Response to the inaccuracies in the report by the US Vote Foundation and Galois Inc.

THE FUTURE OF VOTING END-TO-END VERIFIABLE INTERNET VOTING -- SPECIFICATION AND FEASIBILITY ASSESSMENT STUDY

David Galindo, Jordi Puiggali, July 2015

The US Vote Foundation has recently published the report "The future of voting end-to-end verifiable internet voting -- specification and feasibility assessment study" (hereafter called the Report). The Report evaluates, in detail, the SoA including technology implemented by different vendors and worldwide experiences of Internet voting that included E2E verifiability in their voting systems. The Report, written by Galois Inc., is a deliverable for a project run by the US Vote Foundation aimed at evaluating the requirements for introducing Internet Voting in the US.

We find that the Report, in its current form, is biased and incorrectly reflects (inaccuracies and significant omissions of key information) several properties of the Norwegian electronic voting system that are in-line with those that an E2E-VIV system should, and in this case, do satisfy. In benefit of public interest, it would be necessary to fix these inaccuracies and biased views in a future release of the Report.

When the research process for this report started, Scytl proactively approached the authors and the US Vote Foundation, offering our willingness to collaborate in ensuring an accurate and detailed report, by providing not only feedback on the experiences Scytl participated in, but providing detailed information on all projects. No members of US Vote Foundation or research participants replied to our query or requested any additional information or clarification about our research, technology or projects related to E2E verifiability for Internet voting.

Upon our review of the report, we have identified a series of inaccurate statements and information published in the report relative to online voting projects and technology implemented by Scytl. In an effort to provide a more accurate analysis, detailed below is an overview of the omitted publically available information and a clarification of the inaccurate statements that can help ensure an accurate report.

In the aforementioned report, Chapter 3.3 delves into a study of the end-to-end verifiability features of several electronic voting protocols, including Helios (Section 3.3.6 of the report) and the Norwegian Protocol (Section 3.3.7 of the report), the latter having been implemented by Scytl in 2011-2013. We hereby contest the inaccuracies that are included in this report with respect to the Norwegian system, which remains one of the most comprehensive and transparent online voting experiences – still to be surpassed - deployed for an Internet-based government binding election.

All quotes below refer to Section 3.3.7, page 25 of the report and have been placed between brackets; our response follows each of these bracketed quotes pulled from the Report.

– *"Available descriptions of the Norwegian system are incomplete, so it is not possible to analyze the system in depth."*

  Incorrect and biased.. In reality, and in an effort to provide maximum transparency, the Norwegian government made a strategic and unrivaled transparency effort and published all relevant documentation related to the project on the Ministry of Local Government and Modernisation (KRD) website. Some highlighted material includes:

- Tenders documents including the final proposals of the finalists of the bidding process, the evaluation criteria used for the different requirements setup by the government, the ranking achieved by each vendor on each of the requirements.
    - https://www.regjeringen.no/en/dep/kmd/prosjekter/e-vote-trial/source-code/specification-tenders-evaluation-and-con/id612121/
- Technical documentation of the voting system provided following the Common Criteria framework EAL 4 as reference. The documentation (a set of 15 documents) included the Target of Evaluation (ToE) definition of the different system components (EMS, voting and counting), the system architecture, security architecture, as well as risk assessments of the system.
    - https://www.regjeringen.no/en/dep/kmd/prosjekter/e-vote-trial/source-code/the-system-architecture-/id645240/
- The complete voting system source code (including server and client components). The source code has always been publicly available in a public repository for audit purposes. This made it possible for anyone to download and use the voting system for testing and inspection. In fact, one of the authors of this Report actually downloaded the source code and actively inspected it. The only license limitation is that this source code can only be used for audit purposes but cannot be used for commercial purposes without the previous acquisition of the necessary license.
    - https://www.regjeringen.no/en/dep/kmd/prosjekter/e-vote-trial/source-code/click-here-for-access-to-the-source-code/id646007/
- Videos of the decryption and counting ceremonies that were broadcast live during the execution of the various processes.
- Academic papers and publications related to the e-voting cryptographic protocol and components used in the Norwegian e-voting system:
    - Oliver Spycher, Melanie Volkamer, Reto E. Koenig. Transparency and Technical Measures to Establish Trust in Norwegian Internet Voting. VOTE-ID 2011: 19-35
    - Douglas Wikström. A Commitment-Consistent Proof of a Shuffle. IACR Cryptology ePrint Archive 2011: 168 (2011)
    - Kristian Gjøsteen. Analysis of an internet voting protocol. Cryptology ePrint Archive, Report 2010/380, 2010. http://eprint.iacr.org/2010/380
    - Björn Terelius, Douglas Wikström. Proofs of Restricted Shuffles. AFRICACRYPT 2010: 100-113
    - Jordi Puiggalí, Sandra Guasch. Cast-as-Intended Verification in Norway. Proceedings of the 5th Conference on Electronic Voting 2012 (EVOTE2012) P-167, LNI GI Series, Bonn. July 2012.
    - Jordi Puiggalí, Sandra Guasch. Universally Verifiable Efficient Re-encryption Mixnet. EVOTE2010: The 4th International Conference on Electronic Voting, Bregenz (Austria), July 2010.

- External audit reports
    - OSCE report from the observation of e-elections in 2011:
      https://www.regjeringen.no/en/aktuelt/osse-report-from-the-observation-of-e-el/id673996/
    - IFES report from the observation of e-elections in 2011:
      http://www.regjeringen.no/upload/KRD/Prosjekter/e-valg/evaluering/Topic6_Assessment.pdf
    - OSCE's report from the parliamentary election in 2013:

https://www.regjeringen.no/en/historical-archive/solbergs-government/kmd/nyheter-og-pressemeldinger/osces-report-from-the-parliamentary-elec/id748838/

- Carter Center report from the parliamentary election in 2013:
- https://www.regjeringen.no/globalassets/upload/krd/kampanjer/valgportal/valgobservatorer/2013/rapport_cartersenteret2013.pdf

This information has been available on Norwegian Government website https://www.regjeringen.no/ since 2011 at the inception of the project. This can be confirmed via the following internet links that relate to the archiving project archive.org,:

- https://web.archive.org/web/20110407005511/http:/www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project.html?id=597658
- https://web.archive.org/web/20120309072858/http://www.regjeringen.no/en/dep/krd/prosjekter/e-vote-2011-project/source-code/the-system-architecture-.html?id=645240

– *“However the system’s claims with respect to voter privacy are weak: If the voter’s computer and the return code generator are both honest, the content of the voter’s ballot remains private.”*

Incomplete and biased. First of all, voter privacy compromise is difficult to solve on any remote voting or unsupervised system, be it paper based or electronic. To help address this scenario, in the case of Norway, the possibility of multiple voting was used to prevent any potential attacker being sure if a spied vote is the final that will be cast and counted. This measure is not implemented in traditional remote voting systems such as paper voting, thus providing a significant security improvement in this area.

Regarding the trust assumption, any voting system is also based on trust assumptions, including traditional or even the other voting systems described in the report. What it is important is the strength of the assumption.

In the case of the Norwegian system, by protocol design voter’s computer and return code generator never interact. In fact, the return code generator is a component isolated from Internet that only interacts with the vote collector server and the SMS gateway through an internal network. Controlling if the return code generator is interacting with any other system is one of the measures to check if there is such collusion. So compromising the assumption requires compromising more than the voting client and the return generation server (i.e.: any system that is monitoring the connections and the firewalls that prevent them.)

In the other systems analyzed in the report, if their trust assumption is compromised, voter privacy can be also compromised. In some cases, it is just compromising one component (voting client) or two components that are usually connected to the Internet (i.e. where discerning valid connections from incorrect ones is not trivial). However, the authors of the Report do not point out this fact as a weakness of these systems, but only as a weakness of the Norwegian protocol that requires compromising multiple components.

– *“If a voter’s encryption software and the return code generator share information, they can lead her to believe that her vote was cast accurately even when it was not. As such, the Norwegian system’s property of voter verifiability relies on the voting system software functioning properly.”*

***Incorrect and biased*.** Were the voters’ computer and the return code generator collude against the voter, this would constitute a violation of the trust assumptions under which the system was designed.

As said before, every Internet and non-Internet voting protocol relies on a series of trust assumptions to guarantee the integrity of the election results. Both the Norwegian protocol and Helios rely on trust assumptions as their base, but the authors of this report only pinpoint the Norwegian protocol. As with the Norwegian protocol, in Helios one also needs to assume that the voter's computer and the secondary device that is used to verify the vote do not collude. If those trust assumptions are violated, then either system cannot deliver the corresponding integrity guarantees.

Let us assume that the trust assumption of the Norwegian system holds (namely, the voters' computer and the return code generator do not collude against the voter). Then, **the cast-as-intended integrity property holds regardless of the software implementation**, if the voter follows the individual verification protocol, which consists on checking the return codes provided by its computer against the voter's verification card.

– *"The Norwegian system also does not provide a proof of the tally, and is therefore not universally verifiable."*

Incorrect**.** In the 2011 and 2013 elections, the Norwegian system included verifiable mixnets. In 2013, the mixnet used was Verificatum, developed by Douglas Wikstrom, a world-leading researcher in the e-voting field. By design, these mixnets provide universal verifiability. During the Norwegian election, proofs were generated and verified by auditors before the results were counted (the ceremony was even broadcasted live). Mixnet and decryption proofs were not published on the Internet but offered to any auditor that requested to audit the process. Before the election, an open call to auditors, observers and political parties was publically made for participation in the verification process. Since the specification of the protocol and the structure of the proofs are public, anybody can implement their own proof verification tools. The tools used in the tally were developed by a different company than the one that developed the voting system.

The system was not universally verifiable from the point of view that proofs were not published on the Internet, which would have enabled anybody to download and audit them. However, it was as universally verifiable as any traditional voting system, were the audit process is conducted by observers and auditors. In any case, the mixnets used in Norway supported the publication and verification of the proofs; the decision not to enable this functionality and publish these was a Norwegian Government procedural decision.

Proofs of correct decryption were therefore implemented and verified by the auditors in the same counting ceremony before decryption of the votes, thus making the claim in the report incorrect..

– *"For all these reasons, the Scytl software implementation used in the Norwegian elections is not considered an E2E-V system."*

Incorrect, inaccurate, incomplete and biased. We have already discussed that "all these reasons" either do not correspond to the reality of the Norwegian project, or they apply equally to the voting system Helios. While the Report declares Helios to be E2E-V, it declares the Norwegian protocol non E2E-V. We conclude that the assessments of the Report with respect to these systems are inconsistent, inaccurate or incomplete.

We find that the Report, in its current form, is biased and incorrectly reflects (inaccuracies and significant omissions of key information) several properties of the Norwegian electronic voting system that are in-line with those that an E2E-VIV system should, and in this case does satisfy. In benefit of public interest, it would be necessary to fix these inaccuracies and biased views in a future release of the Report.