How not to build an electronic voting system

Quentin Kaiser

Hack.lu 2015

October 21, 2015

$ whoami

Quentin Kaiser
Security Engineer | Penetration Tester

🏠 www.quentinkaiser.be
✉ contact@quentinkaiser.be
🐦 QKaiser

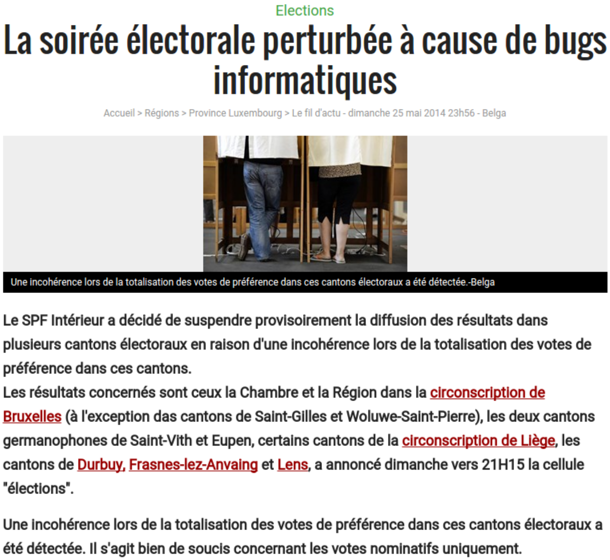
Disclaimer

This research was prepared and accomplished in my personal capacity. The opinions expressed in this talk are my own and do not reflect the view of past, current, or future employer.

Outline

- Introduction
- Evoting Systems in Belgium
- Building Secure Voting Systems
- CODI
  - Polling stations
  - Network infrastructure
  - Web Applications
- Smartmatic
  - Election Configuration Manager
  - PV-VM
- Conclusions

Introduction



Elections

La soirée électorale perturbée à cause de bugs informatiques

Accueil > Régions > Province Luxembourg > Le fil d'actu - dimanche 25 mai 2014 23h56 - Belga

Une incohérence lors de la totalisation des votes de préférence dans ces cantons électoraux a été détectée.-Belga

Le SPF Intérieur a décidé de suspendre provisoirement la diffusion des résultats dans plusieurs cantons électoraux en raison d'une incohérence lors de la totalisation des votes de préférence dans ces cantons.

Les résultats concernés sont ceux la Chambre et la Région dans la circonscription de Bruxelles (à l'exception das cantons de Saint-Gilles et Woluwe-Saint-Pierre), les deux cantons germanophones de Saint-Vith et Eupen, certains cantons de la circonscription de Liège, les cantons de Durbuy, Frasnes-lez-Anvaing et Lens, a annoncé dimanche vers 21H15 la cellule "élections".

Une incohérence lors de la totalisation des votes de préférence dans ces cantons électoraux a été détectée. Il s'agit bien de soucis concernant les votes nominatifs uniquement.

"I think your crypto is broken" - King Albert II

- 1991 - first experiment in two townships
- 1994 - expanded to 20% of electorate
- 1999 - expanded to 44% of electorate, introduction of OCR counting
- 2003 - first experiment with ticketing in two townships
- 2007 - BeVoting report
- 2012 - Introduction of Smartmatic systems

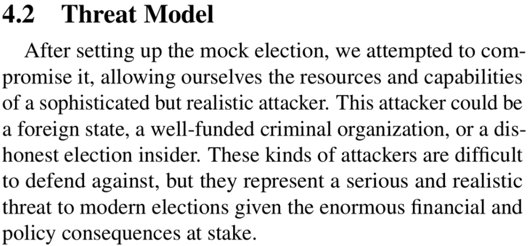
Cryptographically Secure Voting Systems

Building secure voting systems is **complex**.

- Confidentiality
- Non repudiation
- Authenticity
- Integrity
- Non coercion
- Uniqueness
- Audit trail
- Simplicity
- Equity
- Verifiability

Threat Model

And people are out there to get you.



4.2 Threat Model

After setting up the mock election, we attempted to compromise it, allowing ourselves the resources and capabilities of a sophisticated but realistic attacker. This attacker could be a foreign state, a well-funded criminal organization, or a dishonest election insider. These kinds of attackers are difficult to defend against, but they represent a serious and realistic threat to modern elections given the enormous financial and policy consequences at stake.

[1]

[1] Security Analysis of the Estonian Internet Voting System

CODI

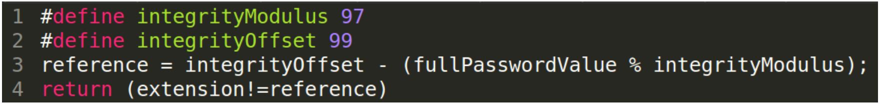
CODI

CODI encompass multiple evoting components:

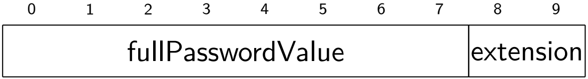
- Jites
- Digivote
- PGM2
- PGM3
- Election Management System

Authentication & Authorization

- polling station president initialize software with a password
- password verified with checksum



```
#define integrityModulus 97
#define integrityOffset 99
reference = integrityOffset - (fullPasswordValue % integrityModulus);
return (extension!=reference)
```

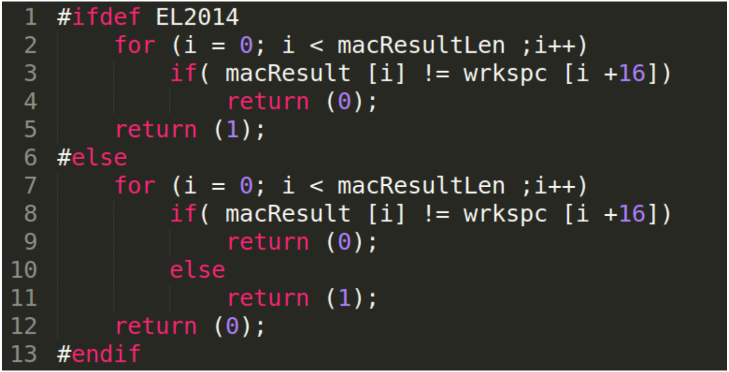


Password checksum

CODI
Voting booths

Integrity Protection

- floppy disk content integrity is checked



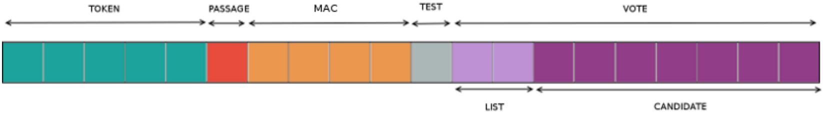
```
#ifdef EL2014
    for (i = 0; i < macResultLen ;i++)
        if( macResult [i] != wrkspc [i +16])
            return (0);
    return (1);
#else
    for (i = 0; i < macResultLen ;i++)
        if( macResult [i] != wrkspc [i +16])
            return (0);
        else
            return (1);
    return (0);
#endif
```

Vote casting

- bug2505 explored by @doegox [2]

[1] http://www.poureva.be/spip.php?article853

Magnetic card layout



- **token** (5 bytes) - uniquely identify a polling station
- **passage** (1 byte) - boolean for vote casting
- **MAC**[3] (4 bytes) - ensure integrity and authenticity of vote
- **test** (1 byte) - identify voter type (N, E, S)
- **vote** ($2 + x$ bytes) - vote value

[3] ISO-9797-1, Algo 2 / Padding 2

Fraud detection

- **Byte length** - Sanity check
- **Token** - Ensure vote was cast in same polling station
- **MAC** - Ensure integrity and authenticity of vote

CODI - Ballot boxes

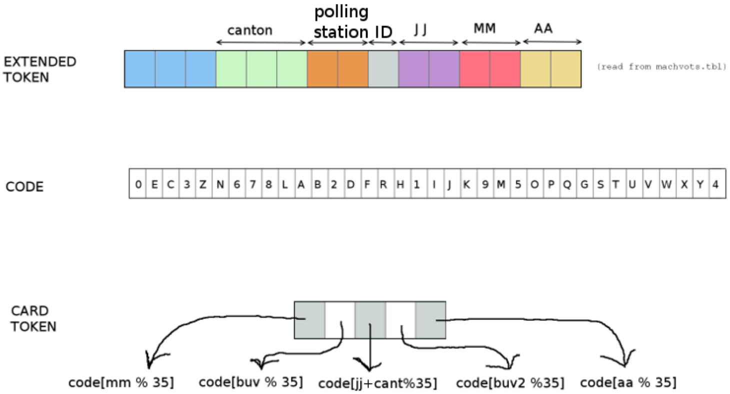
Bypassing fraud detection

Step 1 - Byte length

CODI - Ballot boxes

Bypassing fraud detection

Step 2 - Token recovery

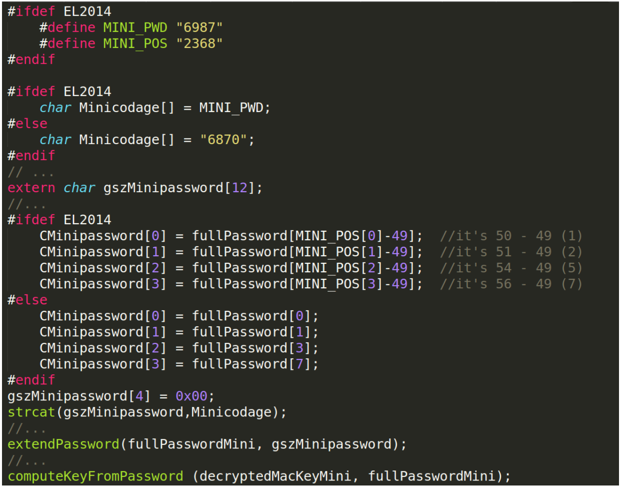


CODE	0	E	C	3	Z	N	6	7	8	L	A	B	2	D	F	R	H	1	I	J	K	9	M	5	O	P	Q	G	S	T	U	V	W	X	Y	4

CODI - Ballot boxes

Bypassing fraud detection

Step 3 - MAC key recovery

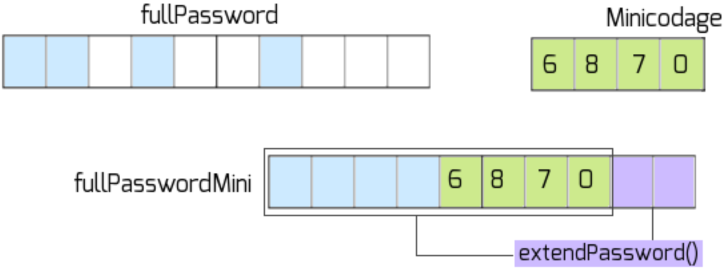


```
#ifdef EL2014
    #define MINI_PWD "6987"
    #define MINI_POS "2368"
#endif

#ifdef EL2014
    char Minicodage[] = MINI_PWD;
#else
    char Minicodage[] = "6870";
#endif
// ...
extern char gszMinipassword[12];
//...
#ifdef EL2014
    CMinipassword[0] = fullPassword[MINI_POS[0]-49];  //it's 50 - 49 (1)
    CMinipassword[1] = fullPassword[MINI_POS[1]-49];  //it's 51 - 49 (2)
    CMinipassword[2] = fullPassword[MINI_POS[2]-49];  //it's 54 - 49 (5)
    CMinipassword[3] = fullPassword[MINI_POS[3]-49];  //it's 56 - 49 (7)
#else
    CMinipassword[0] = fullPassword[0];
    CMinipassword[1] = fullPassword[1];
    CMinipassword[2] = fullPassword[3];
    CMinipassword[3] = fullPassword[7];
#endif
gszMinipassword[4] = 0x00;
strcat(gszMinipassword,Minicodage);
//...
extendPassword(fullPasswordMini, gszMinipassword);
//...
computeKeyFromPassword (decryptedMacKeyMini, fullPasswordMini);
```

CODI - Ballot boxes

Bypassing fraud detection

Step 3 - MAC key recovery



Step 3 - MAC key recovery

- read MAC and vote values off a magnetic card
- foreach 10^4 possible password combinations
  1. derive key from password combination
  2. compute MAC with derived key
  3. compare computed MAC with magnetic card's MAC

Byproduct of MAC key recovery: you also recovered 6 bytes out of 10 of the polling station's president password.

Fraud detection

- **Byte length** - Done
- **Token** - Done
- **MAC** - Done

Being able to create rogue magnetic cards breaks:

- non-coercion (vote buying activities)
- uniqueness (ballot stuffing)

CODI - Ballot boxes

Secure vote storage

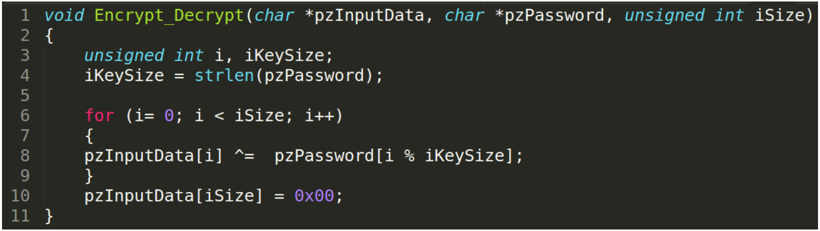
- Votes are stored in temporary file during election process
- temporary file encrypted with AES on polling station closing

CODI - Ballot boxes

Secure vote storage

Temporary file

- "encrypt" each vote with XOR cipher
- randomness of vote position is heavily questionned



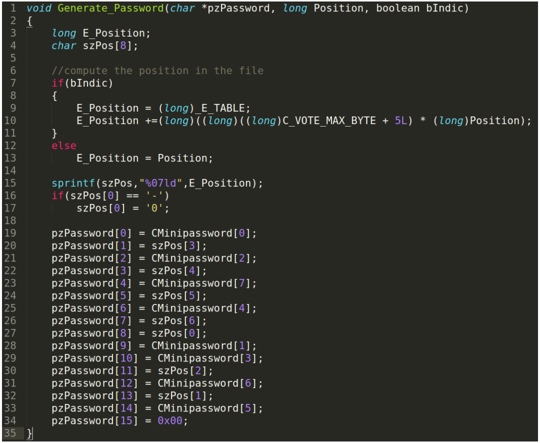
```c
void Encrypt_Decrypt(char *pzInputData, char *pzPassword, unsigned int iSize)
{
    unsigned int i, iKeySize;
    iKeySize = strlen(pzPassword);

    for (i= 0; i < iSize; i++)
    {
    pzInputData[i] ^=  pzPassword[i % iKeySize];
    }
    pzInputData[iSize] = 0x00;
}
```

CODI - Ballot boxes

Secure vote storage

Temporary file

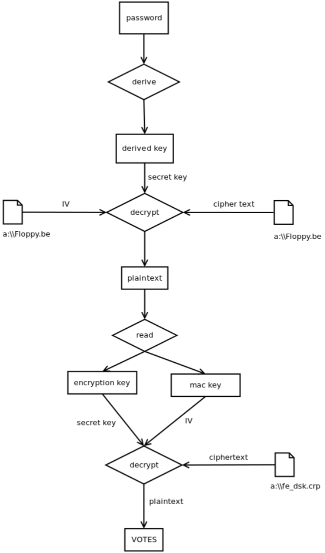
- XOR filter easily recoverable by brute force or offline attack (see fraud detection bypass)



```
void Generate_Password(char *pzPassword, long Position, boolean bIndic)
{
    long E_Position;
    char szPos[8];

    //compute the position in the file
    if(bIndic)
    {
        E_Position = (long)_E_TABLE;
        E_Position +=(long)((long)((long)C_VOTE_MAX_BYTE + 5L) * (long)Position);
    }
    else
        E_Position = Position;

    sprintf(szPos,"%07ld",E_Position);
    if(szPos[0] == '-')
        szPos[0] = '0';

    pzPassword[0] = CMinipassword[0];
    pzPassword[1] = szPos[3];
    pzPassword[2] = CMinipassword[2];
    pzPassword[3] = szPos[4];
    pzPassword[4] = CMinipassword[7];
    pzPassword[5] = szPos[5];
    pzPassword[6] = CMinipassword[4];
    pzPassword[7] = szPos[6];
    pzPassword[8] = szPos[0];
    pzPassword[9] = CMinipassword[1];
    pzPassword[10] = CMinipassword[3];
    pzPassword[11] = szPos[2];
    pzPassword[12] = CMinipassword[6];
    pzPassword[13] = szPos[1];
    pzPassword[14] = CMinipassword[5];
    pzPassword[15] = 0x00;
}
```

CODI - Ballot boxes

Secure vote storage



PGM2 & PGM3

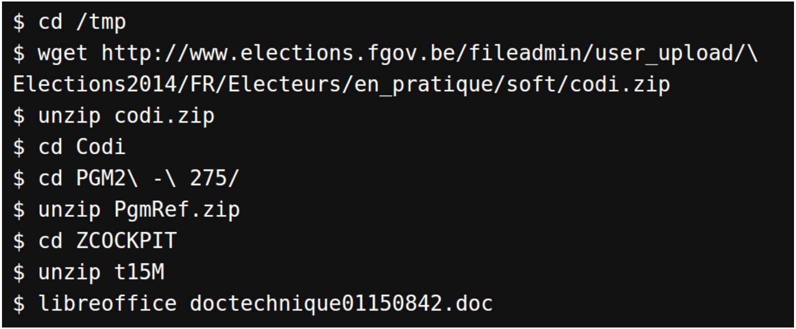
- Microsoft Windows executables
- rely on obscure software (GuptaSQL, anyone ?)
- did not manage to execute them properly :(

Expected behavior:

- generate minutes as PDF file
- PDF file signed with polling station president eID
- encode votes into undocumented ”Format F” format
- minutes PDF + ”Format F” content sent to central server

CODI

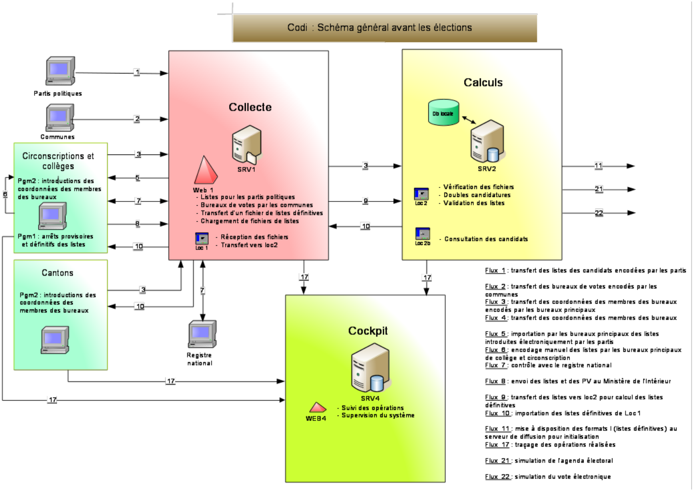
Secure Vote Transmission



```
$ cd /tmp
$ wget http://www.elections.fgov.be/fileadmin/user_upload/\
Elections2014/FR/Electeurs/en_pratique/soft/codi.zip
$ unzip codi.zip
$ cd Codi
$ cd PGM2\ -\ 275/
$ unzip PgmRef.zip
$ cd ZCOCKPIT
$ unzip t15M
$ libreoffice doctechnique01150842.doc
```

Zipping deeper

CODI
Secure Vote Transmission


Codi : Schéma général avant les élections
Partis politiques
Communes
Circonscriptions et collèges
Pgm2 : introductions des coordonnées des membres des bureaux
Pgm1 : arrêts provisoires et définitifs des listes
Cantons
Pgm2 : introductions des coordonnées des membres des bureaux
Registre national
Collecte
SRV1
Web 1
- Listes pour les partis politiques
- Bureaux de votes par les communes
- Transfert d'un fichier de listes définitives
- Chargement de fichiers de listes
Loc 1
- Réception des fichiers
- Transfert vers loc2
Calculs
Db locale
SRV2
Loc2
- Vérification des fichiers
- Doubles candidatures
- Validation des listes
Loc 2b
- Consultation des candidats
Cockpit
SRV4
WEB4
- Suivi des opérations
- Supervision du système
1
2
3
5
6
7
8
10
3
10
7
3
9
10
11
21
22
17
17
17
17

Flux 1 : transfert des listes des candidats encodées par les partis

Flux 2 : transfert des bureaux de votes encodés par les communes

Flux 3 : transfert des coordonnées des membres des bureaux encodés par les bureaux principaux

Flux 4 : transfert des coordonnées des membres des bureaux

Flux 5 : importation par les bureaux principaux des listes introduites électroniquement par les partis

Flux 6 : encodage manuel des listes par les bureaux principaux de collège et circonscription

Flux 7 : contrôle avec le registre national

Flux 8 : envoi des listes et des PV au Ministère de l'Intérieur

Flux 9 : transfert des listes vers loc2 pour calcul des listes définitives

Flux 10 : importation des listes définitives de Loc1

Flux 11 : mise à disposition des formats I (listes définitives) au serveur de diffusion pour initialisation

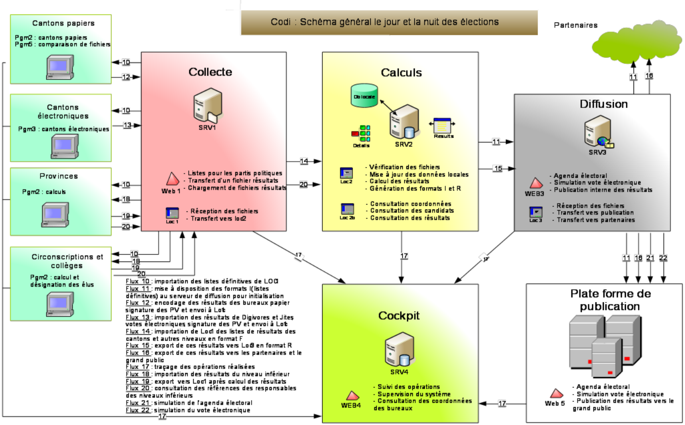
Flux 17 : traçage des opérations réalisées

Flux 21 : simulation de l'agenda électoral

Flux 22 : simulation du vote électronique

CODI

Secure Vote Transmission



Codi : Schéma général le jour et la nuit des élections

Cantons papiers

Pgm2 : cantons papiers
Pgm5 : comparaison de fichiers

Cantons électroniques

Pgm3 : cantons électroniques

Provinces

Pgm2 : calculs

Circonscriptions et collèges

Pgm2 : calcul et désignation des élus

Collecte

SRV1

Web 1
- Listes pour les partis politiques
- Transfert d'un fichier résultats
- Chargement de fichiers résultats

Loc 1
- Réception des fichiers
- Transfert vers loc2

Calculs

Db locale

Details

SRV2

Results

Loc2
- Vérification des fichiers
- Mise à jour des données locales
- Calcul des résultats
- Génération des formats I et R

Loc 2b
- Consultation coordonnées
- Consultation des candidats
- Consultation des résultats

Partenaires

Diffusion

SRV3

WEB3
- Agenda électoral
- Simulation vote électronique
- Publication interne des résultats

Loc 3
- Réception des fichiers
- Transfert vers publication
- Transfert vers partenaires

Cockpit

SRV4

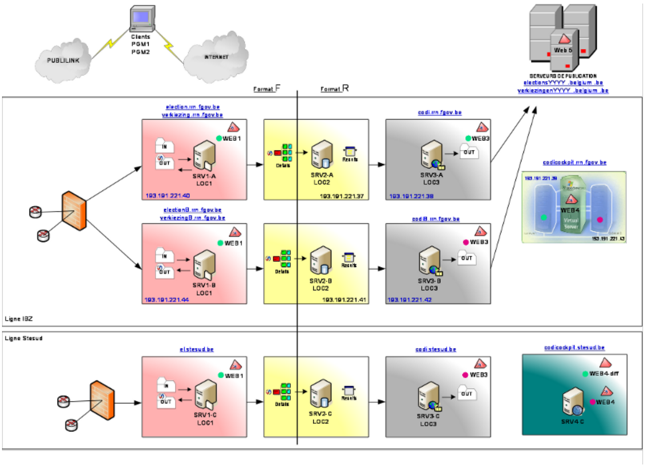
WEB4
- Suivi des opérations
- Supervision du système
- Consultation des coordonnées des bureaux

Plate forme de publication

Web 5
- Agenda électoral
- Simulation vote électronique
- Publication des résultats vers le grand public

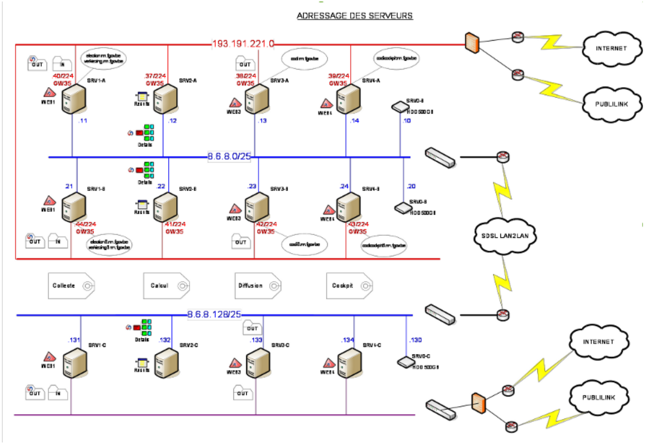
Flux 10 : importation des listes définitives de LOC1
Flux 11 : mise à disposition des formats I(listes définitives) au serveur de diffusion pour initialisation
Flux 12 : encodage des résultats des bureaux papier signature des PV et envoi à Loc1
Flux 13 : importation des résultats de Digivores et Jites votes électroniques signature des PV et envoi à Loc1
Flux 14 : importation de Loc1 des listes de résultats des cantons et autres niveaux en format F
Flux 15 : export de ces résultats vers Loc3 en format R
Flux 16 : export de ces résultats vers les partenaires et le grand public
Flux 17 : traçage des opérations réalisées
Flux 18 : importation des résultats du niveau inférieur
Flux 19 : export vers Loc1 après calcul des résultats
Flux 20 : consultation des références des responsables des niveaux inférieurs
Flux 21 : simulation de l'agenda électoral
Flux 22 : simulation du vote électronique

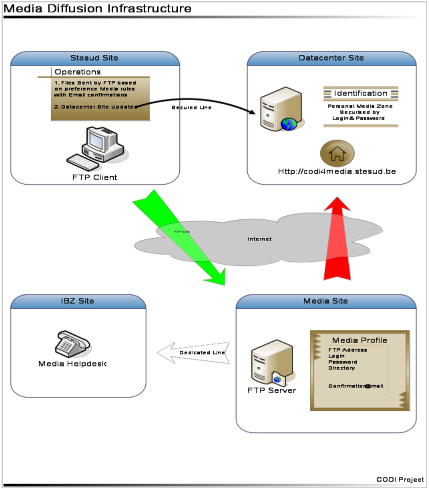
CODI
Secure Vote Transmission



CODI

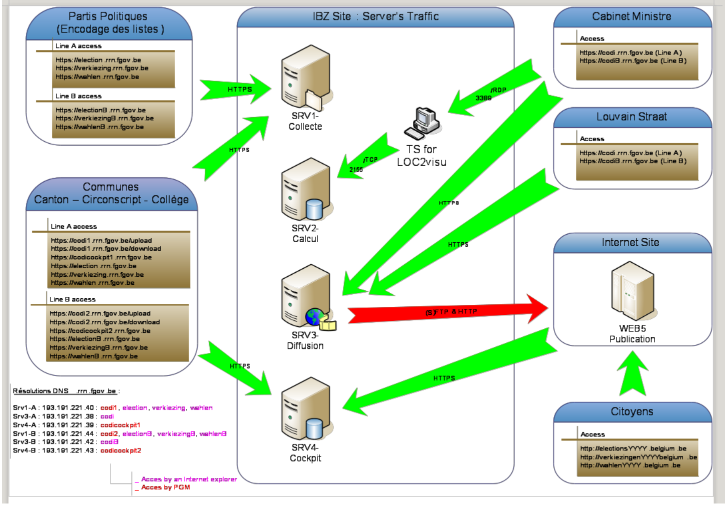
Secure Vote Transmission




Media Diffusion Infrastructure
Stesud Site
Operations
1. Files Sent by FTP based on preference Media rules with Email confirmations
2. Datacenter Site Updated
FTP Client
Secured Line
Datacenter Site
Identification
Personal Media Zone Securised by Login& Password
Http://codi4media.stesud.be
FTP Traffic
Internet
IBZ Site
Media Helpdesk
Dedicated Line
Media Site
FTP Server
Media Profile
FTP Address
Login
Password
Directory
Confirmation@mail
CODI Project

CODI

Secure Vote Transmission



Partis Politiques
(Encodage des listes)

Line A access

https://election .rrn.fgov .be
https://verkiezing.rrn.fgov.be
https://wahlen .rrn.fgov.be

Line B access

https://electionB .rrn.fgov.be
https://verkiezingB .rrn.fgov.be
https://wahlenB .rrn.fgov.be

Communes
Canton – Circonscript - Collège

Line A access

https://codi1 .rrn.fgov.be/upload
https://codi1 .rrn.fgov.be/download
https://codicockpit1 .rrn.fgov .be
https://election .rrn. fgov.be
https://verkiezing.rrn.fgov.be
https://wahlen .rrn.fgov .be

Line B access

https://codi2.rrn.fgov.be/upload
https://codi2.rrn.fgov.be/download
https://codicockpit2 .rrn.fgov .be
https://electionB .rrn.fgov.be
https://verkiezingB .rrn.fgov.be
https://wahlenB .rrn.fgov.be

Résolutions DNS .rrn .fgov .be :

Srv1-A : 193.191 .221 .40 : codi1 , election , verkiezing, wahlen
Srv3-A : 193.191 .221 .38 : codi
Srv4-A : 193.191 .221 .39 : codicockpit1
Srv1-B : 193.191 .221 .44 : codi2, electionB , verkiezingB, wahlenB
Srv3-B : 193.191 .221 .42 : codiB
Srv4-B : 193.191 .221 .43 : codicockpit2

_ Acces by an Internet explorer
_ Acces by PGM

IBZ Site : Server's Traffic

Cabinet Ministre

Access

https://codi .rrn.fgov.be (Line A)
https://codiB .rrn.fgov.be (Line B)

Louvain Straat

Access

https://codi .rrn.fgov.be (Line A)
https://codiB .rrn.fgov.be (Line B)

Internet Site

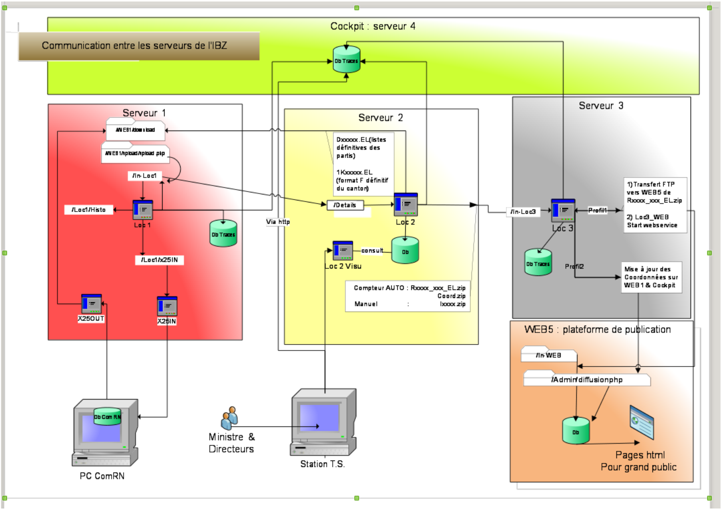
Citoyens

Access

http://electionsYYYY .belgium .be
http://verkiezingenYYYYbelgium .be
http://wahlenYYYY .belgium .be

CODI

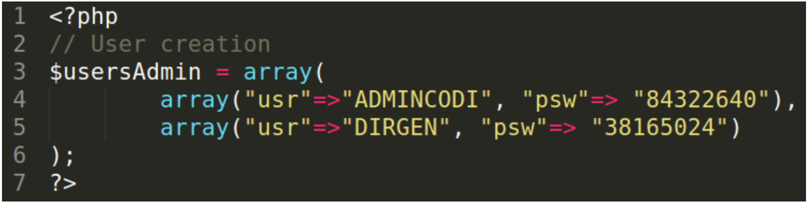
Secure Vote Transmission



aka OWASP Top 10

- Web1 : encoding of lists, candidates, polling stations, ...
- **Web2 : used by belgian ambassies to transmit votes**
- Web3 : Ministry of home affairs intranet webapp holding election results
- Web4 : logging and monitoring of Websomething
- Web5 : webapp that hosts results, available to the general public
- Loc1 : reception of ”format F” files and transmission to Loc2
- Loc2 : results verification, loading in database, transmission to Loc3
- Loc3 : transmission of results to different partners (mostly press, hopefully)

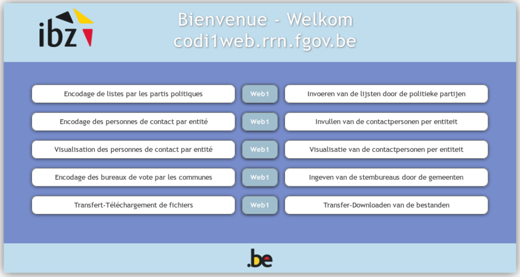
Information leak



```php
<?php
// User creation
$usersAdmin = array(
        array("usr"=>"ADMINCODI", "psw"=> "84322640"),
        array("usr"=>"DIRGEN", "psw"=> "38165024")
);
?>
```

CODI

Election Management System

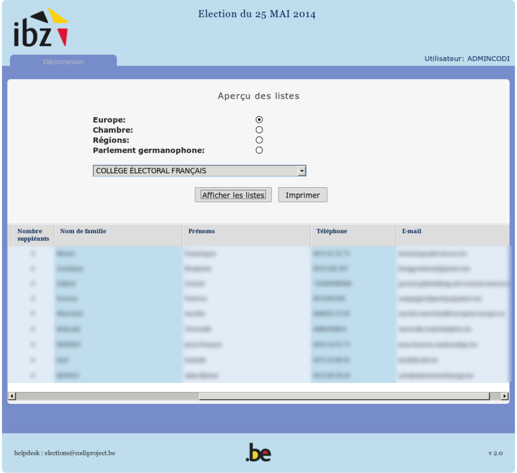


Bienvenue - Welkom
codi1web.rrn.fgov.be

Encodage de listes par les partis politiques	Web1	Invoeren van de lijsten door de politieke partijen
Encodage des personnes de contact par entité	Web1	Invullen van de contactpersonen per entiteit
Visualisation des personnes de contact par entité	Web1	Visualisatie van de contactpersonen per entiteit
Encodage des bureaux de vote par les communes	Web1	Ingeven van de stembureaus door de gemeenten
Transfert-Téléchargement de fichiers	Web1	Transfer-Downloaden van de bestanden

CODI

Election Management System



Election du 25 MAI 2014

Utilisateur: ADMINCODI

Aperçu des listes

- Europe: ●
- Chambre: ○
- Régions: ○
- Parlement germanophone: ○

COLLÈGE ÉLECTORAL FRANÇAIS

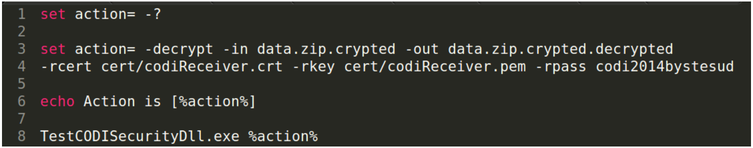
Nombre suppléants	Nom de famille	Prénoms	Téléphone	E-mail
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

helpdesk : elections@codiproject.be

v 2.0

CODI
Election Management System

Keeping your private key private

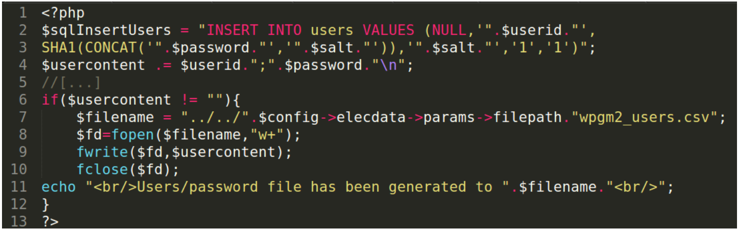


```
set action= -?

set action= -decrypt -in data.zip.crypted -out data.zip.crypted.decrypted
-rcert cert/codiReceiver.crt -rkey cert/codiReceiver.pem -rpass codi2014bystesud

echo Action is [%action%]

TestCODISecurityDll.exe %action%
```

CODI

Election Management System

Storing passwords in plaintext

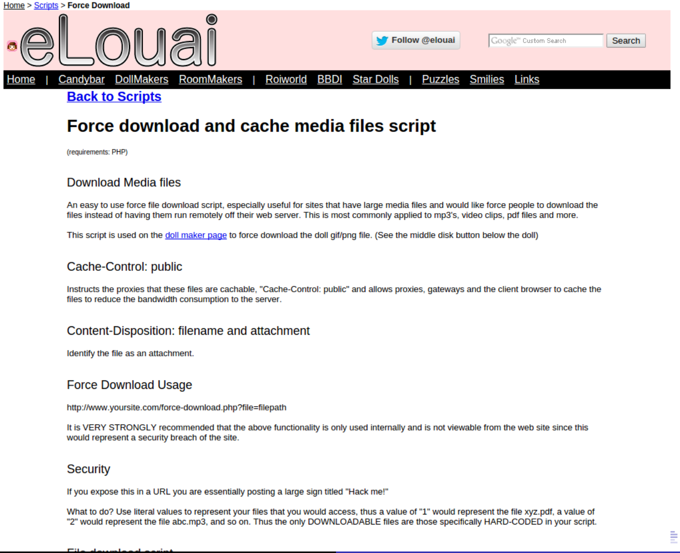


```php
<?php
$sqlInsertUsers = "INSERT INTO users VALUES (NULL,'".$userid."',
SHA1(CONCAT('".$password."','".$salt."')),'".$salt."','1','1')";
$usercontent .= $userid.";".$password."\n";
//[...]
if($usercontent != ""){
    $filename = "../../".$config->elecdata->params->filepath."wpgm2_users.csv";
    $fd=fopen($filename,"w+");
    fwrite($fd,$usercontent);
    fclose($fd);
echo "<br/>Users/password file has been generated to ".$filename."<br/>";
}
?>
```

Arbitrary file download

- discovered unauthenticated arbitrary file download on Web1
- downloaded the script itself to look at it
- ”StackOverflow copy/pasta”

Arbitrary file download


Home > Scripts > Force Download
eLouai
Follow @elouai
Google™ Custom Search
Search
Home | Candybar DollMakers RoomMakers | Roiworld BBDI Star Dolls | Puzzles Smilies Links
Back to Scripts

Force download and cache media files script

(requirements: PHP)

Download Media files

An easy to use force file download script, especially useful for sites that have large media files and would like force people to download the files instead of having them run remotely off their web server. This is most commonly applied to mp3's, video clips, pdf files and more.

This script is used on the doll maker page to force download the doll gif/png file. (See the middle disk button below the doll)

Cache-Control: public

Instructs the proxies that these files are cachable, "Cache-Control: public" and allows proxies, gateways and the client browser to cache the files to reduce the bandwidth consumption to the server.

Content-Disposition: filename and attachment

Identify the file as an attachment.

Force Download Usage

http://www.yoursite.com/force-download.php?file=filepath

It is VERY STRONGLY recommended that the above functionality is only used internally and is not viewable from the web site since this would represent a security breach of the site.

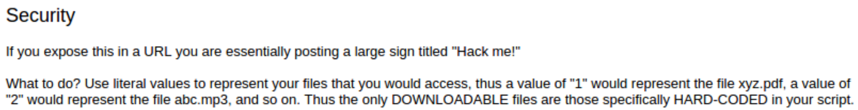
Security

If you expose this in a URL you are essentially posting a large sign titled "Hack me!"

What to do? Use literal values to represent your files that you would access, thus a value of "1" would represent the file xyz.pdf, a value of "2" would represent the file abc.mp3, and so on. Thus the only DOWNLOADABLE files are those specifically HARD-CODED in your script.

File download script

Arbitrary file download



Security

If you expose this in a URL you are essentially posting a large sign titled "Hack me!"

What to do? Use literal values to represent your files that you would access, thus a value of "1" would represent the file xyz.pdf, a value of "2" would represent the file abc.mp3, and so on. Thus the only DOWNLOADABLE files are those specifically HARD-CODED in your script.

CODI

Election Management System

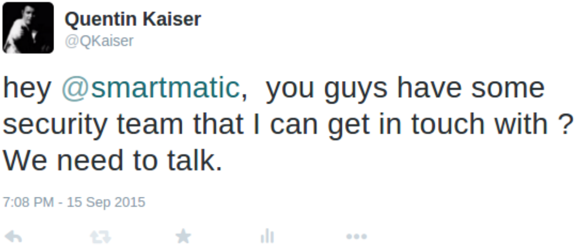
Disclosure timeline:

- 07/2014: first mail to notify Civadis about infoleak
- 07/2014: second email to notify Civadis about private keys
- 08/2014: third email to notify Civadis about arbitrary file download
- 01/09/2014: email again, this time I cc the IBZ
- 02/09/2014: answer from Civadis, I replied back explaining impact
- 03/09/2014: ”no impact, it’s a backup server”[4]
- 05/09/2014: Civadis deactivate the accounts
- 10/09/2014: Civadis shutdown those servers

[4] but it’s not, I can prove it

Smartmatic

Speaking of coordinated disclosure ...



Quentin Kaiser
@QKaiser

hey @smartmatic, you guys have some security team that I can get in touch with ? We need to talk.

7:08 PM - 15 Sep 2015

Smartmatic

Smartmatic

Smartmatic

Smartmatic provides two systems:

- **ECM** - Election Configuration Manager
- **PM-VM** - Voting machines (vote casting + ballot boxes)

Due to limited time, I only managed to look at ECM (for now).

Highlights

- 3 Ubuntu hosts running Linux 2.6.38-8-generic
- each host provided as an .iso file online
  - ECM DB (PostgreSQL)
  - ECM server (JBoss)
  - ECM client (Java client)

Getting access to those f***ing boxes

- no credentials in documentation
- no SSH
- no shell for saes (default user)

I ended up doing this:

- mount iso
- copy to get read/write access
- modify smartmatic seed file to set my own root password
- repackage iso
- install in VM, login, usual post exploitation commands

Election Configuration Manager

Well thought hardening:

- no remote access (rsh, telnet, ssh, whatever)
- file permissions are well set
- iptables config is not great, but good enough
- sudoers file limits capabilities of saes user
- security/access.conf to disable access
- no password for builtin users (e.g. postgres)
- loading of arbitrary remote classes disabled in RMI server
- access to PostgreSQL limited to whitelisted IP

Election Configuration Manager

However...

- PostgreSQL traffic is unencrypted
- No password on PostgreSQL users (ecm, postgres)

Messing with the elections in 4 steps:

1. gain physical access to network
2. ARP spoofing JBoss host and PostgreSQL host
3. connects to PostgreSQL server assuming JBoss host IP
4. dump database, gain RCE as postgres with UDF

Maybe for next year !

Conclusions

Don't believe the hype.

- CODI system was broken from day 1
- Smartmatic system also has its flaws

We need a serious audit of the Election Management System.

Q&A

Thank you for your attention. Any questions ?

References I

- Affront, *Affront analysis of 2003/2004 versions of digivote*, Affront (2004).
- D. Wagner C. Karlof, N. Sastry, *Cryptographic voting protocols: A systems perspective.*, 14th USENIX Security Symposium.
- Internet Policy Institute, *Voting systems design criteria. report of the national workshop on internet voting: Issues and research agenda.*
- Jason Kitcat Margaret MacAlpine Travis Finkenauer Drew Springall J. Alex Halderman, Harri Hursti, *Security analysis of the estonian internet voting system.*
- LaLibre.be, *Le parlement wallon se prononce en faveur de la fin du vote électronique en belgique*, 6 2015, .

References II

- Medor Mag, *Le jour où la belgique a bugué.*, 5 2015, .
- Oladiran Tayo Arulogun Olayemi Mikail Olaniyi, Adeoye Oludotun and Elijah Olusayo Omidior, *Design of secure electronic voting system using multifactor authentication and cryptographic hash functions.*, International Journal of Computer and Information Technology (2013).
- PourEVA, *Comment frauder lors d'une élection communale sans trop de connaissances informatiques ?*, 11 2006, .
- ______, *Victoire de la transparence au conseil d'etat*, 5 2011, .
- ______, *Généalogie du code source des systèmes digivote et jites*, 6 2014, .
- ______, *On vous dit tout ce que l'on sait du bug2505*, 6 2014, .