Swiss Post E-Voting Scope 4: Network Security Analysis

Cyrill Krähenbühl Marc Wyss Robin Burkhard Joel Wanner
Adrian Perrig

Network Security Group, ETH Zurich

January 6, 2022

Executive Summary

In this report, we summarize our evaluation of the Swiss Post e-voting system from the perspective of network security.

Due to the limited time frame of the Scope 4 testing period, the pro-bono nature of our work, and the potentially harmful impact to other infrastructure of Swiss Post through attacks targeting the network, our evaluation does not consider actual penetration tests, but describes potential weaknesses in the network design only from a high-level perspective without exploiting them on the live infrastructure. (As multiple production services provided by Swiss Post are hosted behind the same network connection, including Postfinance and Post E-Health platform, it would be gross negligence to run real-world attacks given the potential for collateral damage.)

The attacks identified in this work mostly relate to issues with name resolution, routing, and availability in general. Our analysis exposes the following main issues:

- Various forms of (selective) denial-of-service attacks,
- DNS spoofing attacks,
- BGP hijacking attacks,
- Attacks on vote secrecy.

Most of the network-level vulnerabilities that we discuss result in a denial-of-service, which means that the service becomes unavailable. As the vote counts or voter privacy is unaffected by (distributed) denial-of-service (DDoS) attacks, the perceived attitude is that such availability attacks are not a concern, as voters can still vote by mail or in person. However, we would like to point out that an unavailability of the e-voting system can be a severe problem, as it can lead to an **erosion of voter's trust in the e-voting infrastructure**. Not all voters are tech-savvy, and they cannot easily differentiate between vote tally issues and system unavailability. Moreover, Swiss citizens living in foreign nations will likely depend on e-voting to cast their votes in time. It is thus recommended that more attention is spent on ensuring high availability of the entire e-voting infrastructure.

Other discussed network-level attacks result in man-in-the-middle capabilities, allowing an attacker to read, modify, or drop communication between the voter and Swiss Post. In particular, if the attack is successful, the votes cast by the user can be learned, thus breaking vote secrecy.

We conclude the report by proposing methods to defend against such attacks or to mitigate their impact. Unfortunately, the current Internet systems such as DNS, BGP, and DDoS mitigation systems have fundamental limitations that make construction of a high availability system close to impossible. Exactly for that reason, the SCION secure Internet architecture has been developed over the past 12 years. Consequently, the addition of SCION-based communication can enhance the availability and resilience of the communication aspects of the Swiss Post's e-voting system in the short term, and achieve close to a guaranteed availability in the long term with additional deployment. In particular, a SCION secure Internet based approach could already today enhance the availability of the Swiss Post e-voting service for 80% of Swiss citizens with minimal overhead, thanks to a new service that can provide fundamental protection against routing and DDoS attacks, for all customers of participating ISPs (without requiring any updates of customers' systems or software).

1 Introduction

Objective. The goal of this work is to analyze the e-voting infrastructure of the Swiss Post in terms of network security. For this, we look at the e-voting system from a higher level perspective. In particular, we do not launch attacks against the e-voting system, as this would likely cause collateral damage to other services of Swiss Post and even unrelated parties. Instead, our analysis is based on the publicly available documentation and the information obtained during the Scope 4 audit session.

Outline. In Section 2, we present our attacker model. The concrete attacks that we have found are listed in Section 3. We discuss the general impact of our findings in Section 4, and discuss our proposed mitigation strategies to address the attacks and vulnerabilities in Section 5.

2 Attacker Model

In general, we use the same trust model as defined by Swiss Post, e.g., that at least one control component is trustworthy, but that the voting server is not. We only deviate from this model if we can explicitly show that some component can indeed be compromised.

In addition to the trust assumptions specified by Swiss Post, we assume that network components (such as compromised routers), individuals, and third parties may behave maliciously. Those assumptions arise from our focus on network-related vulnerabilities and are consistent with the trust assumptions of Swiss Post and the federal chancellery which are based on using the (insecure) Internet and do not assume a secure, highly-available network infrastructure.

Similarly, we do not only focus on attacks targeting individual and universal verifiability or vote secrecy, but also on attacks impacting the availability of the voting services, and in general any attacks that could impact the outcome of the voting process.

3 Attacks

This section describes our findings of possible attacks against the Swiss Post e-voting infrastructure. Our proposed mitigations can be found in Section 5.

We categorize our attacks into the following three classes:

- **Denial-of-Service attacks:** At first glance, DoS attacks on the e-voting service do not impact the outcome of an election since it is believed that a voter can always vote by mail or in person. However, strategically selecting specific time windows (e.g., a few hours before the e-voting time window ends) or specific target audiences (see Section 3.1) might influence the outcome of the vote. DoS attacks can be done via DNS, via BGP, via volumetric flooding attacks, or by abusing DoS defense systems (see Sections 3.2, 3.3 and 3.5). Moreover, as we point out in Section 4.2, unavailability of the service can result in an erosion of citizens' trust in the e-voting system.

- **Man-in-the-middle attacks:** Man-in-the-middle attacks allow an attacker to read, inject, drop, and modify packets sent between the client (voter) and the e-voting infrastructure. Man-in-the-middle attacks can be done via DNS, or BGP, and can even pass TLS certificate validation checks (see Sections 3.2 to 3.4 and 3.8.1).

  Since a man-in-the-middle attack enables the attacker to drop packets, it can also be used as a DoS attack. However, the attack is stronger since it allows the attacker to learn sensitive information about the voter's ballot (see Section 4.1) and provide the voter with arbitrary information, such as a fake hotline number or a modified e-voting application (see Section 3.8.2).

- **Other attacks:**

  Attacks on the hash verification step of the voting application (see Section 3.8.2).

  Network-level attacks during the setup phase, in particular on the voter registers (see Section 3.6).

  Attacks by external entities used for DDoS protection should be considered as well (see Section 3.7).

3.1 DoS against individual or groups of voters

By targeting specific voters (or groups of voters) for which the attacker knows what they are likely to vote, the result of the ballot can be influenced. If an attacker can for example block access to the e-voting platform based on the municipality of the voter (e.g., through IP address/geo-location), then voters from municipalities that are expected not to vote according to the attacker's desire would be targeted. A more elaborate attack is to identify (e.g., through browser fingerprinting) individual voters, guess how they will cast their ballot, and then block voters that are likely to vote contrary to the attacker's preference.

The potential of such attacks was shown in the 2016 US presidential election, where Donald Trump's success over Hillary Clinton was attributed to a fine-grained influencing based on individually targeted advertisements on Facebook [1]. As voter behavior can be predicted based on web sites visited or videos viewed, individual voter targeting has moved into the realm of possibility.

3.2 DNS attacks

Using a website as the e-voting client means the address for the e-voting site's domain first needs to be resolved. Multiple vulnerabilities in the DNS system could be used by an attacker to tamper with this resolution process. The attacks can be broadly categorized into two classes: providing an erroneous response (sending the voter to a different server), or denial-of-service (not providing a response at all, or a response that leads to a non-existent server).

DNS hijacking allows an attacker to observe and potentially modify all network traffic by redirecting the client's traffic to an arbitrary IP address under the attacker's control. A DNS resolver itself could be controlled by the attacker and easily change entries. The resolver could also be the target of attackers injecting false information, e.g., by using DNS Cache Poisoning [9] or by exploiting vulnerabilities in the DNS software. Furthermore, the connection between client and resolver could be insecure and open to attack.

Most users today make use of their ISP for their DNS resolver, which means that they need to fully trust their ISP's resolver's responses. In case of a malicious operator or a software compromise, the DNS responses can be altered, even in case of DNSSEC, which does not protect the connection from the user's system to the DNS resolver, and moreover the user's system does not cryptographically verify the DNS responses.

A recent trend, however, changes the trust relationships. In DNS over HTTPS (DoH) and DNS over TLS (DoT), the users configure public DNS servers (operated for instance by Google, Cloudflare, or Quad9), which then provide the DNS resolution directly for the user's system over a secure HTTPS or TLS connection. Both DoH and DoT prevent a network-based attacker from altering the DNS responses, but they enable the DoH or DoT server to provide arbitrary responses – in essence requiring the user to fully trust these providers. An untrustworthy DoH or DoT provider can not only provide false responses, but it can also mount a denial-of-service attack, and in essence act as a "kill switch" for selected communication [13].

Homograph attacks target the client (user) directly, instead of the client's device or application, by hosting the e-voting application on a different domain whose name appears similar to the original domain, fooling voters to believe that they are on the correct web site. Such homograph attacks are typically done by replacing a character with a similar-looking character or by using a different top-level domain.

The time allocated for this analysis was unfortunately not sufficient to perform an in-depth analysis of resilience against these DNS attacks.

Recommendations & Mitigations. The DNS system needs to be monitored from different vantage points during an election, to facilitate detection of any of the listed attacks. The use of a fixed IPv4 address for the voting server can be considered, which would need to be typed in by the user in case the voting server cannot be reached—which would eliminate DNS-based attacks. Even though usability would decrease, entering an IPv4 address instead of a domain name does not constitute a heavy burden, especially when considering that the user anyway needs to input and compare many codes/digits during the voting process.

Another option is to bypass DNS by providing the voting client as an application instead of a website and having the IP address and certificate information embedded in the application. This requires the

application to be distributed over a secure channel (e.g., a trusted App store). If it is downloaded at a website, DNS attacks could be leveraged again to spread modified programs via spoofed websites, although the application downloaded needs to be signed and verified in any case.

The ultimate solution is to always use end-to-end authenticated naming data. However, DNSSEC does not provide such a mechanism. Because of the large overhead and numerous configuration errors causing resolution failure, clients today almost never validate the DNSSEC chain of trust themselves, but rely on validating resolvers operated by third parties.

3.3 BGP attacks

There are two types of relevant BGP attacks: denial-of-service attacks that disrupt the e-voting service, and man-in-the-middle attacks that work by re-routing traffic and imitating voting servers.

By inserting bogus BGP announcements for the target IP address ranges, e.g., containing the voting server address, an attacker can use BGP prefix hijacking to redirect traffic to a destination under the attacker's control. The attacker then either drops, or modifies and forwards all incoming traffic for denial-of-service or man-in-the-middle attacks, respectively. The Swiss Post network mainly uses Swisscom as an Internet Service Provider and is connected to the Swisscom network via two interfaces at the respective Swiss Post sites. There is a backup interface to UPC / Sunrise that can manually be enabled in case the connectivity over Swisscom deteriorates.

The effectiveness of BGP hijacking depends on the proximity of the attacker, and the network location of the source and destination. For example, a BGP hijacking attack on Swiss citizens living in Switzerland and connected to the Internet via Swisscom is unlikely to be successful, as Swisscom internally assures routing security for communication between their direct customers. Most likely, other Swiss ISPs will prefer the Post's IP prefix announcement from Swisscom, such that external announcements are ignored for most Swiss customers.

However, when the client is further away from the voting server, the hijacking attack becomes more effective, since an attacker controlling an autonomous system (AS) can forge a BGP update with a sub-prefix of Post's address range, and redirect traffic to itself. BGP hijacking is thus most impactful for Swiss citizens living abroad, which would be one of the main beneficiaries of e-voting. DoS vectors against the routing infrastructure are further discussed in Section 3.5.

Denial-of-Service. BGP-based DoS attacks can have a wide range of time scales (up to several hours) and target audiences. Given the current setup, the Post network appears susceptible to routing attacks, because no routing attack mitigation systems seem to be in use (e.g., RPKI ROA, or multiple providers globally announcing the prefix).

Man-in-the-Middle. BGP-based man-in-the-middle attacks are hard to detect, since clients typically have no information on where their traffic is routed to. Even prior knowledge of the IP address of the service does not mitigate these issues since the attacker can hijack an entire IP address range.

Current Network Analysis. Swiss Post has two ASes: AS 12511 and AS 210998. We present a brief analysis of their networks.

AS 12511: CH-POSTNETZ, Die Schweizerische Post AG. This AS has the following four IPv4 and three IPv6 prefixes:

- 84.246.232.0/21
- 138.189.0.0/16
- 138.191.0.0/16
- 194.41.128.0/17
- 2a00:17c8::/32
- 2a00:17c9::/32
- 2a00:17cf::/32

On a global rating, CH-POSTNETZ has rank 2200 for their IPv4 connectivity, and place 758 for their IPv6 connectivity (based on radar.qrator.net, December 2021). The rank is computed among all the approximately 75 000 ASes in existence, and denotes a relative measure of the distance to the Internet backbone.

AS 210998: SWISSPOSTSOLUTION. This AS has only a single IPv4 prefix: 194.6.177.0/24. It is connected via two providers: AS3303 SWISSCOM and AS8220 COLT. SWISSPOSTSOLUTION has 1750th place in terms of their IPv4 connectivity rating.

There are a few important aspects concerning the connectivity that we would like to highlight. The first is that the main Post AS is connected only via a single provider: AS 3303 SWISSCOM. Based on discussions with the Post team, the connectivity can also be manually switched over to Sunrise / UPC (through AS 6830 LibertyGlobal), but there will likely be an associated outage of at least a few minutes. In any case, the global connectivity rating leaves room for improvement, given the critical infrastructure services offered.

Another important aspect is that the Post AS does not have any peering relationships with any other AS. Peering connections would enhance the availability of the network for customers in the other ASes.

The final important aspect is that none of the prefixes is protected by an RPKI ROA. Although the protection is relatively weak, it nevertheless provides a basic level of protection against hijack attacks. As all the main Post prefixes are very large (/16, /17, and /21), it is likely that sub-prefix hijack attacks will be successful.

Recommendations. Multiple providers should be used to increase connectivity, in particular to avoid requiring manual processes for switching in case of the main connectivity loss. Connectivity could be further improved through peerings with other Swiss ISPs. In particular, obtaining RPKI ROAs are highly recommended, as the state-of-the-art in Internet routing security should be attained. It is also recommended to make use of SCION secure Internet connectivity from multiple providers, and offer customers the choice to obtain higher availability by using SCION connectivity as an alternative to traditional Internet connectivity.

3.4 Certificate issuance attacks leveraging attacks on DNS and BGP

While the most basic attacks that aim at redirecting user traffic to a spoofed website can be prevented by the use of certificates, there is a possibility of a two-phase attack on both the certificate issuance phase and the voting phase.

In the first phase, an attacker requests a fraudulent certificate by circumventing the domain control verification process, which can for example be achieved by using an automatic certificate issuance protocol such as ACME, and either (1) spoofing the DNS entries to return an IP address controlled by the attacker, or (2) performing a BGP prefix hijack attack on the actual domain's IP address. This allows the attacker to obtain a fraudulent certificate that can be used to impersonate the website. These attacks have been demonstrated in the wild by Birge-Lee et al. [8]. More powerful attackers such as state-sponsored adversaries might have the capabilities to undermine CAs directly, which would allow them to obtaining an illegitimate certificate even without having to trick the domain control verification process. In the second phase, the attacker performs a man-in-the-middle attack on the voter either using DNS or BGP as explained in the previous sections.

This combined attack violates vote secrecy, as the attacker now has a valid certificate for its own e-voting website and can learn the plaintext votes by crafting a spoofed website that does not encrypt the votes and the keys, but sends them in plaintext to the attacker instead. Furthermore, the attack can be used to shift the outcome of the vote by blocking undesirable votes, and only forwarding votes that are aligned with the attacker's intent to the real Swiss Post voting server (similar to the attack described in Section 3.1). Voters who are allowed by the attacker to cast their votes will not notice any inconsistencies in the e-voting process, as still the correct codes are returned. To prevent suspicion, disliked voters can for example be shown an error page. The attacker could further issue arbitrary votes in an attempt to get the voter blocked from the e-voting system itself, as the start voting key is known to the attacker. If successful, the voter will also not be able to cast its votes later in case the attack ends before the election deadline. Assuming that the voters indeed check the return codes, the attacker cannot just issue votes on behalf of them, as he does not know the ballot casting key to

actually confirm the selected options. He would need to trick the users into entering the ballot casting key before they check the choice return codes to be able to cast votes in their name.

Recommendation. The same measures should be applied as described in Sections 3.2 and 3.3. Furthermore, Swiss Post could actively audit certificate transparency (CT) logs to detect fraudulent certificates, and recommend voters to use browsers that enforce CT (i.e., not Firefox). To prevent vote secrecy from being violated, Swiss Post could also add cryptographic codes to the voting cards that represent voting options. The user would then input those codes instead of an actual Yes/No/Candidate. This way, neither a man-in-the-middle attacker, nor even the voting client can learn the actual votes (which further allows to relax the trust model).

3.5 DoS against e-voting infrastructure

By targeting the e-voting infrastructure or network components on the route from a voter's client to the voting server, an attacker can try to render the e-voting service unavailable and thus prevent voters from casting their vote. In the case of Swiss Post, the current system design has the following potential weaknesses:

- **BGP:** With BGP, only a single path exists from a voting client to the server. If the system or any on-path link is congested, no alternative path is available. In case of link failures, BGP typically requires several minutes to recover and switch paths. The attack traffic will typically also follow onto the switched path.
- **Link Capacity:** Swiss Post uses 5 Gbps upstream links. While certain attacks can already be mitigated by Swisscom, a DDoS attack of at least 5 Gbps with traffic that is likely passed through the filters is quite easy to achieve.
- **System Separation:** As the network infrastructure by the Swiss Post is used both for e-voting and any other business services, volumetric DDoS attacks can impact the availability of multiple services at once.

Furthermore, DDoS defense systems are not perfect. Existing simpler systems can be tricked into blocking IP addresses belonging to legitimate users by flooding the network with packets containing spoofed addresses. Such attacks are quite effective, as an attacker only needs a short-term effort to achieve long-term impact.

Swiss Post is using a DDoS protection system offered by Swisscom. The system is set up in a way that in case of a DDoS attack, the traffic is re-directed internally at Swisscom to pass through scrubbing servers by Netscout, which in the ideal case would only permit legitimate traffic to pass through to the destination Post serves. Although these systems can mitigate most attacks, it is likely that a sophisticated targeted attack will not be mitigated (because of the non-negligible false positive and false negative error rates of current DDoS mitigation systems).

Recommendation. All current DDoS defense systems suffer from the same shortcoming: they are effective against the regular (unsophisticated) attacks, but can be circumvented by a sophisticated adversary. Next-generation DDoS defense mechanisms offered by the SCION secure Internet architecture are needed to provide fundamental guarantees.

3.6 Attacks on voter register

Municipalities keep track of all their eligible voters. For an election, this information needs to be transmitted to other entities such as the canton. Past research [10] revealed that this channel is not secure however – often the register is transmitted by email, which is neither authenticated nor encrypted, and also stored in plaintext. Hence the register can be changed at various points in this process, without such changes being detected. This is not an issue related to Swiss Post, but Swiss Post could help improve this situation, for example by providing appropriate guidelines to the cantons. Such an attack is already possible in today's mail-based voting and its mitigation would therefore also improve the security of the current voting system.

Recommendation. A secure end-to-end communication system should be used to transfer the voter register. As this process happens before the election, only secrecy and integrity properties are needed, but not necessarily high availability. Existing VPN or end-to-end encryption technologies can be used, although the key management is a challenge.

3.7 Trust in external entities

There are potential risks associated in relying on foreign entities for DDoS protection. In particular, the protection services offered by Swisscom are based on hardware and software by the US-based vendor *NETSCOUT Systems* [2]. Such systems implement a large number of filters and thresholds that can be partially configured by the network operator, but ultimately rely on attack signatures from the vendor to identify state-of-the-art attacks. Since such filtering techniques are highly non-transparent (especially given the increasing reliance on machine learning technology), it is difficult to inspect and detect rules that would for instance exclude votes from a certain jurisdiction.

Nationwide deployment of network appliances implanted with spyware has already been observed [3]. A foreign vendor interested in influencing a Swiss election could therefore deploy an attack signature on the DDoS solutions that protect the e-voting infrastructure. This malicious signature has a bias that causes false positives for a certain set of sources, e.g., blocking voters from regions that are expected to vote predominantly in a certain way on an issue. These voters would then be blocked by the filtering service, potentially dissuading them from voting (see Section 4.3). As false positives are common in signature-based attack detection, it would be possible for the vendor to maintain plausible deniability.

Recommendation. DDoS defense mechanisms should be used that offer transparency, such that the risk of external tampering can be mitigated. Such tampering could potentially also be detected by enabling voters to submit a report that they could not submit their vote, which will likely result in a detectable pattern if an entity attempts to perform large-scale voter fraud.

3.8 Miscellaneous other attacks

3.8.1 Certificate fingerprint validation circumvention

All of the man-in-the-middle attacks discussed so far can be prevented by a diligent tech-savvy voter by checking the hash of the e-voting website's certificate which is printed on the voting card. However, even if a voter verifies the fingerprint of the certificate, an attacker performing a man-in-the-middle attack and using a bogus certificate might be able to trick the voter into validating the wrong information.

Several approaches exist to mount such an attack. One option is to make the voter validate the certificate of the legitimate website instead of the bogus one by opening a new browser tab for this purpose. This is an instance of a time-of-check-to-time-of-use (TOCTOU) problem, where the user validates the correct web site but is tricked to submit the vote on a different / malicious site. Other approaches deceive users with graphical elements such as fake browser bars into validating information provided by the attacker itself.

Recommendation. A stand-alone e-voting application should be used on mobile devices, as a thorough certificate validation can be more challenging on mobile devices. On desktop / laptop systems with larger screens, the instructions for user-based validation of browser indicators need to be very carefully crafted, such that enough users would detect and report attacks.

3.8.2 Missing subresource integrity verification

The voter is supposed to check the hash values of platformRootCA.js and ov-api.min.js JavaScript files in order to ensure their correctness. However, the reference hashes are published on the e-voting website, and can therefore also be changed by an attacker that has compromised the web server. Furthermore, the correctness of the JavaScript files does not imply that the whole content of the website is correct. A spoofed website may include the original and correct JavaScript files, but simply not make use of them, and execute malicious code instead.

Also, for the current implementation, while the hash of platformRootCA.js is checked as follows,

```
<script src="platformRootCA.js"
integrity="sha256-KznD70fQG9IDMlYZut8P6ckTrUQ2iS/r8i9h/BtiqZY="></script>
```

the hash of ov-api.min.js is not verified:

```
<script src="crypto/ov-api.min.js"></script>
```

The missing subresource integrity verification prevents the browser from automatically verifying the integrity of ov-api.min.js, and makes it more cumbersome for the user to check the corresponding hash value.

Recommendation. As an immediate step, the missing subresource integrity verification should be added. The reference hashes of the JavaScript files should be distributed through a less tightly coupled channel, for example by including them on the voting card.

4 Discussion

4.1 Implications of compromised voting server

According to the trust model of the e-voting architecture, a voting server is not considered trustworthy. However, in case of a compromised voting server (the voter portal front-end to be more precise, see Section 3.8.2), it can provide voters with malicious web content, which learns the user's votes and sends it to the attacker, which thus breaks vote secrecy.

4.2 DoS as a means to reduce trust

While the traditional voting method of physical ballots provides an important safeguard against attacks on the availability of the system, it is important to consider the potential **damage in reputation** and **erosion of trust** that can be incurred by outages of the e-voting infrastructure. Not all voters are tech-savvy, and they cannot easily discern between vote tally issues and service unavailability. It is thus recommended that more attention is spent on ensuring high availability of the entire e-voting infrastructure.

4.3 DoS on individual voters to shift election

Even though the unavaliability of the e-voting system does not make an election invalid, since voting in person is still available after e-voting has closed, it is nevertheless conceivable that some voters forego their vote due to the unavailability of the online system. The ease of voting from home that comes with the e-voting system will incentivize some citizens to vote who have not voted before. The participation rate for votes has been below 50% on average in Switzerland [4]. Using attacks to block the votes of selected voters may thus have an impact on the results.

4.4 Interplay with voting by mail

Voters that still vote by postal mail, for example because they do not trust e-voting in general, do not have a concrete assurance that no one voted in their place electronically. The problem arises from the votes cast through e-voting taking precedence over votes cast through postal mail in order to prevent double voting. As a possible solution, such voters could get a feedback letter confirming that they indeed voted by postal mail, or a letter indicating that their postal vote was ignored as the e-vote took precedence.

4.5 Swiss Citizens living abroad

Given the large number of Swiss citizens living abroad (10.7% in the year 2020 [5]), their potential impact on the voting results can be significant. Many expats are dependent on e-voting, as postal delivery can be delayed in some nations, leaving insufficient time to send the vote in time. Unfortunately, it is also simpler to mount network-level attacks targeting communication to and from foreign nations. DDoS attacks for example become simpler due to the increased attack surface and a higher number of

potential adversaries, and BGP attacks get more powerful due to the large distance between the Swiss Post servers and foreign ASes.

In this context it becomes even more apparent why availability of the e-voting system is crucial. While Swiss citizens residing in Switzerland can still cast their vote in person in case the e-voting system is unavailable, i.e., on the last day of the election after e-voting is closed at the latest, expats do not have this option.

5 General Approaches for Attack Mitigation

5.1 SCION

With the goal of creating a fundamentally secure communication infrastructure, the work on SCION has begun in 2009. After over 12 years of research and development, SCION is today available across the globe, with the most penetration in Switzerland. Most of the attacks described in the previous sections can be mitigated through the use of SCION [12]. SCION connectivity is available from Swisscom [6], Sunrise [7], and SWITCH, with more ISPs joining and making their offerings available. Swiss Post can thus benefit from SCION's advantages:

- SCION's control plane ensures that all announced on-path ASes are authentic, inherently preventing the path hijacking attacks that are still possible in BGP (see Section 3.3), as well as BGP with ROV [11].
- Our network security group is working on a secure-by-design naming system called RHINE, which aims to fundamentally address the limitations of DNSSEC with a new security architecture. It allows lightweight authentication of naming data signed by zone owners, while leaving the complex authentication of zone delegation chain to a well-established PKI. RHINE is under active development and the first prototype will be released soon in early 2022.
- Instead of keeping idle backup links, SCION allows Swiss Post to announce all of its access links, which leads to more efficiency and significantly increases the capacity available to e-voting traffic. When a link goes down, SCION can immediately switch to a different path (fast failover).
- Due to efficient per-packet source authentication, firewalls can detect spoofed traffic, which allows to mitigate a large range of DDoS attacks. SCION provides a sovereign, more transparent, and verifiable DDoS solution.

E-voting users do not need to be SCION-aware or install any additional software on their device. Instead, the benefits above can be achieved already with a SCION-IP Gateway (SIG) deployed at the ISP. In this deployment model, which is already available today, the ISPs re-direct traffic for certain destinations to the SIG deployed at the ISP, which converts the IP packets into SCION packets and sends them toward the destination. With Swisscom and Sunrise / UPC deploying this technology, already 80% of all Swiss citizens are covered, achieving close-to guaranteed packet delivery to the e-voting server. A detailed system design is outside the scope of this report, but the core message is that with a relatively simple deployment, very strong security properties can be achieved.

5.2 Monitoring

One approach to detect DoS and MitM attacks is by monitoring the vulnerable service from different vantage points in the network and detect disruptions and adversarial actions early. As a simple metric, the vantage points could periodically fetch the voting application webpage and compare the hash of the returned html page to the expected hash. A slightly more involved approach would be to (additionally) extract the used TLS certificate and validate its fingerprint.

5.3 Manual Investigation

Manual investigations, for example performed by a government agency are a powerful tool to detect large-scale attacks. In general, manual interventions are less effective against unexpected attacks and are typically used to track the impact of an attack after it has occurred. Certain attacks, such as

DoS against groups of individuals to impact the result, see Section 3.1, are detectable through manual investigation if executed without discretion and at large scale.

References

[1] https://www.sciencedaily.com/releases/2018/10/181025103303.htm.

[2] https://www.netscout.com/arbor-ddos.

[3] https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/.

[4] https://www.bfs.admin.ch/bfs/de/home/statistiken/politik/abstimmungen/stimmbeteiligung.html.

[5] https://www.bfs.admin.ch/bfs/en/home/statistics/population/migration-integration/swiss-abroad.html.

[6] https://www.swisscom.ch/de/business/enterprise/angebot/wireline/scion.html.

[7] https://www.sunrise.ch/business/de/grossunternehmen/internet-networking/business-wan/scion.

[8] Henry Birge-Lee, Yixin Sun, Anne Edmundson, Jennifer Rexford, and Prateek Mittal. Bamboozling Certificate Authorities with BGP. In *Proceedings of the 27th USENIX Security Symposium*, August 2018.

[9] Tianxiang Dai, Philipp Jeitner, Haya Shulman, and Michael Waidner. From IP to transport and beyond: cross-layer attacks against applications. In *Proceedings of ACM SIGCOMM Conference*, August 2021.

[10] Christian Killer and Burkhard Stiller. *The Swiss Postal Voting Process and Its System and Security Analysis*, pages 134–149. Springer International Publishing, 09 2019.

[11] Reynaldo Morillo, Justin Furuness, Cameron Morris, James Breslin, Amir Herzberg, and Bing Wang. ROV++: Improved deployable defense against BGP hijacking. In *Proceedings of Network and Distributed Systems Security (NDSS)*, February 2021.

[12] Adrian Perrig, Pawel Szalachowski, Raphael M. Reischuk, and Laurent Chuat. *SCION: A Secure Internet Architecture*. Springer, 2017.

[13] Benjamin Rothenberger, Daniele E. Asoni, David Barrera, and Adrian Perrig. Internet kill switches demystified. In *Proceedings of European Workshop on Systems Security (EuroSec)*, April 2017.