłącz się do sieci WiFi.
- ④ Jeśli zostaniesz poproszony o hasło administratora, wpisz "admin".
- ⑤ Przez opcję udostępniania plików ściągnij bazę danych z głosami.
- ⑥ Za pomocą prostego, darmowego narzędzia złam hasło do bazy danych ("shoup").

# Jak zaatakować wybory? (1)

- ① Weź laptopa do lokalu wyborczego i usiądź na parkingu.
- ② Złam proste hasło WEP.
- ③ Podłącz się do sieci WiFi.
- ④ Jeśli zostaniesz poproszony o hasło administratora, wpisz "admin".
- ⑤ Przez opcję udostępniania plików ściągnij bazę danych z głosami.
- ⑥ Za pomocą prostego, darmowego narzędzia złam hasło do bazy danych ("shoup").
- ⑦ Za pomocą Accessa zmieniaj, usuwaj i dodawaj głosy według uznania.

# Jak zaatakować wybory? (1)

- ① Weź laptopa do lokalu wyborczego i usiądź na parkingu.
- ② Złam proste hasło WEP.
- ③ Podłącz się do sieci WiFi.
- ④ Jeśli zostaniesz poproszony o hasło administratora, wpisz "admin".
- ⑤ Przez opcję udostępniania plików ściągnij bazę danych z głosami.
- ⑥ Za pomocą prostego, darmowego narzędzia złam hasło do bazy danych ("shoup").
- ⑦ Za pomocą Accessa zmieniaj, usuwaj i dodawaj głosy według uznania.
- ⑧ Wgraj zmienioną bazę danych z powrotem na serwer.

## Jak zaatakować wybory? (2)

Po kontroli maszyny utraciły certyfikat. Do wyborów pozostały dwa miesiące, a wszystkie urządzenia musiały zostać zastąpione.

## Jak zaatakować wybory? (2)

Po kontroli maszyny utraciły certyfikat. Do wyborów zostały dwa miesiące, a wszystkie urządzenia musiały zostać zastąpione.

Jeremy Epstein, Freedom To Tinker

Bottom line is that \*if\* no Virginia elections were ever hacked (and we have no way of knowing if it happened), it's because no one with even a modicum of skill tried.

# Diebold AccuVote-TS (1)



Rozwiązanie DRE od firmy *Diebold Election Systems* (produkującej DRE dla Brazylii).

# Diebold AccuVote-TS (1)



Rozwiązanie DRE od firmy *Diebold Election Systems* (produkującej DRE dla Brazylii). Kiedyś najpopularniejsze urządzenie DRE w USA. W wyborach w 2006 oddano przy jego pomocy 10% wszystkich głosów.

## Diebold AccuVote-TS (2)

- Grupa naukowców z Princeton University dokonała analizy bezpieczeństwa tego systemu.

## Diebold AccuVote-TS (2)

- Grupa naukowców z Princeton University dokonała analizy bezpieczeństwa tego systemu.
- Odkryli, że możliwe było wgranie złośliwego kodu na maszynę.

## Diebold AccuVote-TS (2)

- Grupa naukowców z Princeton University dokonała analizy bezpieczeństwa tego systemu.
- Odkryli, że możliwe było wgranie złośliwego kodu na maszynę.
- Taki kod mógłby wykradać głosy i zacierać za sobą ślady.

## Diebold AccuVote-TS (2)

- Grupa naukowców z Princeton University dokonała analizy bezpieczeństwa tego systemu.
- Odkryli, że możliwe było wgranie złośliwego kodu na maszynę.
- Taki kod mógłby wykradać głosy i zacierać za sobą ślady.
- Naukowcom udało się stworzyć wirusa instalującego złośliwy kod na innych maszynach (mimo braku połączenia z internetem).

## Diebold AccuVote-TS (2)

- Grupa naukowców z Princeton University dokonała analizy bezpieczeństwa tego systemu.
- Odkryli, że możliwe było wgranie złośliwego kodu na maszynę.
- Taki kod mógłby wykradać głosy i zacierać za sobą ślady.
- Naukowcom udało się stworzyć wirusa instalującego złośliwy kod na innych maszynach (mimo braku połączenia z internetem).
- Zaatakowanie tej maszyny było trudniejsze niż WINVote'a, ale w razie powodzenia mogło wpłynąć na większą liczbę głosów.

# Inne przypadki (e-voting)

## Inne przypadki (e-voting)

- W 2007 Sekretarz Stanu Kalifornia zarządziła kontrolę używanych tam systemów DRE. Ekspertyza wykazała podatności wszystkich rozwiązań na wykradanie głosów i złamanie prywatności . Uznano, że błędy są na tyle poważne, że działający w pojedynkę przestępca (niekoniecznie ekspert) mógłby zagrozić bezpieczeństwu wyborów w całym stanie.

## Inne przypadki (e-voting)

- W 2007 Sekretarz Stanu Kalifornia zarządziła kontrolę używanych tam systemów DRE. Ekspertyza wykazała podatności wszystkich rozwiązań na wykradanie głosów i złamanie prywatności . Uznano, że błędy są na tyle poważne, że działający w pojedynkę przestępca (niekoniecznie ekspert) mógłby zagrozić bezpieczeństwu wyborów w całym stanie.
- Okazuje się, że uzyskanie certyfikatu od władz nie gwarantuje bezpieczeństwa.

## Inne przypadki (e-voting)

- W 2007 Sekretarz Stanu Kalifornia zarządziła kontrolę używanych tam systemów DRE. Ekspertyza wykazała podatności wszystkich rozwiązań na wykradanie głosów i złamanie prywatności . Uznano, że błędy są na tyle poważne, że działający w pojedynkę przestępca (niekoniecznie ekspert) mógłby zagrozić bezpieczeństwu wyborów w całym stanie.
- Okazuje się, że uzyskanie certyfikatu od władz nie gwarantuje bezpieczeństwa.
- Wykryto podatność komputera wyborczego *Nedap ES3B* podobną do tej znalezionej w AccuVote-TS. Za jego pośrednictwem oddawano w Holandii 90% głosów.

## Inne przypadki (e-voting)

- W 2007 Sekretarz Stanu Kalifornia zarządziła kontrolę używanych tam systemów DRE. Ekspertyza wykazała podatności wszystkich rozwiązań na wykradanie głosów i złamanie prywatności . Uznano, że błędy są na tyle poważne, że działający w pojedynkę przestępca (niekoniecznie ekspert) mógłby zagrozić bezpieczeństwu wyborów w całym stanie.
- Okazuje się, że uzyskanie certyfikatu od władz nie gwarantuje bezpieczeństwa.
- Wykryto podatność komputera wyborczego *Nedap ES3B* podobną do tej znalezionej w AccuVote-TS. Za jego pośrednictwem oddawano w Holandii 90% głosów.
- Podobny problem dotyczył rozwiązania stosowanego w Indiach.

## Inne przypadki (e-voting)

- W 2007 Sekretarz Stanu Kalifornia zarządziła kontrolę używanych tam systemów DRE. Ekspertyza wykazała podatności wszystkich rozwiązań na wykradanie głosów i złamanie prywatności . Uznano, że błędy są na tyle poważne, że działający w pojedynkę przestępca (niekoniecznie ekspert) mógłby zagrozić bezpieczeństwu wyborów w całym stanie.
- Okazuje się, że uzyskanie certyfikatu od władz nie gwarantuje bezpieczeństwa.
- Wykryto podatność komputera wyborczego *Nedap ES3B* podobną do tej znalezionej w AccuVote-TS. Za jego pośrednictwem oddawano w Holandii 90% głosów.
- Podobny problem dotyczył rozwiązania stosowanego w Indiach.
- Nie tylko systemy DRE - udało się też zaatakować urządzenia do skanowania optycznego.

# Testowanie w Waszyngtonie (1)

- W 2010 w Waszyngtonie zdecydowano się stworzyć system do internetowego głosowania dla żołnierzy i ekspatriantów.

# Testowanie w Waszyngtonie (1)

- W 2010 w Waszyngtonie zdecydowano się stworzyć system do internetowego głosowania dla żołnierzy i ekspatriantów.
- Na tydzień przed rzeczywistymi wyborami zdecydowano się przeprowadzić wybory próbne.

# Testowanie w Waszyngtonie (1)

- W 2010 w Waszyngtonie zdecydowano się stworzyć system do internetowego głosowania dla żołnierzy i ekspatriantów.
- Na tydzień przed rzeczywistymi wyborami zdecydowano się przeprowadzić wybory próbne.
- Każdy mógł przetestować zabezpieczenia bez konsekwencji.

# Testowanie w Waszyngtonie (1)

- W 2010 w Waszyngtonie zdecydowano się stworzyć system do internetowego głosowania dla żołnierzy i ekspatriantów.
- Na tydzień przed rzeczywistymi wyborami zdecydowano się przeprowadzić wybory próbne.
- Każdy mógł przetestować zabezpieczenia bez konsekwencji.
- Kod systemu został opublikowany. Okazało się, że zawierał błędy.

# Testowanie w Waszyngtonie (1)

- W 2010 w Waszyngtonie zdecydowano się stworzyć system do internetowego głosowania dla żołnierzy i ekspatriantów.
- Na tydzień przed rzeczywistymi wyborami zdecydowano się przeprowadzić wybory próbne.
- Każdy mógł przetestować zabezpieczenia bez konsekwencji.
- Kod systemu został opublikowany. Okazało się, że zawierał błędy.
- Naukowcy odnaleźli lukę, która pozwoliła im przejąć kontrolę nad serwerem.

## Testowanie w Waszyngtonie (2)

- Udało się uzyskać dostęp do kamer monitoringu.

# Testowanie w Waszyngtonie (2)

- Udało się uzyskać dostęp do kamer monitoringu.
- Atakujący najpierw wykradli wszystkie hasła.

## Testowanie w Waszyngtonie (2)

- Udało się uzyskać dostęp do kamer monitoringu.
- Atakujący najpierw wykradli wszystkie hasła.
- Później zmienili oddane głosy na swoje.

# Testowanie w Waszyngtonie (2)

- Udało się uzyskać dostęp do kamer monitoringu.
- Atakujący najpierw wykradli wszystkie hasła.
- Później zmienili oddane głosy na swoje.
- Dodali kod, który modyfikował nowe głosy.

## Testowanie w Waszyngtonie (2)

- Udało się uzyskać dostęp do kamer monitoringu.
- Atakujący najpierw wykradli wszystkie hasła.
- Później zmienili oddane głosy na swoje.
- Dodali kod, który modyfikował nowe głosy.
- Dodali backdoor, który pozwalał im podglądać głosy.

## Testowanie w Waszyngtonie (2)

- Udało się uzyskać dostęp do kamer monitoringu.
- Atakujący najpierw wykradli wszystkie hasła.
- Później zmienili oddane głosy na swoje.
- Dodali kod, który modyfikował nowe głosy.
- Dodali backdoor, który pozwalał im podglądać głosy.
- Wyczyściли wszystkie logi.

# Testowanie w Waszyngtonie (3)

- Atakujący celowo zostawili ślad.

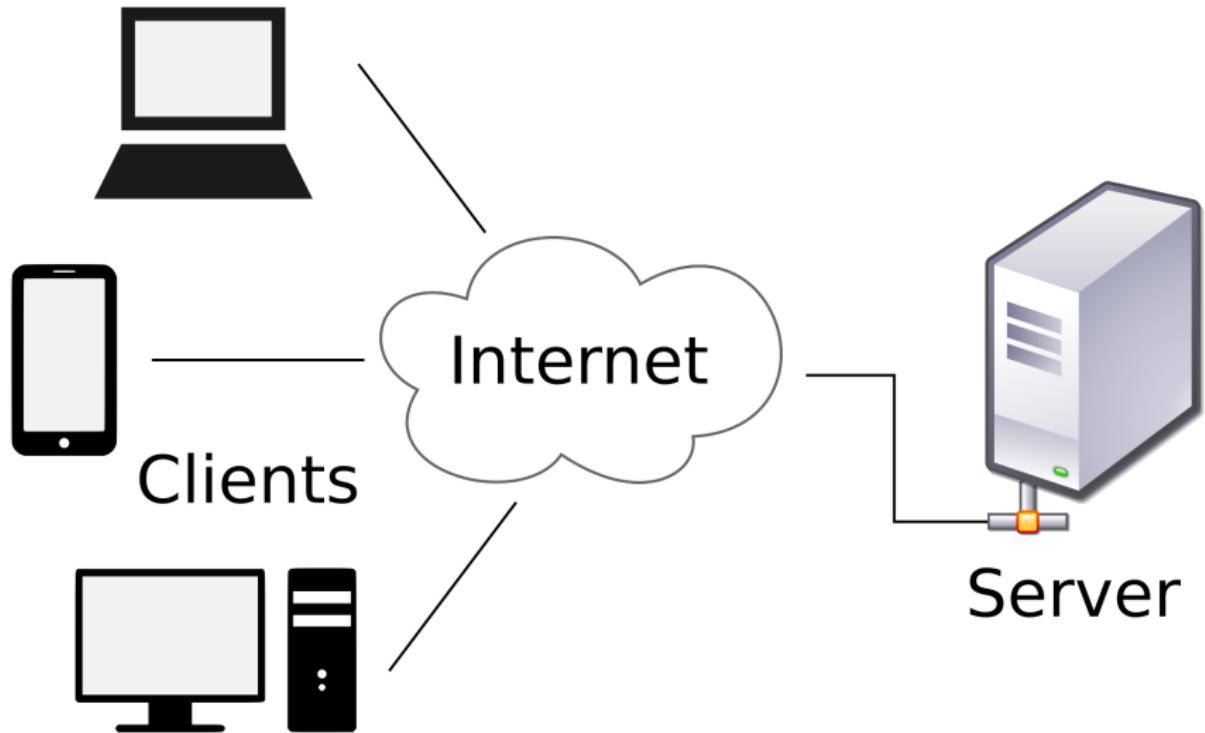
## Testowanie w Waszyngtonie (3)

- Atakujący celowo zostawili ślad.
- Włamanie zostało wykryte dopiero po dwóch dniach.

## Testowanie w Waszyngtonie (3)

- Atakujący celowo zostawili ślad.
- Włamanie zostało wykryte dopiero po dwóch dniach.
- Waszyngton zrezygnował z systemu i zezwolił na przesyłanie głosów pocztą.

# Jak zaatakować wybory w Estonii?



# Kto mógłby spróbować?

[Low graphics](#) | [Accessibility help](#)



[One-Minute World News](#)



## News services

Your news when you want it



### News Front Page



Africa  
Americas  
Asia-Pacific  
**Europe**  
Middle East  
South Asia

UK  
Business  
Health  
Science & Environment  
Technology

Entertainment

Also in the news

Video and Audio

Programmes

Have Your Say

Last Updated: Thursday, 17 May 2007, 15:21 GMT 16:21 UK

[E-mail this to a friend](#)

[Printable version](#)

## Estonia hit by 'Moscow cyber war'

**Estonia says the country's websites have been under heavy attack for the past three weeks, blaming Russia for playing a part in the cyber warfare.**

Many of the attacks have come from Russia and are being hosted by Russian state computer servers, Tallinn says. Moscow denies any involvement.

Estonia says the attacks began after it moved a Soviet war memorial in Tallinn. The move was condemned by the Kremlin.

A Nato spokesman said the organisation was giving Estonia technical help.



Estonia says many state websites have been affected

### SEE ALSO

- ▶ [The cyber pirates hitting Estonia](#)  
17 May 07 | Europe
- ▶ [Views diverge on Estonia's history](#)  
27 Apr 07 | Europe
- ▶ [Russia accused of 'attack on EU'](#)  
02 May 07 | Europe
- ▶ [Estonia unearths Soviet war dead](#)  
30 Apr 07 | Europe
- ▶ [Tallinn tense after deadly riots](#)  
28 Apr 07 | Europe
- ▶ [In pictures: Estonia clashes](#)  
27 Apr 07 | In Pictures
- ▶ [Country profile: Estonia](#)  
30 Apr 07 | Country profiles
- ▶ [Hi-tech crime: A glossary](#)  
05 Oct 06 | UK

### RELATED INTERNET LINKS

- ▶ [Estonian foreign ministry](#)
  - ▶ [Russian government](#)
- The BBC is not responsible for the

# Atak od strony serwera (1)

- Metody zbliżone do ataków na systemy DRE.

## Atak od strony serwera (1)

- Metody zbliżone do ataków na systemy DRE.
- Atakujący wgrywa złośliwy kod na komputer gromadzący lub zliczający głosy.

## Atak od strony serwera (1)

- Metody zbliżone do ataków na systemy DRE.
- Atakujący wgrywa złośliwy kod na komputer gromadzący lub zliczający głosy.
- Trudniejszy i łatwiejszy do wykrycia niż atak na klienta.

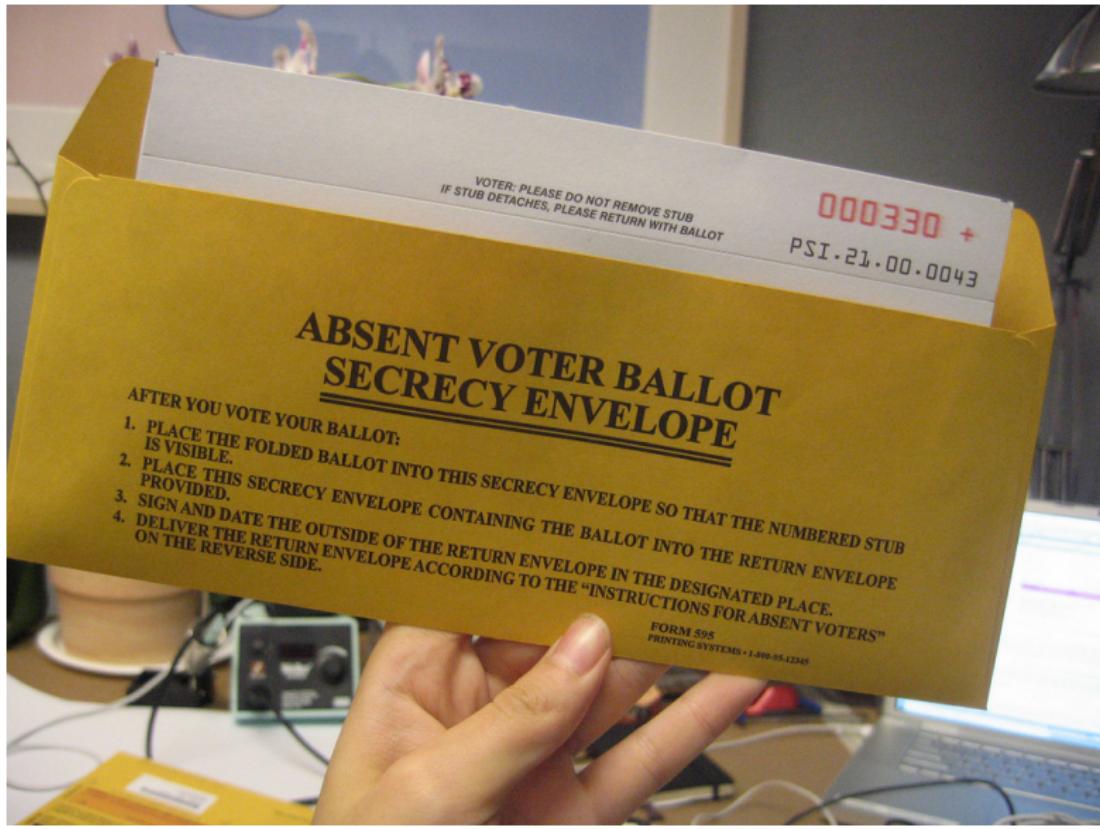
## Atak od strony serwera (1)

- Metody zbliżone do ataków na systemy DRE.
- Atakujący wgrywa złośliwy kod na komputer gromadzący lub zliczający głosy.
- Trudniejszy i łatwiejszy do wykrycia niż atak na klienta.
- W efekcie daje kontrolę nad wszystkimi głosami.

## Atak od strony serwera (1)

- Metody zbliżone do ataków na systemy DRE.
- Atakujący wgrywa złośliwy kod na komputer gromadzący lub zliczający głosy.
- Trudniejszy i łatwiejszy do wykrycia niż atak na klienta.
- W efekcie daje kontrolę nad wszystkimi głosami.
- W Estonii kod serwera jest publiczny.

## Atak od strony serwera (2)



## Atak od strony serwera (3)

- Atakujący musi dostać się do serwera zliczającego głosy.

## Atak od strony serwera (3)

- Atakujący musi dostać się do serwera zliczającego głosy.
- Sam serwer jest dość dobrze zabezpieczony.

## Atak od strony serwera (3)

- Atakujący musi dostać się do serwera zliczającego głosy.
- Sam serwer jest dość dobrze zabezpieczony.
- Ale na czymś przecież go napisano...

## Atak od strony serwera (3)

- Atakujący musi dostać się do serwera zliczającego głosy.
- Sam serwer jest dość dobrze zabezpieczony.
- Ale na czymś przecież go napisano...
- Okazuje się, że możliwe jest zaatakowanie serwera deweloperskiego.

## Atak od strony serwera (3)

- Atakujący musi dostać się do serwera zliczającego głosy.
- Sam serwer jest dość dobrze zabezpieczony.
- Ale na czymś przecież go napisano...
- Okazuje się, że możliwe jest zaatakowanie serwera deweloperskiego.
- Potem jest już łatwo.

## Atak od strony serwera (3)

- Atakujący musi dostać się do serwera zliczającego głosy.
- Sam serwer jest dość dobrze zabezpieczony.
- Ale na czymś przecież go napisano...
- Okazuje się, że możliwe jest zaatakowanie serwera deweloperskiego.
- Potem jest już łatwo.
- Bezpieczeństwo wyborów zależy od bezpieczeństwa operacyjnego. W Estonii nie było najlepiej...

# Atak od strony klienta (1)

# Atak od strony klienta (1)

- Klient to najsłabsze ogniwo.

# Atak od strony klienta (1)

- Klient to najsłabsze ogniwo.
- Według analityków da się napisać wirusa, który bez wiedzy wyborcy zmieni jego głos. Taki wirus mógłby ominąć wszystkie zabezpieczenia estońskiego systemu (e-dowód, PIN i aplikację weryfikującą).

# Atak od strony klienta (1)

- Klient to najsłabsze ogniwo.
- Według analityków da się napisać wirusa, który bez wiedzy wyborcy zmieni jego głos. Taki wirus mógłby ominąć wszystkie zabezpieczenia estońskiego systemu (e-dowód, PIN i aplikację weryfikującą).
- Atakujące może tak zmienić jeden głos. A co jeśli jest właścicielem botnetu? A co jeśli jest właścicielem wielu botnetów?

# Atak od strony klienta (1)

- Klient to najsłabsze ogniwo.
- Według analityków da się napisać wirusa, który bez wiedzy wyborcy zmieni jego głos. Taki wirus mógłby ominąć wszystkie zabezpieczenia estońskiego systemu (e-dowód, PIN i aplikację weryfikującą).
- Atakujące może tak zmienić jeden głos. A co jeśli jest właścicielem botnetu? A co jeśli jest właścicielem wielu botnetów?
- W Estonii kod klienta jest tajny.

## Atak od strony klienta (1)

- Klient to najsłabsze ogniwo.
- Według analityków da się napisać wirusa, który bez wiedzy wyborcy zmieni jego głos. Taki wirus mógłby ominąć wszystkie zabezpieczenia estońskiego systemu (e-dowód, PIN i aplikację weryfikującą).
- Atakujące może tak zmienić jeden głos. A co jeśli jest właścicielem botnetu? A co jeśli jest właścicielem wielu botnetów?
- W Estonii kod klienta jest tajny.
- Jeden z nich zademonstrował estoński student - Paavo Pihelglas. Zażądał unieważnienia wyborów, ale przegrał przez sądem. Wymiar sprawiedliwości uznał, że skoro on sam, dobrowolnie stworzył wirusa, to jego prawa nie zostały pogwałcone.

## Atak od strony klienta (2)

- Atakujący musi zainstalować swojego wirusa na komputerze klienta.

## Atak od strony klienta (2)

- Atakujący musi zainstalować swojego wirusa na komputerze klienta.
- Wirus wykrada PIN wyborcy.

## Atak od strony klienta (2)

- Atakujący musi zainstalować swojego wirusa na komputerze klienta.
- Wirus wykrada PIN wyborcy.
- I zmienia głos bez wiedzy użytkownika.

## Atak od strony klienta (2)

- Atakujący musi zainstalować swojego wirusa na komputerze klienta.
- Wirus wykrada PIN wyborcy.
- I zmienia głos bez wiedzy użytkownika.
- Analitycy zademonstrowali jak ominąć aplikację weryfikacyjną.

## Atak od strony klienta (2)

- Atakujący musi zainstalować swojego wirusa na komputerze klienta.
- Wirus wykrada PIN wyborcy.
- I zmienia głos bez wiedzy użytkownika.
- Analitycy zademonstrowali jak ominąć aplikację weryfikacyjną.
- Jak zainstalować wirusy?

# Zagrożenia



# Podstawowe wymagania

# Podstawowe wymagania

- ① Rzetelność - system musi dokładnie oddać wolę narodu.

# Podstawowe wymagania

- ① Rzetelność - system musi dokładnie oddać wolę narodu.
- ② Anonimowość - każdy głos powinien być całkowicie tajny. Nikt nie może mieć możliwości udowodnienia, że na kogoś głosował.

# Podstawowe wymagania

- ① Rzetelność - system musi dokładnie oddać wolę narodu.
- ② Anonimowość - każdy głos powinien być całkowicie tajny. Nikt nie może mieć możliwości udowodnienia, że na kogoś głosował.
- ③ Dostępność - wybory muszą odbyć się w wyznaczonym terminie.

# Podstawowe wymagania

- ① Rzetelność - system musi dokładnie oddać wolę narodu.
- ② Anonimowość - każdy głos powinien być całkowicie tajny. Nikt nie może mieć możliwości udowodnienia, że na kogoś głosował.
- ③ Dostępność - wybory muszą odbyć się w wyznaczonym terminie.
- ④ Przejrzystość - metoda przeprowadzania wyborów musi być prosta, przejrzysta i zrozumiała. Musi być możliwe obserwowanie całego procesu.

# Podstawowe wymagania

- ① Rzetelność - system musi dokładnie oddać wolę narodu.
- ② Anonimowość - każdy głos powinien być całkowicie tajny. Nikt nie może mieć możliwości udowodnienia, że na kogoś głosował.
- ③ Dostępność - wybory muszą odbyć się w wyznaczonym terminie.
- ④ Przejrzystość - metoda przeprowadzania wyborów musi być prosta, przejrzysta i zrozumiała. Musi być możliwe obserwowanie całego procesu.
- ⑤ Bezpieczeństwo - system musi działać sprawnie nawet w przypadku spisku oraz ataku hakerskiego. Musi istnieć metoda na wykrycie prób ataku i skontrolowanie wyniku.

# Bezpieczeństwo narodowe

- W praktyce stworzenie takiego systemu jest trudne.

# Bezpieczeństwo narodowe

- W praktyce stworzenie takiego systemu jest trudne.
- Bezpieczeństwa wyborów to bezpieczeństwo narodowe (nie komercyjne).

# Bezpieczeństwo narodowe

- W praktyce stworzenie takiego systemu jest trudne.
- Bezpieczeństwa wyborów to bezpieczeństwo narodowe (nie komercyjne).
- Głosowanie papierowe nie jest idealne, ale im więcej głosów chcemy ukraść, tym bardziej trudna jest organizacja ataku. Inaczej jest z głosowaniem elektronicznym.

# Bezpieczeństwo narodowe

- W praktyce stworzenie takiego systemu jest trudne.
- Bezpieczeństwa wyborów to bezpieczeństwo narodowe (nie komercyjne).
- Głosowanie papierowe nie jest idealne, ale im więcej głosów chcemy ukraść, tym bardziej trudna jest organizacja ataku. Inaczej jest z głosowaniem elektronicznym.
- Wystarczy nam system przynajmniej tak bezpieczny, jak głosowanie papierowe.

# Przejrzystość (e-voting)

# Przejrzystość (e-voting)

- DRE przyjmuje głosy i wydaje werdykt.

# Przejrzystość (e-voting)

- DRE przyjmuje głosy i wydaje werdykt.
- Skąd wyborca ma mieć pewność, że oprogramowanie działa tak, jak zapewnia producent?

# Przejrzystość (e-voting)

- DRE przyjmuje głosy i wydaje werdykt.
- Skąd wyborca ma mieć pewność, że oprogramowanie działa tak, jak zapewnia producent?
- Jednym z rozwiązań jest opublikowanie kodu źródłowego.

# Przejrzystość (e-voting)

- DRE przyjmuje głosy i wydaje werdykt.
- Skąd wyborca ma mieć pewność, że oprogramowanie działa tak, jak zapewnia producent?
- Jednym z rozwiązań jest opublikowanie kodu źródłowego.
- Skąd wyborca ma wiedzieć, że kod, który faktycznie działa na maszynie to ten, który został opublikowany?

# Przejrzystość (e-voting)

- DRE przyjmuje głosy i wydaje werdykt.
- Skąd wyborca ma mieć pewność, że oprogramowanie działa tak, jak zapewnia producent?
- Jednym z rozwiązań jest opublikowanie kodu źródłowego.
- Skąd wyborca ma wiedzieć, że kod, który faktycznie działa na maszynie to ten, który został opublikowany?
- Może zaufać.

# Przejrzystość (e-voting)

- DRE przyjmuje głosy i wydaje werdykt.
- Skąd wyborca ma mieć pewność, że oprogramowanie działa tak, jak zapewnia producent?
- Jednym z rozwiązań jest opublikowanie kodu źródłowego.
- Skąd wyborca ma wiedzieć, że kod, który faktycznie działa na maszynie to ten, który został opublikowany?
- Może zaufać.
- Albo sprawdzić sumami kontrolnymi.

# Bezpieczeństwo (e-voting)

- DRE są często podatne.

# Bezpieczeństwo (e-voting)

- DRE są często podatne.
- Być może atakom dałoby się zapobiec poprzez dalsze zabezpieczenia.

# Bezpieczeństwo (e-voting)

- DRE są często podatne.
- Być może atakom dałoby się zapobiec poprzez dalsze zabezpieczenia.
- Implementacja może być błędna, a rozwiązanie niekompletne.

# Bezpieczeństwo (e-voting)

- DRE są często podatne.
- Być może atakom dałoby się zapobiec poprzez dalsze zabezpieczenia.
- Implementacja może być błędna, a rozwiązanie niekompletne.
- Im więcej zabezpieczeń, tym mniej ludzi ufa systemowi. Im mniej ludzi ufa systemowi, tym mniej ludzi ufa wynikom.

# Bezpieczeństwo (e-voting)

- DRE są często podatne.
- Być może atakom dałoby się zapobiec poprzez dalsze zabezpieczenia.
- Implementacja może być błędna, a rozwiązanie niekompletne.
- Im więcej zabezpieczeń, tym mniej ludzi ufa systemowi. Im mniej ludzi ufa systemowi, tym mniej ludzi ufa wynikom.
- Co jeśli ktoś zaatakuje producenta? Używając DRE uzależniamy bezpieczeństwo narodowe od wewnętrznych zabezpieczeń korporacji.

# Problemy z i-votingiem (1)

# Problemy z i-votingiem (1)

- Łańcuch komunikacyjny pomiędzy wyborcą, a centralnym serwerem jest długi.

# Problemy z i-votingiem (1)

- Łańcuch komunikacyjny pomiędzy wyborcą, a centralnym serwerem jest długi.
- Taki system może zaatakować każdy - od samotnego hakera, do agencji wywiadowczej obcego rządu.

# Problemy z i-votingiem (1)

- Łańcuch komunikacyjny pomiędzy wyborcą, a centralnym serwerem jest długi.
- Taki system może zaatakować każdy - od samotnego hakera, do agencji wywiadowczej obcego rządu.
- Atakujący może cały proces przeprowadzić z dowolnego miejsca na świecie.

# Problemy z i-votingiem (1)

- Łańcuch komunikacyjny pomiędzy wyborcą, a centralnym serwerem jest długi.
- Taki system może zaatakować każdy - od samotnego hakera, do agencji wywiadowczej obcego rządu.
- Atakujący może cały proces przeprowadzić z dowolnego miejsca na świecie.
- Może nastąpić kilka ataków jednocześnie.

# Problemy z i-votingiem (1)

- Łańcuch komunikacyjny pomiędzy wyborcą, a centralnym serwerem jest długi.
- Taki system może zaatakować każdy - od samotnego hakera, do agencji wywiadowczej obcego rządu.
- Atakujący może cały proces przeprowadzić z dowolnego miejsca na świecie.
- Może nastąpić kilka ataków jednocześnie.
- Jeden atak może wpływać na wynik całych wyborów.

# Problemy z i-votingiem (1)

- Łańcuch komunikacyjny pomiędzy wyborcą, a centralnym serwerem jest długi.
- Taki system może zaatakować każdy - od samotnego hakera, do agencji wywiadowczej obcego rządu.
- Atakujący może cały proces przeprowadzić z dowolnego miejsca na świecie.
- Może nastąpić kilka ataków jednocześnie.
- Jeden atak może wpływać na wynik całych wyborów.
- Centralny serwer działa podobnie do maszyny DRE, więc jest podatny na te same ataki. Trzeba zatem:

# Problemy z i-votingiem (1)

- Łańcuch komunikacyjny pomiędzy wyborcą, a centralnym serwerem jest długi.
- Taki system może zaatakować każdy - od samotnego hakera, do agencji wywiadowczej obcego rządu.
- Atakujący może cały proces przeprowadzić z dowolnego miejsca na świecie.
- Może nastąpić kilka ataków jednocześnie.
- Jeden atak może wpłynąć na wynik całych wyborów.
- Centralny serwer działa podobnie do maszyny DRE, więc jest podatny na te same ataki. Trzeba zatem:
  - zweryfikować oprogramowanie serwera,

# Problemy z i-votingiem (1)

- Łańcuch komunikacyjny pomiędzy wyborcą, a centralnym serwerem jest długi.
- Taki system może zaatakować każdy - od samotnego hakera, do agencji wywiadowczej obcego rządu.
- Atakujący może cały proces przeprowadzić z dowolnego miejsca na świecie.
- Może nastąpić kilka ataków jednocześnie.
- Jeden atak może wpływać na wynik całych wyborów.
- Centralny serwer działa podobnie do maszyny DRE, więc jest podatny na te same ataki. Trzeba zatem:
  - zweryfikować oprogramowanie serwera,
  - zabezpieczyć go przed atakiem hakerów,

# Problemy z i-votingiem (1)

- Łącuch komunikacyjny pomiędzy wyborcą, a centralnym serwerem jest długi.
- Taki system może zaatakować każdy - od samotnego hakera, do agencji wywiadowczej obcego rządu.
- Atakujący może cały proces przeprowadzić z dowolnego miejsca na świecie.
- Może nastąpić kilka ataków jednocześnie.
- Jeden atak może wpływać na wynik całych wyborów.
- Centralny serwer działa podobnie do maszyny DRE, więc jest podatny na te same ataki. Trzeba zatem:
  - zweryfikować oprogramowanie serwera,
  - zabezpieczyć go przed atakiem hakerów,
  - zaufać dostawcy oprogramowania, że jego serwery były bezpieczne

# Problemy z i-votingiem (1)

- Łącuch komunikacyjny pomiędzy wyborcą, a centralnym serwerem jest długi.
- Taki system może zaatakować każdy - od samotnego hakera, do agencji wywiadowczej obcego rządu.
- Atakujący może cały proces przeprowadzić z dowolnego miejsca na świecie.
- Może nastąpić kilka ataków jednocześnie.
- Jeden atak może wpływać na wynik całych wyborów.
- Centralny serwer działa podobnie do maszyny DRE, więc jest podatny na te same ataki. Trzeba zatem:
  - zweryfikować oprogramowanie serwera,
  - zabezpieczyć go przed atakiem hakerów,
  - zaufać dostawcy oprogramowania, że jego serwery były bezpieczne
  - dodatkowo: zapewnić, że serwer będzie działa (DDoS)

## Problemy z i-votingiem (2)

- Dodatkowy problem: weryfikacja i autoryzacja wyborcy z zachowaniem anonimowości i przejrzystości.

## Problemy z i-votingiem (2)

- Dodatkowy problem: weryfikacja i autoryzacja wyborcy z zachowaniem anonimowości i przejrzystości.
- Nie można nic certyfikować - za wiele się zmienia.

## Problemy z i-votingiem (2)

- Dodatkowy problem: weryfikacja i autoryzacja wyborcy z zachowaniem anonimowości i przejrzystości.
- Nie można nic certyfikować - za wiele się zmienia.
- Pozostają ataki na transmisję i klienta.

## Problemy z i-votingiem (2)

- Dodatkowy problem: weryfikacja i autoryzacja wyborcy z zachowaniem anonimowości i przejrzystości.
- Nie można nic certyfikować - za wiele się zmienia.
- Pozostają ataki na transmisję i klienta.
- Nad tymi elementami procesu praktycznie nie ma kontroli.

## Problemy z i-votingiem (2)

- Dodatkowy problem: weryfikacja i autoryzacja wyborcy z zachowaniem anonimowości i przejrzystości.
- Nie można nic certyfikować - za wiele się zmienia.
- Pozostają ataki na transmisję i klienta.
- Nad tymi elementami procesu praktycznie nie ma kontroli.
- Atak na transmisję - przechwytywanie formularzy.

## Problemy z i-votingiem (2)

- Dodatkowy problem: weryfikacja i autoryzacja wyborcy z zachowaniem anonimowości i przejrzystości.
- Nie można nic certyfikować - za wiele się zmienia.
- Pozostają ataki na transmisję i klienta.
- Nad tymi elementami procesu praktycznie nie ma kontroli.
- Atak na transmisję - przechwytywanie formularzy.
- Ataki na klienta - wirusy.

# Kontrola wyniku

# Kontrola wyniku

- Zabezpieczenie jakiegokolwiek oprogramowania przed *wszystkimi* atakami nie jest możliwe.

# Kontrola wyniku

- Zabezpieczenie jakiegokolwiek oprogramowania przed *wszystkimi* atakami nie jest możliwe.
- Musi istnieć możliwość ponownego skontrolowania wyniku wyborów i wykrycia próby manipulacji (niezależna od systemu informatycznego).

# Kontrola wyniku

- Zabezpieczenie jakiegokolwiek oprogramowania przed *wszystkimi* atakami nie jest możliwe.
- Musi istnieć możliwość ponownego skontrolowania wyniku wyborów i wykrycia próby manipulacji (niezależna od systemu informatycznego).
- W przypadku głosowania czysto elektronicznego nie jest to możliwe, bo nie ma trwałego śladu po głosach wyborców.

# Zagrożenie bezpieczeństwa narodowego

- Niektóre ataki mogą zostać przeprowadzone przez jedną osobę.

# Zagrożenie bezpieczeństwa narodowego

- Niektóre ataki mogą zostać przeprowadzone przez jedną osobę.
- Gdyby się powiodły, mogłyby wpływać na wynik całych wyborów.

# Zagrożenie bezpieczeństwa narodowego

- Niektóre ataki mogą zostać przeprowadzone przez jedną osobę.
- Gdyby się powiodły, mogłyby wpłynąć na wynik całych wyborów.
- W razie wątpliwości niemożliwe byłoby przeprowadzenie kontroli.

# Zagrożenie bezpieczeństwa narodowego

- Niektóre ataki mogą zostać przeprowadzone przez jedną osobę.
- Gdyby się powiodły, mogłyby wpłynąć na wynik całych wyborów.
- W razie wątpliwości niemożliwe byłoby przeprowadzenie kontroli.
- Problemy z ewentualnym ściganiem atakujących.

# Lepsze rozwiązania



- Pozwala wyeliminować najpoważniejszy zarzut - niemożność przeprowadzenia kontroli.

- Pozwala wyeliminować najpoważniejszy zarzut - niemożność przeprowadzenia kontroli.
- Wciąż możemy korzystać z szybkiego przeliczania wyników.

- Pozwala wyeliminować najpoważniejszy zarzut - niemożność przeprowadzenia kontroli.
- Wciąż możemy korzystać z szybkiego przeliczania wyników.
- Bezpieczeństwo podobne jak przy wyborach tradycyjnych.

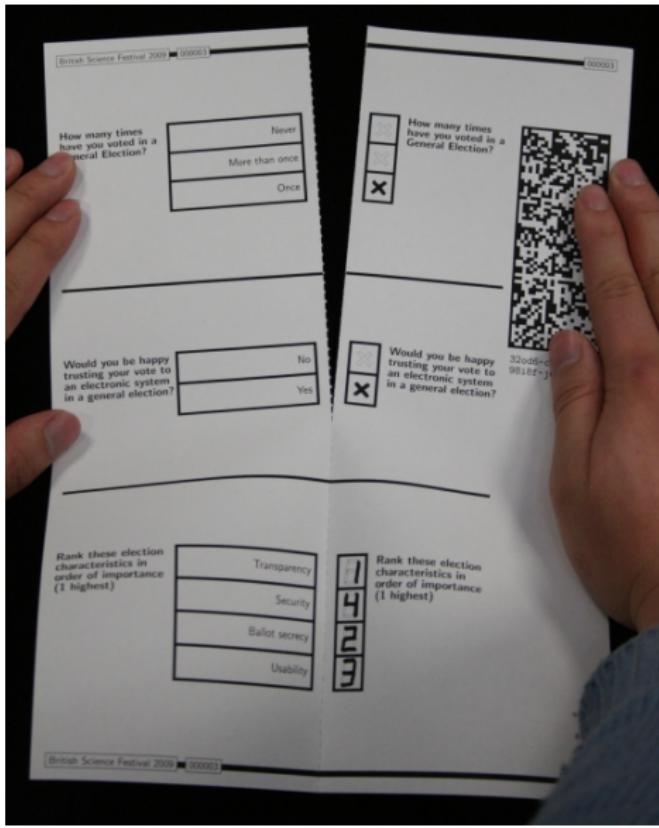
- Pozwala wyeliminować najpoważniejszy zarzut - niemożność przeprowadzenia kontroli.
- Wciąż możemy korzystać z szybkiego przeliczania wyników.
- Bezpieczeństwo podobne jak przy wyborach tradycyjnych.
- Wady:

- Pozwala wyeliminować najpoważniejszy zarzut - niemożność przeprowadzenia kontroli.
- Wciąż możemy korzystać z szybkiego przeliczania wyników.
- Bezpieczeństwo podobne jak przy wyborach tradycyjnych.
- Wady:
  - W całości zależy od potwierdzania wydruków przez wyborców.

- Pozwala wyeliminować najpoważniejszy zarzut - niemożność przeprowadzenia kontroli.
- Wciąż możemy korzystać z szybkiego przeliczania wyników.
- Bezpieczeństwo podobne jak przy wyborach tradycyjnych.
- Wady:
  - W całości zależy od potwierdzania wydruków przez wyborców.
  - Zwiększa koszty i ryzyko awarii.

- Pozwala wyeliminować najpoważniejszy zarzut - niemożność przeprowadzenia kontroli.
- Wciąż możemy korzystać z szybkiego przeliczania wyników.
- Bezpieczeństwo podobne jak przy wyborach tradycyjnych.
- Wady:
  - W całości zależy od potwierdzania wydruków przez wyborców.
  - Zwiększa koszty i ryzyko awarii.
- Jest wprowadzane w Indiach po wykryciu podatności ich DRE.

# Prêt à Voter



# Dlaczego głosowanie jest tak trudne?

# Dlaczego głosowanie jest tak trudne?

Bruce Schneier

Technology gets in the way of accuracy by adding steps. Each additional step means more potential errors, simply because no technology is perfect.

# Dlaczego głosowanie jest tak trudne?

Bruce Schneier

Technology gets in the way of accuracy by adding steps. Each additional step means more potential errors, simply because no technology is perfect.

- Bezpieczeństwo wyborów należy rozpatrywać w kategorii bezpieczeństwa narodowego.

# Dlaczego głosowanie jest tak trudne?

Bruce Schneier

Technology gets in the way of accuracy by adding steps. Each additional step means more potential errors, simply because no technology is perfect.

- Bezpieczeństwo wyborów należy rozpatrywać w kategorii bezpieczeństwa narodowego.
- Połączenie wymogów anonimowości, przejrzystości i bezpieczeństwa.

# Dlaczego głosowanie jest tak trudne?

Bruce Schneier

Technology gets in the way of accuracy by adding steps. Each additional step means more potential errors, simply because no technology is perfect.

- Bezpieczeństwo wyborów należy rozpatrywać w kategorii bezpieczeństwa narodowego.
- Połączenie wymogów anonimowości, przejrzystości i bezpieczeństwa.
- Głos każdego wyborcy jest równie istotny.

# Dlaczego głosowanie jest tak trudne?

Bruce Schneier

Technology gets in the way of accuracy by adding steps. Each additional step means more potential errors, simply because no technology is perfect.

- Bezpieczeństwo wyborów należy rozpatrywać w kategorii bezpieczeństwa narodowego.
- Połączenie wymogów anonimowości, przejrzystości i bezpieczeństwa.
- Głos każdego wyborcy jest równie istotny.
- Nikt nie wie, jaki będzie wynik.

# Dlaczego głosowanie jest tak trudne?

Bruce Schneier

Technology gets in the way of accuracy by adding steps. Each additional step means more potential errors, simply because no technology is perfect.

- Bezpieczeństwo wyborów należy rozpatrywać w kategorii bezpieczeństwa narodowego.
- Połączenie wymogów anonimowości, przejrzystości i bezpieczeństwa.
- Głos każdego wyborcy jest równie istotny.
- Nikt nie wie, jaki będzie wynik.
- Szczególny nacisk na bezpieczeństwo - odwrócenie skutków ataku może być trudne.

# Ostatnie wybory w USA (1)



## Ostatnie wybory w USA (2)

## Ostatnie wybory w USA (2)

- Hillary Clinton otrzymała znaczaco mniej głosów w okręgach używających elektroniki niż w tych, gdzie głosuje się papierowo.

## Ostatnie wybory w USA (2)

- Hillary Clinton otrzymała znaczco mniej głosów w okręgach używających elektroniki niż w tych, gdzie głosuje się papierowo.
- Dokładnie takiego wyniku oczekiwaliśmy, gdyby wybory zostały zmanipulowane.

## Ostatnie wybory w USA (2)

- Hillary Clinton otrzymała znaczaco mniej głosów w okręgach używających elektroniki niż w tych, gdzie głosuje się papierowo.
- Dokładnie takiego wyniku oczekiwaliśmy, gdyby wybory zostały zmanipulowane.
- Prawdopodobieństwo ataku niskie.

## Ostatnie wybory w USA (2)

- Hillary Clinton otrzymała znaczaco mniej głosów w okręgach używających elektroniki niż w tych, gdzie głosuje się papierowo.
- Dokładnie takiego wyniku oczekiwaliśmy, gdyby wybory zostały zmanipulowane.
- Prawdopodobieństwo ataku niskie.
- Nie ma kto, ani jak tego sprawdzić.

## Ostatnie wybory w USA (2)

- Hillary Clinton otrzymała znaczaco mniej głosów w okręgach używających elektroniki niż w tych, gdzie głosuje się papierowo.
- Dokładnie takiego wyniku oczekiwaliśmy, gdyby wybory zostały zmanipulowane.
- Prawdopodobieństwo ataku niskie.
- Nie ma kto, ani jak tego sprawdzić.
- Nawet jeśli były zmanipulowane, to nie za bardzo jest jak to odkręcić.

## Ostatnie wybory w USA (2)

- Hillary Clinton otrzymała znaczco mniej głosów w okręgach używających elektroniki niż w tych, gdzie głosuje się papierowo.
- Dokładnie takiego wyniku oczekiwaliśmy, gdyby wybory zostały zmanipulowane.
- Prawdopodobieństwo ataku niskie.
- Nie ma kto, ani jak tego sprawdzić.
- Nawet jeśli były zmanipulowane, to nie za bardzo jest jak to odkręcić.
- Żółta kartka dla elektronicznego głosowania.

### Bruce Schneier

But we only have two years until the next national elections, and it's time to start fixing things if we don't want to be wondering the same things about hackers in 2018. The risks are real: Electronic voting machines that don't use a paper ballot are vulnerable to hacking.