Analyzing the feasibility of the recently reported attacks to the Swiss e-voting system

Barcelona, March 13, 2019 –Following the publication of the recent finding regarding the Swiss e-voting code, several media and social media outlets have echoed the assumptions provided by the group of researchers, according to which the lack of universal verifiability caused by a missing audit mechanism would potentially allow attackers to manipulate individual votes under two different scenarios.

However, in practice, such attacks are highly unlikely – not to say impossible – to perform. Here are the reasons why:

- **Scenario 1**

In order to manipulate individual votes, following the first scenario described by the researchers, a combination of two attacks would need to be performed:

1. attacking a voter's voting device during the voting process and

2. getting full control of one of the Mixing servers during the counting process

Getting control over the voters' voting devices would be aimed at learning the secret parameters used to encrypt the vote. The amount of voting devices that need to be compromised must therefore be proportional to the number of votes the attacker would want to manipulate.

In addition, the attack would also require the attacker to get full control of one of the Mixing servers and substitute the Mixnet software by a new software that could cheat the system. It is important to mention that this server is, according to legal requirements, physically and logically isolated from the rest of the voting system components, managed by a dedicated team and accessible only from the same datacenter.

The attack described is extremely complex to implement in a real environment as it requires combining multiple attacks to different systems that are not interconnected (a mixnet server and voter devices) as well as overcoming multiple layers of firewalls and physical protection and receiving support from several insiders with in-depth knowledge of the system.

- **Scenario 2**

The attack described in the second scenario by the researchers is aimed at manipulating the votes after being decrypted but before being counted.

This scenario only works in a very specific type of election where the voter is provided with the possibility to select from one to several candidates for a single race. The attack consists in checking which ballots – once decrypted – have less candidates than allowed, add the desired candidate if it hasn't been selected and generate a new proof that would cheat the system.

Performing such attack would require an attacker to get full control of one Mixnet server and make sure that the decryption process is also carried out in this same server.

The attack described is extremely complex to implement in a real environment as the Mixing process is taking place in an air-gapped machine disconnected from any network. The possibility of an external attack is therefore practically zero as the attacker needs to have physical access to the system and receive support from several insiders with in-depth knowledge of the system. In addition, in the current Swiss Canton Mixnet setups, the decryption process is always carried out in a separate air-gapped machine.

Although the mentioned attacks are highly theoretical and extremely difficult to implement in a real environment, Scytl considered the finding important as it affects the universal verifiability property of the voting system and updated the code and its related documentation immediately.

To put the researchers' finding in perspective, the above-mentioned attacks would actually be more feasible in traditional elections scenarios since, in those cases, the attacker would only need to have access to a ballot box.

The foremost objective of the source code publication and the public intrusion test is to ensure secure and transparent online voting processes. We are thankful to those researchers who have been sharing their findings with us since the beginning of the initiative and as part of the source code access program. The objective of this program is indeed to identify any potential vulnerabilities in a transparent manner. These findings should not be used to create controversy or adverse reactions towards online voting, but instead to foster a constructive dialogue with experts and, together, enhance the security of our electoral system. The public intrusion test on the e-voting system is running until 24 March 2019.

WHAT WE DO
We Power Democracy (https://www.scytl.com/en/we-power-democracy/)
Election Solutions (https://www.scytl.com/en/election-solutions/)

ELECTION TYPES
Political Elections (https://www.scytl.com/en/election-types/political-elections/)
Political Party Elections (https://www.scytl.com/en/election-types/political-party-elections/)
Referendums & Consultations (https://www.scytl.com/en/election-types/referendums-consultations/)
Professional Association Elections (https://www.scytl.com/en/election-types/professional-association-elections/)
Labour Union Elections (https://www.scytl.com/en/election-types/labour-union-elections/)
University Elections (https://www.scytl.com/en/election-types/university-elections/)
Parliament & Assembly Elections (https://www.scytl.com/en/election-types/parliament-assembly-elections/)
Shareholder Meetings (https://www.scytl.com/en/election-types/shareholder-meetings/)

RESEARCH
Articles and Publications (https://www.scytl.com/en/articles-and-publications/)
Research and Development Team (https://www.scytl.com/en/research-and-development-team/)
Collaboration Agreements (https://www.scytl.com/en/collaboration-agreements/)
Projects & Reports (https://www.scytl.com/en/projects-reports/)
Scientific Advisory Board (https://www.scytl.com/en/scientific-advisory-board/)

ONLINE VOTING
Benefits (https://www.scytl.com/en/online-voting-benefits/)
Expertise (https://www.scytl.com/en/online-voting-expertise/)
Technology and Security (https://www.scytl.com/en/online-voting-technology-security/)
Resources (https://www.scytl.com/en/online-voting-resources/)

ELECTION SOLUTIONS
Pre-Election
Election Training (https://www.scytl.com/en/election-training/)
Online Voter Registration (https://www.scytl.com/en/online-voter-registration/)
Candidate Management (https://www.scytl.com/en/candidate-management/)

Election Day
Online Voting (https://www.scytl.com/en/online-voting/)
Electronic Ballot Delivery (https://www.scytl.com/en/electronic-ballot-delivery/)
Electronic PollBook (https://www.scytl.com/en/electronic-pollbook/)

Post-Election
Results Consolidation (https://www.scytl.com/en/results-consolidation/)
Election Night Reporting (https://www.scytl.com/en/election-night-reporting/)

COMPANY
Company Overview (https://www.scytl.com/en/company-overview/)
Management Team (https://www.scytl.com/en/management-team/)
Awards (https://www.scytl.com/en/awards/)
Investors (https://www.scytl.com/en/investors/)
Quality Policy (https://www.scytl.com/en/quality-policy/)
Board of Directors (https://www.scytl.com/en/board-of-directors/)
Shareholders Meetings and Other Announcements (https://www.scytl.com/en/general-shareholders-meetings-and-other-announcements/)

CUSTOMERS (HTTPS://WWW.SCYTL.COM/EN/CUSTOMERS/)

NEWS (HTTPS://WWW.SCYTL.COM/EN/NEWS/)

PARTNERS (HTTPS://WWW.SCYTL.COM/EN/PARTNERS/)

CONTACT (HTTPS://WWW.SCYTL.COM/EN/CONTACT/)

CAREERS (HTTPS://WWW.SCYTL.COM/EN/CAREERS/)

FOLLOW US