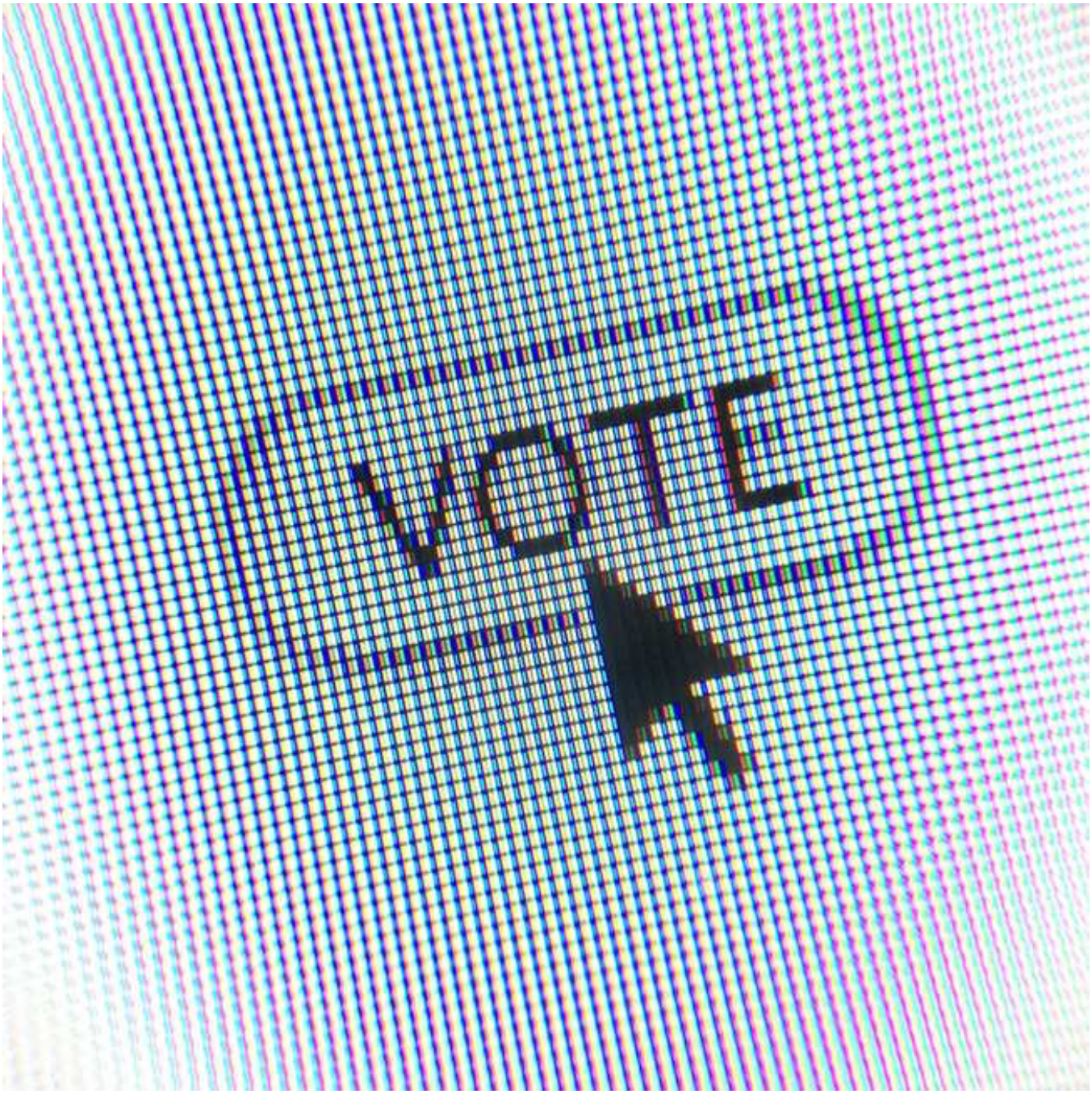
Researchers Find Critical Backdoor in Swiss Online Voting System

Researchers have found a severe issue in the new Swiss internet voting system that they say would let someone alter votes undetected. They say it should put a halt to Switzerland's plan to roll out the system in real elections this year. SHARE TWEET

Kim Zetter



Switzerland made headlines this month for the transparency of its internet voting system when it launched a public penetration test and bug bounty program to test the resiliency of the system to attack.

But after source code for the software and technical documentation describing its architecture were leaked online last week, critics are already expressing concern about the system's design and about the transparency around the public test.

Cryptography experts who spent just a few hours examining the leaked

code say the system is a poorly constructed and convoluted maze that makes it difficult to follow what's going on and effectively evaluate whether the cryptography and other security measures deployed in the system are done properly.

"It is simply not the standard we would expect."

"Most of the system is split across hundreds of different files, each configured at various levels," Sarah Jamie Lewis, a former security engineer for Amazon as well as a former computer scientist for England's GCHQ intelligence agency, told Motherboard. "I'm used to dealing with Java code that runs across different packages and different teams, and this code somewhat defeats even my understanding."

She said the system uses cryptographic solutions that are fairly new to the field and that have to be implemented in very specific ways to make the system auditable, but the design the programmers chose thwarts this.

"It is simply not the standard we would expect," she told Motherboard.

Even if the system is designed securely in principle, for it to operate securely in practice, each of its many parts has to be configured correctly or risk creating vulnerabilities that would let an attacker subvert the system and alter votes.

"Someone could wire the thing in the wrong place and suddenly the system is compromised," said Lewis, who is currently executive director of the Open Privacy Research Society, a Canadian nonprofit that develops secure and privacy-enhancing software for marginalized communities. "And when you're talking about code that is supposed to be protecting a national election, that is not a statement someone should be able to make."

It isn't just outside attackers that are a concern; the system raises the possibility for an insider to intentionally misconfigure the system to make it easier to manipulate, while maintaining plausible deniability that the misconfiguration was unintentional.

"Nobody has ever deployed a voting system with this level of complexity."

"You expect secure code to be defensively written that would prevent the implementers of the code from wiring it up incorrectly," Lewis told Motherboard. But instead of building a system that doesn't allow for this, the programmers simply added a comment to their source code telling anyone who compiles and implements it to take care to configure it properly, she said.

Matthew Green, a noted cryptographer who teaches cryptography at Johns Hopkins University, agreed with Lewis and told Motherboard the system is "enormously complex."

"To the best of my knowledge, nobody has ever deployed a voting system with this level of complexity," he told Motherboard. "At this point I think the only appropriate way to evaluate it is through a professional evaluation by someone trained in this sort of advanced cryptography. And even then I'd be concerned, given the stakes."

The system was developed by Swiss Post, the country's national postal service, and the Barcelona-based company Scytl, which was formed by a group of academics who spun it off of their research work at the Universidad Autónoma de Barcelona (Autonomous University of Barcelona) in 2001. Local cantons, or states, in Switzerland are the ones who administer elections and would be responsible for the configuration.

Scytl claims the system uses end-to-end encryption that only the Swiss Electoral Board would be able to decrypt. But there are reasons to be concerned about such claims.

In 2015, a different Scytl system used in elections in New South Wales, Australia, was found to have vulnerabilities that researchers at the University of Michigan and the University of Melbourne could use to bypass the end-to-end encryption in order to see and alter votes. Another group of researchers examined the Australian system again in 2017 and found different vulnerabilities that would still allow an attacker to see and alter votes. The Australian and Swiss systems use a lot of the same underlying cryptographic libraries, but "the Australian system doesn't have the security the Swiss system purports to have," according to Vanessa Teague, who teaches cryptography at the University of Melbourne and was part of both studies. This, on its face, suggests it's more secure, but Teague agreed with Lewis that the convoluted design raises red flags that require the system to be scrutinized more carefully.

Nathalie Dérobert, a spokeswoman for Swiss Post, said the public intrusion test is not meant to be an audit of the code "or to prove the security of the Swiss Post online voting system." Instead, it's meant to help inform the developers about improvements they need to make.

"Security is a process and even if the source code passed numerous previous security audits, we expected criticism and even outright negative comments," Dérobert wrote in an email to Motherboard. "After all, that is the whole point of publishing the source code: we want a frank response and an honest discussion about the merits and shortcomings of our work... [W]e are determined to take up the negative comments, discuss them with our developing partner Scytl and to get in touch with the people where we see a benefit."

But Lewis says such discussion is a little late.

"If you've already built your million-dollar house on sand, no amount of honest discussion is going to turn the foundations into stone," she told Motherboard.

Although Swiss Post claims the system has undergone three audits by auditing giant KPMG— among them an audit of the end-to-end encryption—it has never made the auditing reports public or indicated if anything significant got changed as a result of the audits.

“I think they don’t get the concept of free and open code.”

Lewis said she’s not sure how someone could effectively audit the complicated code and certify it.

“Even if you sat down and read every line and determined everything was good, the code still wouldn’t pass the bar for being good code,” Lewis said.

Internet voting isn’t new to Switzerland. It’s been used a couple hundred times in various cantons on a trial basis since 2004. But Switzerland wants to make it available as an option nationwide, with plans to offer it in three-fourths of the country’s cantons before October.

Internet voting has faced a lot of detractors in the computer security community. Last November, members of the Swiss branch of the Chaos Computer Club found that basic security hadn’t been implemented on the web site of another internet voting system used in Switzerland, which would allow someone to perform a DNS cache poisoning attack. Last month, critics of the system launched a public initiative to halt the internet voting program until Swiss authorities can demonstrate that it’s secure.

Although the issues around the code might be specific to Switzerland, they raise questions about other Scytl systems in use in elections. Scytl isn’t a small player in the elections industry. It has taken the lead in developing various internet and other voting solutions for national or regional elections in 42 countries, including at least 1,400 counties in the US. In the US, however, the Scytl system doesn’t collect votes over the

internet as the Swiss system does; it just delivers ballots via the internet to U.S. military and other citizens overseas, who print them out and return them via fax or offline mail. Scytl has been the center of controversy in the past for alleged misuse of European Union funds and mishap with an election.

The way the Swiss system works is that voters authenticate themselves to the voting web site using their birthdate and an initialization code they receive from Swiss Post in the mail. When they make their selections on screen, the votes are encrypted before going to the Swiss Post servers, where they are processed through a so-called "mix network" that cryptographically shuffles the votes to separate them from anything that would match them to the voter. Once the votes are shuffled, they're counted then decrypted.

So far more than 2,000 people have registered to participate in the public hacking test of the Swiss system, which runs from February 25 to March 24. The bug bounty program will pay 20,000 Swiss francs to anyone who can manipulate votes in the mock election or 30,000 to 50,000 francs if they manage to manipulate votes without being detected. As part of the test, the Swiss Post is making the source code for the software available to participants. But the code wasn't supposed to be open to just anyone to examine.

Instead, to obtain access to it, participants have to agree to terms that were published with the announcement of the bug bounty program.

"[Y]ou need to agree to these strange rules they have. So in the concept of free and open source code, it's not really accessible," said Hernani Marques, board member and spokesperson of the Chaos Computer Club of Switzerland. "I think they don't get the concept of free and open code."

The terms allow participants to publish information about vulnerabilities

they find in the code or system, but requires them to report them first to the organizers through a specified channel, as all bug bounty programs do. Participants can go public after the organizers acknowledge receipt of their report but have to wait 45 days after that acknowledgement or after the last communication the organizers send them about the vulnerability. This gives the appearance that participants are free to publish anything after this time period. But in three technical documents from Scytl that are provided with the source code and outline the architecture and protocols used in the system there is a notice indicating that none of the information in the documents can be communicated to the public or otherwise distributed.

This presents a significant barrier to publicly disclosing vulnerabilities found in the system because a system's architecture and protocols provide context for explaining the nature of a vulnerability and can even contain vulnerabilities themselves.

"[Y]ou can't publish ... if you can't describe the architecture," said a participant who was given access to the code and asked not to be identified. "Doesn't matter if you can quote the code, you'll need to be able to show why the bit of code is relevant, by showing the architecture."

Someone else who objected to the terms posted the source code and the three documents detailing the architecture and protocols online, where anyone can now examine the code for vulnerabilities without registering for the public pentest and also anonymously post information about vulnerabilities without being subject to Scytl's confidentiality terms.

Swiss Post responded to the publication of the code, saying the source code was not leaked since it was already available to anyone who wanted to see it—as long as they registered with Swiss Post. Swiss Post also wrote that there is no NDA or confidentiality agreement around

publishing information about the source code or citing parts of the code, but the statement did not say anything about the Scytl technical documents themselves and the architecture and protocol information that is contained in them.

Motherboard reached out to Scytl to ask about the confidentiality clause, but a spokeswoman's response was unclear, saying only that "researchers are allowed to publish their findings on their own after the official publication" by the organizers of the bounty program. She referred any additional questions about disclosure to Swiss Post, which referred Motherboard to the Swiss federal government. That entity did not respond.

Katie Moussouris, CEO of Luta Security, which works with companies and governments to develop bug bounty programs, agreed that there's a conflict between the conditions for the bug bounty and the boilerplate confidentiality language in the Scytl documents. Generally, to prevent participants from disclosing information in such documents the company would need to have participants sign an NDA, so it's not clear if this language was left in as an oversight or if Scytl would enforce it. She noted that because the disclosure terms for the bug bounty program require participants to coordinate with the organizers before publishing anything, this raises the possibility that restrictions could arise there.

"It's there where they might possibly ask for redactions, or not," she told Motherboard.

Correction: This story originally stated that members of the Swiss branch of the Chaos Computer Club found that basic security hadn't been implemented on the Swiss Post's web site. The vulnerability the Chaos Computer Club found was in a different internet voting system, not the one that's being tested next week. Motherboard regrets the error.