Technical and Socio-technical Attacks on the Danish Party Endorsement System

Carsten Schürmann and Alessandro Bruni

Center for Information Research and Trust
IT University of Copenhagen

May 23, 2019

Paper Endorsements before 2016

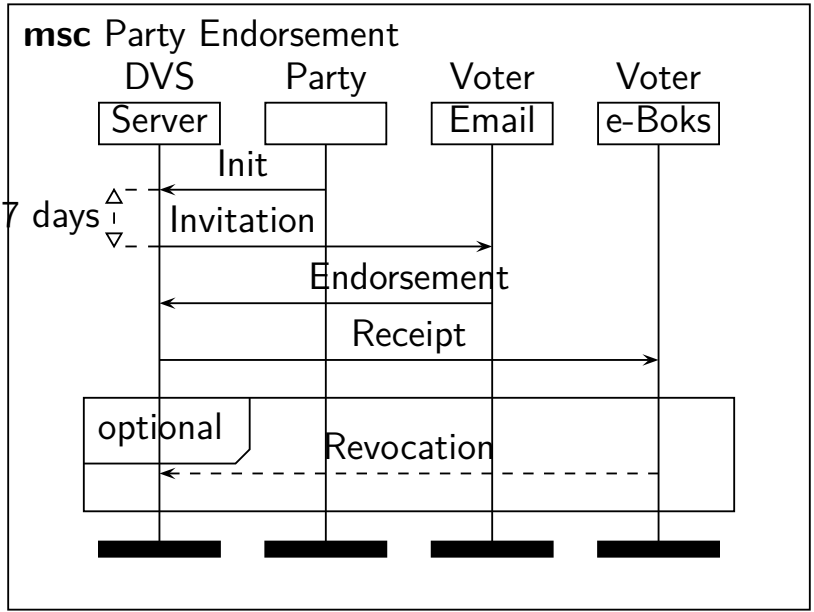
The Updated Legal Framework

Law Change, March 2014

- Allowed for the use of a digital online system.

Administrative Regulation, January 2016

- New technology: database of endorsements
- New roles: Party Administrator
- Technical jargon: “send email”, “a voters’ declarations’ key”
- No mention of *security*, *verifiability* or *accountability*
- Builds on existing services: NemID, e-Boks


msc Party Endorsement
DVS
Party
Voter
Voter
Server
Email
e-Boks
Init
7 days
Invitation
Endorsement
Receipt
optional
Revocation

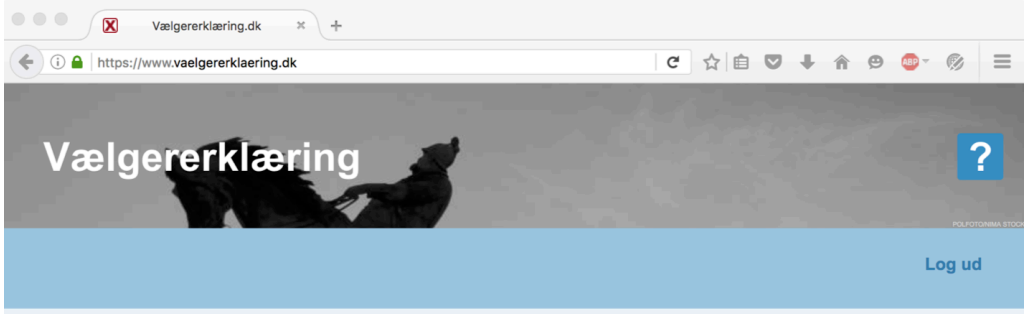

Vælgererklæring.dk
https://www.vaelgererklaering.dk
Vælgererklæring
?
Log ud
Velkommen til vælgererklæring.dk
Velkommen til vælgererklæring.dk
Social- og Indenrigsministeriet har ansvar for vælgererklæring.dk, som er en løsning, der understøtter nye partiers indsamling af vælgererklæringer til at kunne opstille til enten folketingsvalg eller Europa-Parlamentsvalg.
Hvis du ønsker at støtte et nyt partis opstilling til folketingsvalg eller Europa-Parlamentsvalg, skal du kontakte partiet.
Partiet skal bruge din e-mailadresse (eller CPR-nummer,
Login for partier og ministeriet
Hvis du er bruger af vælgererklæring.dk kan du logge ind her:
Parti
Log på
For at blive

Table of Contents

A Technical Attack

Interaction with the Ministry

Task

- We were asked (allowed) to endorse a test party
- Aka client security analysis

Non-Task

We were *not* asked to

- Conduct a rigorous security analysis of the system
- Review requirements and design documents
- Review the implementation

Fra: noreply@vaelgererklaering.dk
Dato: 3. august 2016 kl. 02.02.27 CEST
Til: [redacted]@gmail.com
Emne: Link til at afgive vælgererklæring

Social- og Indenrigsministeriet

Kære [redacted]@gmail.com

Du har tilkendegivet at ville afgive en vælgererklæring til et parti, der søger at blive opstillingsberettiget til Folketingsvalg

For at afgive din vælgererklæring til partiet skal du klikke på linket nedenfor. Hvis linket ikke er klikbart, skal du kopiere det og indsætte det i adresselinjen (øverst) i browseren. Vil du alligevel ikke afgive en vælgererklæring til partiet, eller har du ikke selv oplyst din e-mailadresse, kan du benytte linket til at trække støttetilkendegivelsen tilbage og få slettet oplysningerne om dig. Benytter du ikke linket inden datoen nedenfor, vil alle oplysninger om dig automatisk blive slettet. Ønsker du herefter at afgive en vælgererklæring, skal du henvende dig til det parti, som du vil støtte.

Klik på linket for at komme til den hjemmeside, hvor du kan afgive en vælgererklæring:

https://www.vaelgererklaering.dk/apos2/eve/vaelger?uuid=2c4e0be1-60b9-4a60-9c98-5f5d0890cb48

Linket er aktivt til-og-med 30/08/2016

Venlig hilsen
Social- og Indenrigsministeriet

Technical Aspects of the Attack

Observe and Learn

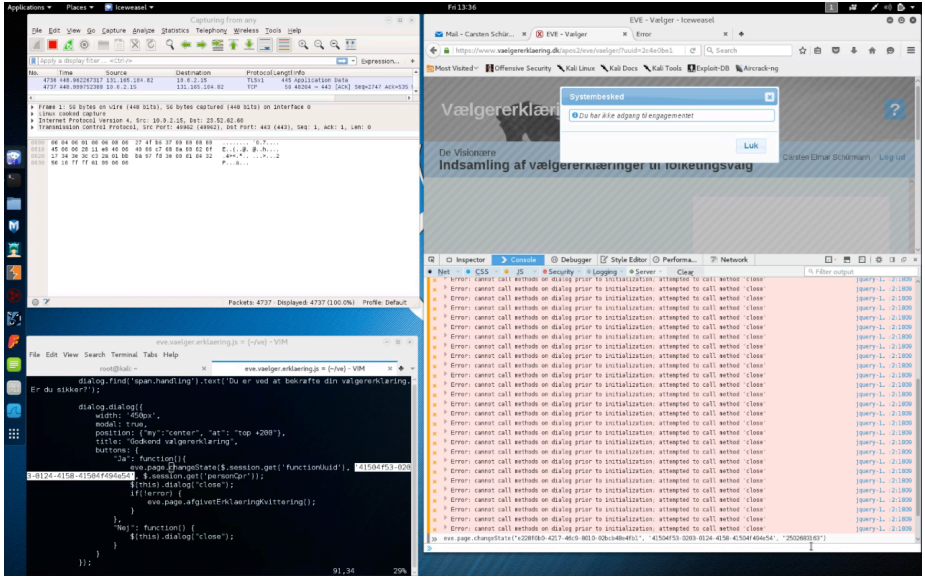
We observe the network traffic between

- the server (hosted by the vendor) and
- the client (running on my laptop)

We learn structure, identifiers, names, session cookies, cryptographic keys, etc.

Compose and Inject

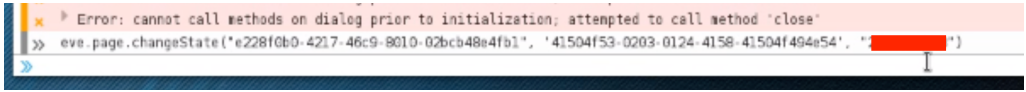
From what we have learned, we compose new messages and inject them into the network traffic between client and server


Applications
Places
Iceweasel
Fri 13:36
Capturing from any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
4738 440.062267317 131.165.164.82 10.6.2.15 TLSv1 445 Application Data
4737 440.099752988 10.6.2.15 131.165.164.82 TCP 56 48204 > 443 [ACK] Seq=2747 Ack=535
Frame 1: 56 bytes on wire (448 bits), 56 bytes captured (448 bits) on interface 0
Linux cooked capture
Internet Protocol Version 4, Src: 10.9.2.15, Dst: 23.62.62.60
Transmission Control Protocol, Src Port: 49962 (49962), Dst Port: 443 (443), Seq: 1, Ack: 1, Len: 0
Packets: 4737 · Displayed: 4737 (100.0%) Profile: Default
eve.vaelger.erklaering.js = (~/vve) - VIM
File Edit View Search Terminal Tabs Help
root@kali: ~
eve.vaelger.erklaering.js = (~/vve) - VIM
dialog.find('span.handling').text('Du er ved at bekræfte din valgerklæring.
Er du sikker?');
dialog.dialog({
width: '450px',
modal: true,
position: {"my":"center", "at": "top +200"},
title: 'Godkend valgerklæring',
buttons: {
"Ja": function(){
eve.page.changeState($.session.get('functionUuid'), '41504f53-020
3-8124-4158-4158d4f494e54', $.session.get('personCpr'));
$(this).dialog("close");
if(!error) {
eve.page.afgivetErklaeringKvittering();
}
},
"Nej": function() {
$(this).dialog("close");
}
}
});
91,34 29%
EVE - Vælger - Iceweasel
Mail - Carsten Schür...
EVE - Vælger
Error
https://www.vaelgererklaering.dk/apos2/eve/vaelger/?uuid=2c4e0be1
Search
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit-DB
Aircrack-ng
Vælgererklæri
Systembesked
Du har ikke adgang til engagementet
Luk
De Visionære
Indsamling af vælgererklæringer til folketingsvalg
Carsten Elmar Schürmann · Log ud
Inspector
Console
Debugger
Style Editor
Performa...
Network
Net
CSS
JS
Security
Logging
Server
Clear
Filter output
Error: cannot call methods on dialog prior to initialization; attempted to call method 'close'
jquery-1. :2:1809
eve.page.changeState('e328f0b0-4217-46c9-8010-02bcb48b4fb1', '41504f53-0203-0124-4158-4158d4f494e54', '2502603163')

```
page.find('a.button').bind('click', function(e){
$.ajax({
success: function(xml){
  if($(xml).find('respMsg').attr('resp')
     == "success"){
    eve.page.confirmAfgivErklaering();
  } else if($(xml).find('respMsg').attr('resp')
     == "dobbelterklaering"){
    $.session.set('afvistGrund', 'dobbelt');
    eve.page.afvistErklaeringKvittering();
  } else if($(xml).find('respMsg').attr('resp')
     == "valgret"){
    $.session.set('afvistGrund', 'mangledeValgret');
    eve.page.afvistErklaeringKvittering();
```

```
confirmAfgivErklaering: function(){
  var dialog = $('#confirm_dialog');
  dialog.dialog({
    buttons: {
      "Ja": function(){
        eve.page.changeState(
          $.session.get('functionUuid'),
          '41504f53-0203-0124-4158-41504f494e54',
          $.session.get('personCpr'));
        $(this).dialog("close");
        if(!error) {
          eve.page.afgivetErklaeringKvittering();
        }
      },
```

Firefox Developer Tools Console ...



~~Social- og~~ Indenrigsministeriet
Holmens Kanal 22
1060 København

Carsten Elmar Schürmann
Ribegade 19,st th
2100 København Ø

Social- og Indenrigsministeriet

Journalnøgle
2c4e0be1-60b9-4a60-9c98-5f5d0890cb48

Dato
12. august 2016

Kvittering for afgivelse af vælgererklæring

Du har nu afgivet vælgererklæring til partiet:

De Visionære
Prins Jørgens Gård 1
1218 København K
Tlf.: 22460608
Www.Visionaer.dk

Din vælgererklæring er gyldig i 18 måneder fra datoen for afgivelsen. Du kan ikke afgive vælgererklæring til støtte for et andet partis opstilling til folketingsvalg, så længe vælgererklæringen er gyldig. Når gyldigheden udløber, slettes din vælgererklæring og alle øvrige oplysninger om din afgivelse af vælgererklæring automatisk i den digitale løsning. Du kan dog trække din vælgererklæring tilbage via nedenstående link, hvis du ikke længere ønsker at deltage i anmeldelse af partiet, eller hvis du ønsker at afgive vælgererklæring til et andet parti. Har partiet allerede anmeldt sig for social- og indenrigsministeren, kan du dog ikke trække din vælgererklæring tilbage. Anmeldelsen af et parti er gyldig indtil førstkommende folketingsvalg, dog mindst 18 måneder. Herefter kan du igen frit afgive vælgererklæring til et parti.

Klik på linket for at komme til vælgererklæring.dk, hvis du ønker at trække din vælgererklæring tilbage:

https://www.vaelgererklaering.dk/apos2/eve/vaelger?uuid=2c4e0be1-60b9-4a60-9c98-5f5d0890cb48

Linket er aktivt til og med 3. februar 2018.

Venlig hilsen
Social- og Indenrigsministeriet

4695011

Summary of the Attack

Important

- We did not break into/penetrate any server
- Everyone can launch this attack
- There is no evidence to go after us
- Threat against public confidence in the election

Summary of the Attack

Important

- We did not break into/penetrate any server
- Everyone can launch this attack
- There is no evidence to go after us
- Threat against public confidence in the election

December 2016

- Ministry informs that the vulnerability has been fixed
- Undisclosed security review report exists
- No further technical interaction with the ministry

A Socio-technical Attack

Party Endorsement Tokens

Fra: noreply@vaelgererklaering.dk
Dato: 3. august 2016 kl. 02.02.27 CEST
Til: [redacted]@gmail.com
Emne: Link til at afgive vælgererklæring

Social- og Indenrigsministeriet

Kære [redacted]@gmail.com

Du har tilkendegivet at ville afgive en vælgererklæring til et parti, der søger at blive opstillingsberettiget til Folketingsvalg

For at afgive din vælgererklæring til partiet skal du klikke på linket nedenfor. Hvis linket ikke er klikbart, skal du kopiere det og indsætte det i adresselinjen (øverst) i browseren. Vil du alligevel ikke afgive en vælgererklæring til partiet, eller har du ikke selv oplyst din e-mailadresse, kan du benytte linket til at trække støttetilkendegivelsen tilbage og få slettet oplysningerne om dig. Benytter du ikke linket inden datoen nedenfor, vil alle oplysninger om dig automatisk blive slettet. Ønsker du herefter at afgive en vælgererklæring, skal du henvende dig til det parti, som du vil støtte.

Klik på linket for at komme til den hjemmeside, hvor du kan afgive en vælgererklæring:

https://www.vaelgererklaering.dk/apos2/eve/vaelger?uuid=2c4e0be1-60b9-4a60-9c98-5f5d0890cb48

Linket er aktivt til-og-med 30/08/2016

Venlig hilsen
Social- og Indenrigsministeriet

Socio-technical Vulnerability

A (Potential) Attack

- Tokens are not linked to the identity of the endorser
- The Party Administrator generates n tokens (sent to an email address under the administrator's control)
- The Party Administrator forwards the tokens to potential endorsers on a by need basis, circumventing the 7 day rule!
- The endorsers can be coerced to endorse on the spot

Socio-political Implications

Summary: Database has no integrity

- May contain endorsements from ineligible endorser
- May contain coerced endorsements

Summary: Database has no integrity

- May contain endorsements from ineligible endorser
- May contain coerced endorsements

Warnings ignored

Paper ballots added to the database

Summary: Database has no integrity

- May contain endorsements from ineligible endorser
- May contain coerced endorsements

Warnings ignored

Paper ballots added to the database

Decisions made

- Nye Borgelige: Approved (Oct 6, 2016)
- Nationalpartiet: Declined (Fall 2016)
- Klaus Riskær Pedersen: Approved (Feb 27, 2019)
- Stram Kurs: Approved (May 6, 2019)

Responsible Disclosure

Time line of events

Aug 3, 2016 DemTech receives an endorsement token

Aug 12, 2016 Discovery of the technical flaw

Aug 25, 2016 Ministry asked for findings

Sep 14, 2016 Presented a talk at the ministry

Sep 27, 2016 Offered help

Oct 25, 2016 Invited vendor to ITU

Dec 19, 2016 The technical vulnerability fixed

Spring 2019 Ministry under public scrutiny

Jul 30, 2019 Newspaper article on our findings published

Conclusion

Take-away messages

- Collecting party endorsements $\approx$ collecting votes
- Legal and technical framework must be revisited
- Different people in the ministry have different objectives

Currently ongoing

- A new law proposal is currently in hearing
- A new party endorsement system will be build