E-Voting Remote (unsupervised)

Protocol Enhancements

Multi Secret Management

Usability Studies

Secure Platform
E-Voting Remote (unsupervised)

Usability
How the f*ck does it work? What am I supposed to do here?

Efficiency
Will there ever be a result?

Secure-Platform
"All your data are belong to us" (sic.)

Correctness
My neighbour had the NSA vote instead?!

Coercion Resistance
We know your kid’s location... vote ‘yes’ and all is well!

Everlasting Privacy
Your family is punished as your grandfather voted ‘yes’!

E2E-Verifiability
I do not have a clue if my intention made it to the final tally!"
Usability
How the f*ç@ does it work? What am I supposed to do here?
Efficiency

Will there ever be a result?
Secure-Platform
"All your data are belong to us" (sic.)
Correctness
My neighbour had the NSA vote instead?!
Coercion Resistance
We know your kid's location... vote 'yes' and all is well!
Everlasting Privacy
Your family is punished as your grandfather voted 'yes'!
E2E-Verifiability

I do not have a clue if my intention made it to the final tally?!
E-Voting Remote
(unsupervised)

Usability
How the f*ck does it work? What am I supposed to do here?

Efficiency
Will there ever be a result?

Secure-Platform
"All your data are belong to us" (sic.)

Correctness
My neighbour had the NSA vote instead?!

Coercion Resistance
We know your kid's location... vote 'yes' and all is well!

Everlasting Privacy
Your family is punished as your grandfather voted 'yes'!

E2E-Verifiability
I do not have a clue if my intention made it to the final tally?!
E-Voting Remote (unsupervised)

Usability
How the UI/UX does it work? What am I supposed to do here?

Efficiency
Will there ever be a return?

Scalability
All your data are being stored (yes)

Correctness
My neighbor had the NFA vote instead!

Disenfranchisement
We know your vote location, vote yes and all is well.

Correcting Privacy
Your history is followed as your grandchild voted yes!

GSS/Verifiability
I do not have a clue if my intention made it to the final tally!

Protocol Enhancements

Multi Secret Management
User must be able to:
... manage multiple, usable secrets (by password)
... hide the true amount of credentials (plagiarism)
... having access to the surrender (from multiplication)

Secure Platform

Usability Studies
Protocol Enhancements

Voter casts with genuine intention

Real ballot \((A_1, B, \pi) | A_1 = \text{Enc}_G(\sigma_0, r_1), B = \text{Enc}_K(v, r'_1), \pi = zkp(r_1, r'_1 : A_1, B)\)

Simulated ballot \((A_2, B, \pi) | A_2 = \text{Enc}_G(\tau_1, r_2), B = \text{Enc}_K(v, r'_2), \pi = zkp(r_2, r'_2 : A_2, B)\)

Voter casts with genuine intention

Duplicate ballot \((A_3, B, \pi) | A_3 = \text{Enc}_G(\sigma_3, r_3)\)

Unintended voter error

Credential stolen \(\rightarrow\) Attack

Voter / Someone casts

Invalid ballot \((A_4, B, \pi) | A_4 = \text{Enc}_G(x, r_4)\)

Unintended voter error

Voter cannot remember

Board Flooding \(\rightarrow\) Attack

JCJ-05

Damned \(\rightarrow\) Covias

KHF-11
Voter casts with genuine intention

Real ballot \( (A_1, B, \pi) \mid A_1 = Enc_y(\sigma_a, r_1), B = Enc'_y(v, r_1'), \pi = zkp(r_1, r_1' : A_1, B) \)
Voter casts with genuine intention

Real ballot \( (A_1, B, \pi) | A_1 = Enc_y(\sigma_a, r_1), B = Enc'_y(v, r'_1), \pi = zkp(r_1, r'_1 : A_1, B) \)

Simulated ballot \( (A_2, B, \pi) | A_2 = Enc_y(\tau_{a_\alpha}, r_2), B = Enc'_y(v, r'_2), \pi = zkp(r_2, r'_2 : A_2, B) \)
Voter casts with genuine intention

Duplicate ballot \((A_3, B, \pi)\) \(A_3 = Enc_y(\sigma_a, r_3)\)
Voter casts with genuine intention

Duplicate ballot \((A_3, B, \pi) | A_3 = Enc_y(\sigma_a, r_3)\)

Unintended voter error
Credentialed stolen \(\rightarrow\) Attack
(A, B, π) \rightarrow \text{Duplicate Cred. Elimination}

\begin{align*}
\sigma_a & \quad A_1 = \text{Enc}_y(\sigma_a, r_1) \\
\sigma_a & \quad A_2 = \text{Enc}_y(\sigma_a, r_2) \\
\sigma_b & \quad A_3 = \text{Enc}_y(\sigma_b, r_3) \\
\sigma_c & \quad A_4 = \text{Enc}_y(\sigma_c, r_4) \\
\end{align*}

A^z_1 = \prod\{A^z_1, A^z_2, \ldots, A^z_m\} \\
A^z_2 = \prod\{A^z_1, A^z_2, \ldots, A^z_m\} \\
A^z_3 = \prod\{A^z_1, A^z_2, \ldots, A^z_m\} \\
A^z_4 = \prod\{A^z_1, A^z_2, \ldots, A^z_m\}

\begin{align*}
\sigma^z_a = \text{Dec}_x(A^z_1) & \quad \sigma^z_a \\
\sigma^z_b = \text{Dec}_x(A^z_2) & \quad \sigma^z_b \\
\sigma^z_c = \text{Dec}_x(A^z_3) & \quad \sigma^z_c \\
\end{align*}

\text{Distributed } z \\
\text{Distributed } x \\
\text{Talliers}
\((\sigma, T)\) 

\((A, B, \pi)\) 

Voter 

Voting Phase 

Duplicate Cred. 

Elimination
Voter / Someone casts
Invalid ballot \((A_4, B, \pi)|A_4 = Enc_y(\chi, r_4)\)
Voter / Someone casts

Invalid ballot \((A_4, B, \pi)|A_4 = Enc_y(x, r_4)\)

- Unintended voter error
- Voter cannot remember
- Board Flooding -> Attack
Voter

$(A, B, \pi)$

Invalid Cred. Elimination

\[
\begin{align*}
U_{1}^z &= \prod \{ U_{1}^{z1}, U_{i}^{z}, U_{1}^{zm} \} \\
U_{z} &= \prod \{ U_{z1}, U_{\ldots}, U_{zm} \} \\
U_{u} &= \prod \{ U_{u1}, U_{u}, U_{u}^{zm} \} \\
\sigma_{a}^{z} &= Dec_x(U_{1}^{z}) \\
\ldots z &= Dec_x(U_{\ldots}^{z}) \\
\tau_{q}^{z} &= Dec_x(U_{u}^{z}) \\
\end{align*}
\]

\[
\begin{align*}
A_{1}^z &= \prod \{ A_{1}^{z1}, A_{i}^{z}, A_{1}^{zm} \} \\
\chi_{z} &= Dec_x(A_{1}^{z})
\end{align*}
\]

Distributed $z$

Distributed $x$

Talliers

$A_i = Enc_y(\chi, r_1)$
Simulation Elimination

\[ S_1' = \prod \{ S_1^{z_1'}, S_1^{z_2'}, ..., S_1^{z_m'} \} \]
\[ S_z' = \prod \{ S_z^{z_1'}, S_z^{z_2'}, ..., S_z^{z_m'} \} \]
\[ S_u' = \prod \{ S_u^{z_1'}, S_u^{z_2'}, ..., S_u^{z_m'} \} \]

\[ \sigma_{a'} = \text{Dec}_x(S_1^{z'}) \quad \sigma_n^{z'} \]

\[ \hat{A}_1' = \prod \{ \hat{A}_1^{z_1'}, \hat{A}_1^{z_2'}, ..., \hat{A}_1^{z_m'} \} \]
\[ \hat{A}_2' = \prod \{ \hat{A}_2^{z_1'}, \hat{A}_2^{z_2'}, ..., \hat{A}_2^{z_m'} \} \]
\[ \hat{A}_3' = \prod \{ \hat{A}_3^{z_1'}, \hat{A}_3^{z_2'}, ..., \hat{A}_3^{z_m'} \} \]
\[ \hat{A}_4' = \prod \{ \hat{A}_4^{z_1'}, \hat{A}_4^{z_2'}, ..., \hat{A}_4^{z_m'} \} \]

\[ \sigma_{a'} = \text{Dec}_x(\hat{A}_1^{z'}) \quad \sigma_n^{z'} \]

\[ \tau_e^{z'} = \text{Dec}_x(\hat{A}_3^{z'}) \quad \tau_q^{z'} \]

\[ \mathcal{B}_4 \]

Distributed \( z' \)

Distributed \( x \)

Talliers
E-Voting Remote
(unsupervised)

Usability
How does it work? What am I supposed to do here?

Efficiency
Will there ever be a recall?

Security/Platform
All your data are going to us (and)?

Correctness
The nearest node has the media vote instead?

Coercion Resistance
We know your kid's location... vote yes and all is well.

Compacting Privacy
Your family is punished as your grandfather voted yes?

End/Verifiable
I do not have a clue if my intention made it to the final tally?

Protocol Enhancements

Multi Secret Management

Secure Platform

Usability Studies
Usability Studies
Volksinitiative «Schutz vor Passivrauchen»

Wollen Sie die Volksinitiative «Schutz vor Passivrauchen» annehmen?

Yes
No
Uncompleted ballot
Usability Studies
E-Voting Remote (unsupervised)

Protocol Enhancements

Multi Secret Management

Usability Studies

Secure Platform
Multi Secret Management

Voter must be able to...

..... manage multiple credentials seamlessly (no search)
..... hide the true amount of credentials (chaffing)
..... having access to the credentials (non-challengeable)
Multi Secret Management

Voter must be able to...

.... manage multiple credentials seamlessly (no search)
.... hide the true amount of credentials (chaffing)
.... having access to the credentials (non-challengeable)
\[ c = \sum_{i=0}^{\left| K \right|+\left| R \right|-1} a_i x^i \]
\[ c = \sum_{i=0}^{\pm |K| + |R| - 1} a_i x^i \]

\[ \mathbb{Z}_p \]
\[ c = \sum_{i=0}^{\|K\|+|R|-1} a_i x^i \mod p \]
Multi Secret Management

Voter must be able to...

..... manage multiple credentials seamlessly (no search)
..... hide the true amount of credentials (chaffing)
..... having access to the credentials (non-challengeable)
E-Voting Remote (unsupervised)

Protocol Enhancements

Multi Secret Management

Usability Studies

Secure Platform
Secure Platform

The Secure Platform Module must
... be restricted in its usage (finite state machine / software close)
... provide trust (analyzable down to the metal by 'experts')
... indicate tampering
... make the calculation for the cryptographic aspects
... make the calculation of the E2E-verification aspects
... provide entropy to the rest of us (not to the user)
... intuitive to use
... easily replacable (no secrets within)
Secure Platform

The Secure Platform Module must
... be restricted in its usage (finite state machine / software close)
... provide trust (analyzable down to the metal by 'experts')
... indicate tampering
... make the calculation for the cryptographic aspects
... make the calculation of the E2E-verification aspects
... provide entropy to the rest of us (not to the user)
... intuitive to use
... easily replacable (no secrets within)
Secure Platform

The Secure Platform Module must
... be restricted in its usage (finite state machine / software close)
... provide trust (analyzable down to the metal by 'experts')
... indicate tampering
... make the calculation for the cryptographic aspects
... make the calculation of the E2E-verification aspects
... provide entropy to the rest of us (not to the user)
... intuitive to use
... easily replacable (no secrets within)
Secure Platform

The Secure Platform Module must
... be restricted in its usage (finite state machine / software close)
... provide trust (analyzable down to the metal by 'experts')
... indicate tampering
... make the calculation for the cryptographic aspects
... make the calculation of the E2E-verification aspects
... provide entropy to the rest of us (not to the user)
... intuitive to use
... easily replacable (no secrets within)
E-Voting Remote (unsupervised)

Protocol Enhancements

Multi Secret Management

Usability Studies

Secure Platform