

# How not to build an electronic voting system

Quentin Kaiser

Hack.lu 2015

October 21, 2015

Quentin Kaiser  
Security Engineer | Penetration Tester

🏠 [www.quentinkaiser.be](http://www.quentinkaiser.be)

✉ [contact@quentinkaiser.be](mailto: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.

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

Elections

## La soirée électorale perturbée à cause de bugs informatiques

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



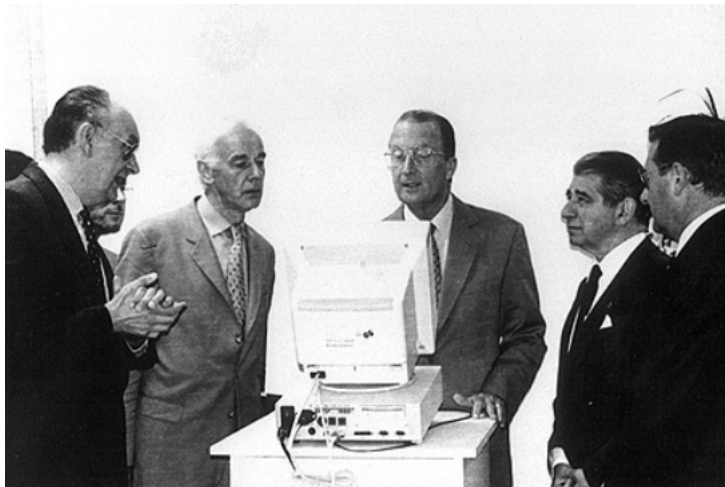
Le SPF Intérieur a décidé de suspendre provisoirement la diffusion des résultats dans plusieurs cantons électoraux en raison d'une incohérence lors de la totalisation des votes de préférence dans ces cantons.

Les résultats concernés sont ceux la Chambre et la Région dans la [circonscription de Bruxelles](#) (à l'exception des 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.

# E-voting Systems in Belgium

## Historical Background



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

# E voting Systems in Belgium

## Historical Background

- 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

Building secure voting systems is **complex**.

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



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

# CODI

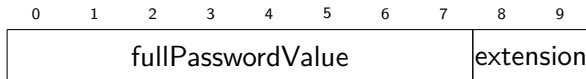
CODI encompass multiple evoting components:

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

## Authentication & Authorization

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

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



Password checksum

## Integrity Protection

- floppy disk content integrity is checked

```
1  #ifdef EL2014
2      for (i = 0; i < macResultLen ;i++)
3          if( macResult [i] != wrkspc [i +16])
4              return (0);
5      return (1);
6  #else
7      for (i = 0; i < macResultLen ;i++)
8          if( macResult [i] != wrkspc [i +16])
9              return (0);
10         else
11             return (1);
12     return (0);
13 #endif
```

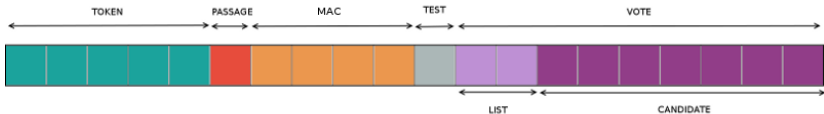
### Vote casting

- bug2505 explored by @doegox <sup>2</sup>

---

<sup>1</sup><http://www.poueva.be/spip.php?article853>

## Magnetic card layout



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

<sup>3</sup>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

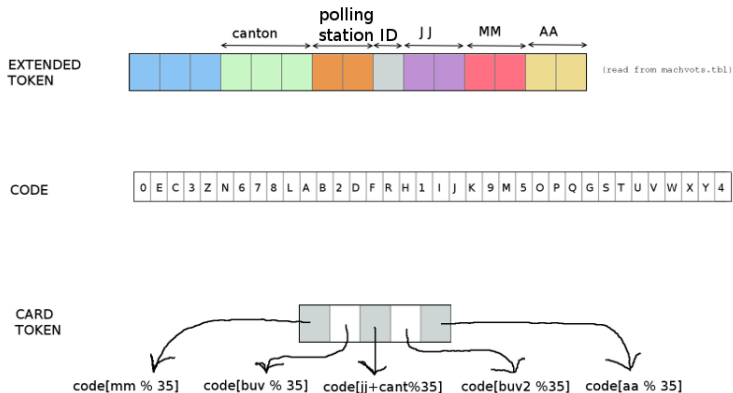
Bypassing fraud detection

## Step 1 - Byte length

# CODI - Ballot boxes

## Bypassing fraud detection

### Step 2 - Token recovery



### Step 3 - MAC key recovery

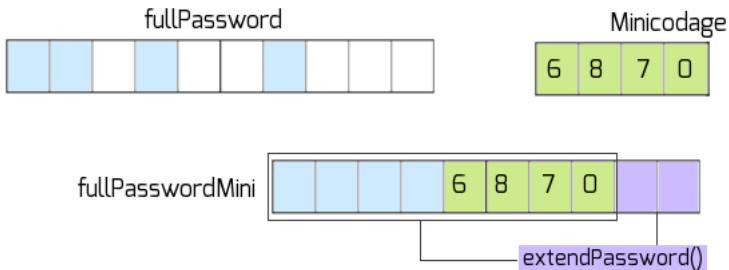
```
#ifndef EL2014
#define MINI_PwD "6987"
#define MINI_Pos "2368"
#endif

#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 questioned

```
1 void Encrypt_Decrypt(char *pzInputData, char *pzPassword, unsigned int iSize)
2 {
3     unsigned int i, iKeySize;
4     iKeySize = strlen(pzPassword);
5
6     for (i= 0; i < iSize; i++)
7     {
8         pzInputData[i] ^= pzPassword[i % iKeySize];
9     }
10    pzInputData[iSize] = 0x00;
11 }
```



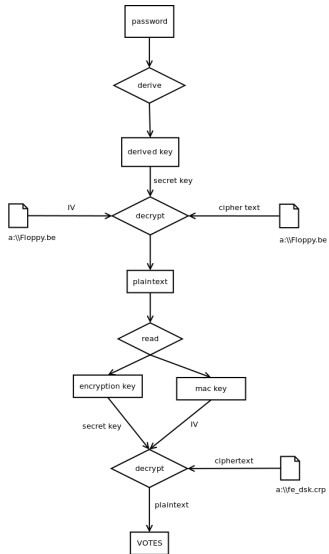
### Temporary file

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

```
1 void Generate_Password(char *pzPassword, long Position, boolean bIndic)
2 {
3     long E_Position;
4     char szPos[8];
5
6     //compute the position in the file
7     if(bIndic)
8     {
9         E_Position = (long)E_TABLE;
10        E_Position +=(long)((long)((long)C_VOTE_MAX_BYTE + 5L) * (long)Position);
11    }
12    else
13        E_Position = Position;
14
15    sprintf(szPos,"%07ld",E_Position);
16    if(szPos[0] == '-')
17        szPos[0] = '0';
18
19    pzPassword[0] = CMinipassword[0];
20    pzPassword[1] = szPos[3];
21    pzPassword[2] = CMinipassword[2];
22    pzPassword[3] = szPos[4];
23    pzPassword[4] = CMinipassword[7];
24    pzPassword[5] = szPos[5];
25    pzPassword[6] = CMinipassword[4];
26    pzPassword[7] = szPos[6];
27    pzPassword[8] = szPos[0];
28    pzPassword[9] = CMinipassword[1];
29    pzPassword[10] = CMinipassword[3];
30    pzPassword[11] = szPos[2];
31    pzPassword[12] = CMinipassword[6];
32    pzPassword[13] = szPos[1];
33    pzPassword[14] = CMinipassword[5];
34    pzPassword[15] = 0x00;
35 }
```

# 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:

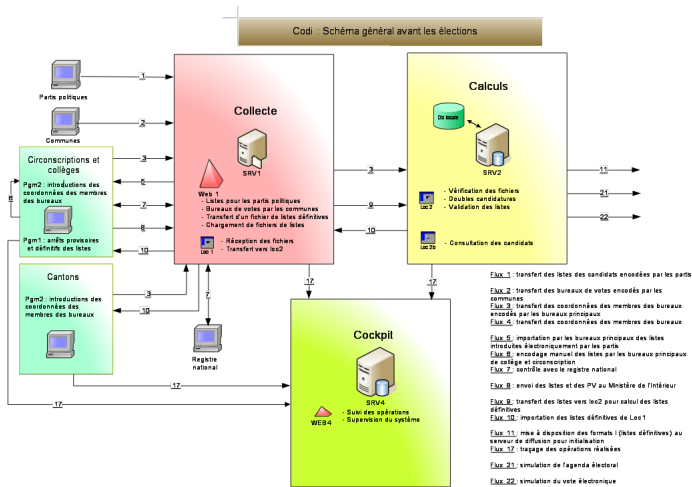
- generate minutes as PDF file
- PDF file signed with polling station president eID
- encode votes into undocumented "Format F" format
- minutes PDF + "Format F" content sent to central server

```
$ 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

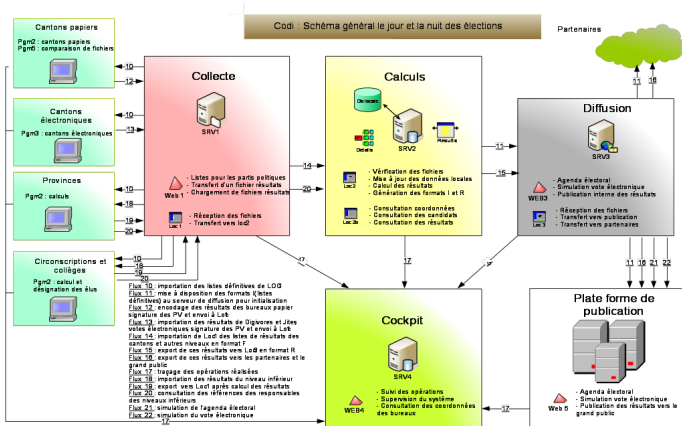
# CODI

## Secure Vote Transmission



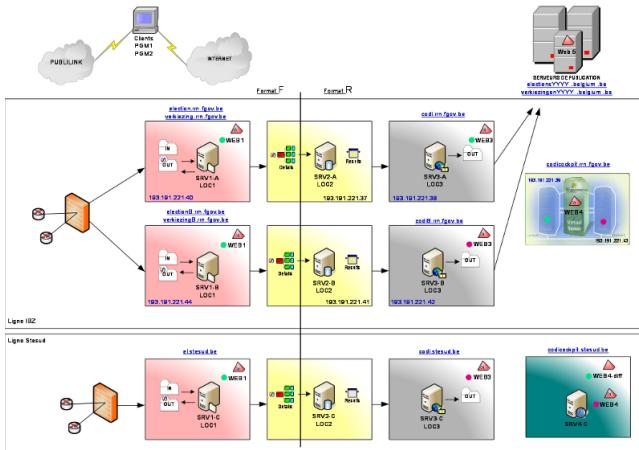
# CODI

## Secure Vote Transmission



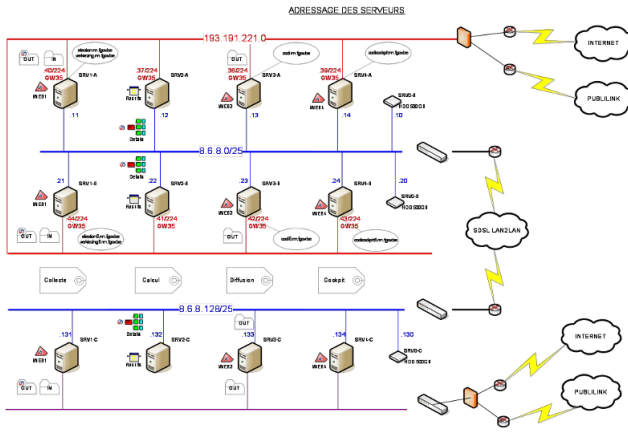
# CODI

## Secure Vote Transmission

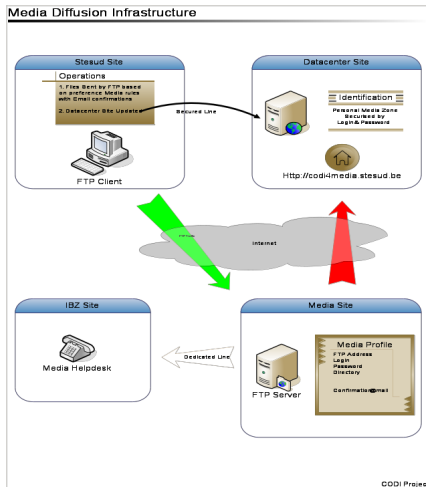


# CODI

## Secure Vote Transmission

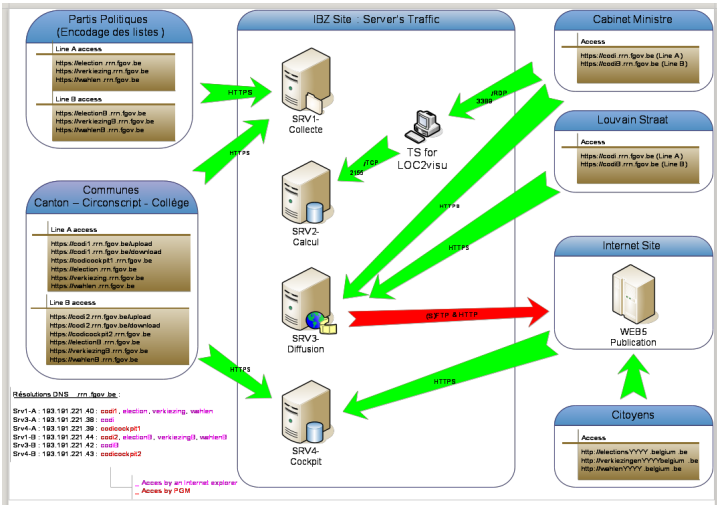






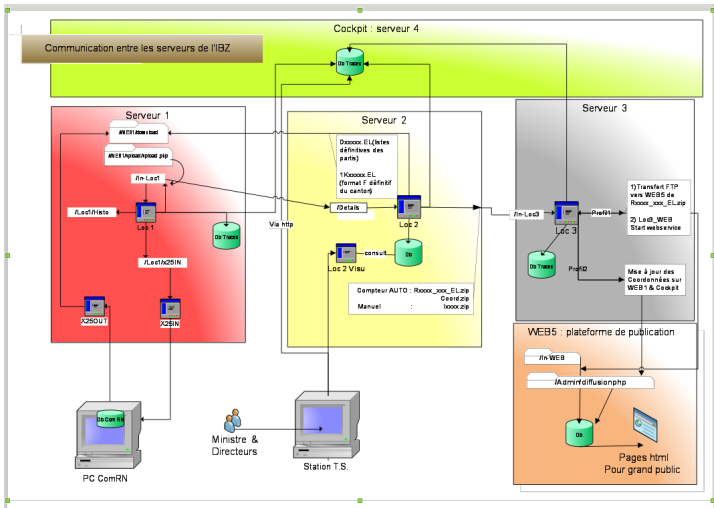
# CODI

## Secure Vote Transmission



# CODI

## Secure Vote Transmission



aka OWASP Top 10

- Web1 : encoding of lists, candidates, polling stations, ...
- **Web2 : used by belgian embassies 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

```
1 <?php
2 // User creation
3 $usersAdmin = array(
4     array("usr"=>"ADMINCODI", "psw"=> "84322640"),
5     array("usr"=>"DIRGEN", "psw"=> "38165024")
6 );
7 ?>
```



The screenshot shows the CODI Election Management System interface for the 2014 election. The header includes the 'ibz' logo, the text 'Election du 25 MAI 2014', and the user name 'Utilisateur: ADMINCODI'. The main content area is titled 'Aperçu des listes' and contains several radio buttons for selection: 'Europe:', 'Chambre:', 'Régions:', and 'Parlement germanophone:'. A dropdown menu is set to 'COLLÈGE ELECTORAL FRANÇAIS'. Below these are buttons for 'Afficher les listes' and 'Imprimer'. A table with five columns is displayed: 'Nombre suppléants', 'Nom de famille', 'Prénoms', 'Téléphone', and 'Email'. The table contains several rows of data, though the text is somewhat blurred. At the bottom of the interface, there is a footer with the contact information 'helpdesk : elections@codiproject.be', the 'be' logo, and the version number 'v 2.0'.



### Keeping your private key private

```
1 set action= -?  
2  
3 set action= -decrypt -in data.zip.crypted -out data.zip.crypted.decrypted  
4 -rcert cert/codiReceiver.crt -rkey cert/codiReceiver.pem -rpass codi2014bystesud  
5  
6 echo Action is [%action%]  
7  
8 TestCODISecurityDll.exe %action%
```

## Storing passwords in plaintext

```
1 <?php
2 $sqlInsertUsers = "INSERT INTO users VALUES (NULL, '$userid.',
3 SHA1(CONCAT('$password.', '$salt.')), '$salt.', '1', '1')";
4 $usercontent .= $userid."; '$password.'" . "\n";
5 // [...]
6 if($usercontent != ""){
7     $filename = "../.." . $config->elecdata->params->filepath . "wpgm2_users.csv";
8     $fd=fopen($filename, "w+");
9     fwrite($fd, $usercontent);
10    fclose($fd);
11    echo "<br/>Users/password file has been generated to ".$filename."<br/>";
12 }
13 ?>
```

### 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



[Follow @elouai](#)

[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.

## 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.

## 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"<sup>4</sup>
- 05/09/2014: Civadis deactivate the accounts
- 10/09/2014: Civadis shutdown those servers

---

<sup>4</sup>but it's not, I can prove it

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 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

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

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 !






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.**

Thank you for your attention. Any questions ?



-  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, .

-  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'état*, 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, .