Halifax Election Security and Privacy concerns

September 28, 2012

ATTN: Candian Cyber Incident Response Centre (CCIRC)
FROM: Kevin McArthur

The Halifax online election may be vulnerable to SSL stripping attack, [redacted] This is not intended to be a complete listing of concerns and does not address social concerns such as voter coercion, credential stealing or vote selling.

The following information was collected through public source research on 10 September 2012. This information has been determined through simple web browsing, whois, dns queries and ssl negotiation with the publicly available websites. It may not be current as of the polls opening on October 6th.

**SSL/TLS Stripping Attack**

The Halifax election appears to be vulnerable to SSL/TLS stripping attack.[1] Before election day voters are provided a card directing them to visit "vote.halixfax.ca". The voting card example found at http://www.halifax.ca/election/evoting12.html does not contain instructions to use a HTTPS url or instructions on how to verify the polling site identity presented to the voter. All major browsers will interpret a voter input of 'vote.halifax.ca' to mean http://vote.halifax.ca. Because the initial request is sent over unauthenticated and unverified plain http, rather than https, this allows for the removal of SSL security from that point onwards. This attack can be achieved through DNS, ARP Spoofing, Route Replacement, Local System Tampering, Remote System Tampering, and many other vectors. This can be achieved at scale sufficient to draw into question the election result and is difficult, if not impossible to detect as there are limitless network perspectives that could be attacked. The attack could be as broad as the entire election or could simply target a group of electors as small as a neighbourhood or even individual computers. The limited security that is supposed to be afforded by SSL/TLS is defeated before it even begins due to the voter instructions.

Additionally, even without SSL stripping, a Certificate Authority compromise or collusion could similarly allow for direct MITM attacks on sessions that do setup SSL/TLS encryption. There are a large number of non-halifax and non-Canadian identity validating organizations capable of defeating this security model either through negligence or purpose[2][3][4]. No combination of voter credentials or captcha measures can mitigate a man-in-the-middle attack from SSL security stripping or failure. In such a failure, the voters credentials and voting intention can be intercepted and/or modified in transit. Additionally voter names can be obtained through simple social engineering attack by simply including a "Legal Name:" field within the replacement site. Such an inclusion may likely defeat attempts to anonymize the vote through numerical credentials.

---

[1] http://www.thoughtcrime.org/software/sslstrip/

[2] Certied Lies: Detecting and Defeating Government Interception Attacks Against SSL http://files.cloudprivacy.net/ssl-mitm.pdf

[3] I.E. The "comodohacker" and similar attacks on SSL Certificate Authorities.

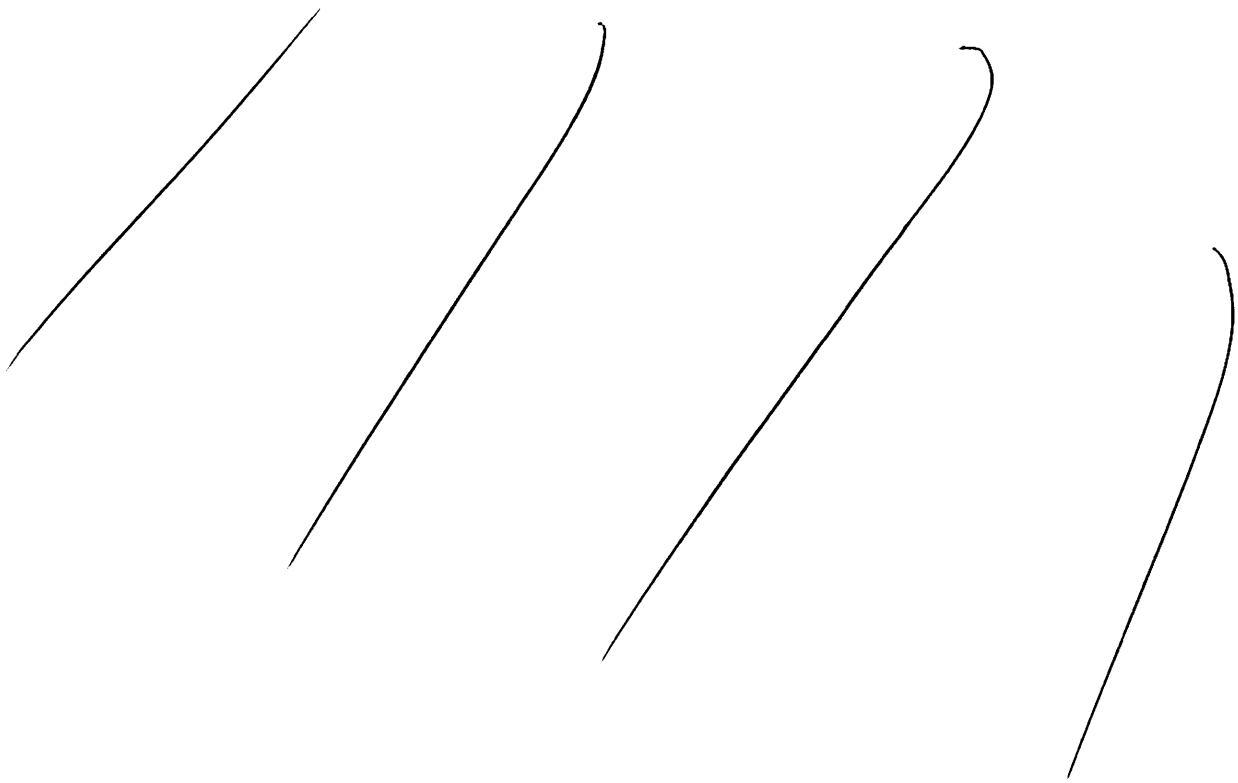
[4] EFF Map of CA's https://www.eff.org/files/map-of-CAs.pdf

**Third Party Domain In Use**

As of 10 Sep 2012, the Halifax election site presents the login link as a third-party domain, with voters being directed from the vote.halifax.ca site to securevote.ca. The securevote.ca site appears to be owned by a third party, but no identity documentation is provided that this company is the legitimate delegate of the Halifax Election.

An attacker targetting the election by man-in-the-middle attack (eg ssl stripping) could simply direct voters to an alternative domain name: eg securervote.ca or reallysecurevote.ca, and voters would have no reasonable way to tell the difference between these domains and the actual domain they are expected to use. SSL features such as the lock icon can still be provided as domain-validation certs are the comparison and no instruction is given to voters on how to discern a legitimate certificate for halifax from another identity certificate provided.

Further, it is unclear who electors are actually submitting their votes to. Consider this to be like casting a ballot at a location labelled 'polling station' around the city without any way to verify the polling station is legitimate or being monitored by party scrutineers. The ballot simply leaves the users computer heading to an unauthenticated and unverified third party that is unknown to the elector and is expected to make it to the official count untampered.



throughout the city. Such attacks would be very hard if not impossible to detect due to number of possible network perspectives.

**Conclusion**

The election process in use may present a number of security and privacy challenges that electors may not be sufficiently aware of when deciding to cast their votes online. These vulnerabilities and lack of auditability may affect the perceived validity of the election result for those that did not use the online mechanisms to vote.

The online election may need to be suspended in order to address these and other issues not here disclosed.