REPUBLIQUE ET CANTON DE GENEVE
Département des infrastructures
Office cantonal des systèmes d'information et du numérique

Réponses concernant le DNS Cache Poisoning et le Vote Electronique

Contexte

La SRF nous informe que des membres du CCC auraient relevé l'absence de protection contre des attaques de type DNS Cache Poisoning pour le site de Vote Electronique hébergé par le canton de Genève.

Introduction technique

Les attaques de type DNS Cache Poisoning consistent à corrompre un "annuaire" de l'Internet de telle sorte que les utilisateurs qui utilisent cet "annuaire" soient redirigés vers un site malicieux sous contrôle de l'attaquant.

Réponses aux questions de la SRF

1. Saviez-vous qu'il y a eu cette brèche dans la sécurité ?

Il ne s'agit pas à proprement parler d'une brèche, mais du fonctionnement nominal d'Internet. L'annonce du Chaos Computer Club (CCC) fait indirectement référence au système DNSSEC, conceptualisé en 2005[1] et introduit progressivement depuis, et qui permet de rendre une attaque de ce type plus compliquée.
C'est donc un scénario d'attaque connu et identifié depuis l'introduction du Vote Electronique, qui prédate la conception de DNSSEC, puisque la première utilisation du Vote Electronique à Genève date de 2003. **Pour référence, le rapport concernant la sécurité du Vote Electronique du 4 février 2002 mentionne déjà les attaques de ce type ainsi que le moyen de protection mis en œuvre.**

2. Comment évaluez-vous le danger posé par cette vulnérabilité ?

Il ne s'agit pas d'une vulnérabilité parce qu'il y a des mesures de sécurité qui sont en place et décrites dans la réponse à la question 3.

3. Avez-vous déjà pris des mesures pour remédier à la vulnérabilité ou envisagez-vous de le faire ?

Depuis son instigation, le projet de Vote Electronique à propose des mesures de protection aux électeurs pour éviter que leurs suffrages soient détournés.
La première de ces mesures est la présence sur le matériel de vote de l'empreinte électronique du certificat du serveur légitime du système de Vote Electronique. Cette empreinte est accompagnée d'une marche à suivre pour valider que l'électeur est bien en communication avec le serveur officiel du système, seul à pouvoir fournir le certificat correspondant à l'empreinte imprimée sur la carte de vote de l'électeur. **Ce certificat permet donc d'authentifier le serveur légitime du système.**
Avec l'introduction de l'Ordonnance sur le Vote Electronique de 2013, entrée en vigueur en 2014, les exigences sur les systèmes de Vote Electronique en Suisse se sont enrichies d'un élément supplémentaire qui vient également mitiger le scénario d'attaque dont il est question ici. Le principe de vérifiabilité individuelle consiste à afficher des codes dits *de vérification* aux électeurs une fois qu'ils ont finalisé leur bulletin, mais avant de l'enregistrer. Ces codes sont uniques pour chaque électeur, chaque scrutin et chacune des possibilités de réponse à chacune des questions posées. Ils font office de secret partagé entre le système de Vote Electronique et l'électeur et ne peuvent pas être devinés avec une probabilité suffisante. Ils ne peuvent donc pas être falsifiés.
Ainsi donc, un électeur dont le vote serait manipulé ne recevrait pas les codes

[1] Voir https://tools.ietf.org/html/rfc4033

OCSIN • rue du Grand-Pré 64-66 • 1202 Genève
Tél. +41 (22) 388 00 00 • Fax +41 (22) 388 00 99 • www.geneve.ch

correspondant à ses choix et ne confirmerait pas son vote au moyen de son *code de confirmation*. Sans ce code de confirmation, le système n'enregistre pas le bulletin de l'électeur, qui est alors redirigé vers les autres canaux de vote et prié d'avertir le support de l'incohérence de codes constatée. Ceci, quelle que soit la manière par laquelle un attaquant chercherait à altérer les choix du votant.
Enfin, une surveillance régulière du système permet de détecter les variations anormales de trafic qui résulterait de ce scénario d'attaque: si une trop forte proportion des électeurs est redirigée vers un site malicieux, une baisse de trafic anormale serait constatée et analysée.

4. **Ce n'est pas la première fois que des pirates informatiques découvrent des vulnérabilités dans les systèmes de vote électronique. Les pirates informatiques sont convaincus que ce n'est qu'une question de temps avant que d'autres vulnérabilités n'apparaissent dans le système. Y a-t-il quelque chose que vous puissiez faire ?**

Comme le démontrent les réponses ci-dessus, les méthodes pour détourner un vote ne sont pas nouvelles et sont déjà connues et prises en considération par d'autres mesures préventives.
Elles sont d'ailleurs référencées dans l'analyse des risques maintenue à jour conjointement par la Chancellerie de Genève et l'Office Cantonal des Systèmes d'Information et du Numérique qui doit être présentée régulièrement à la Chancellerie Fédérale pour obtenir un agrément pour l'utilisation du système de Vote Electronique.
Cette analyse des risques permet de définir des mesures de protection contre les scénarios identifiés et de faire valider ces mesures par la Chancellerie Fédérale, ainsi que par les experts en sécurité informatique avec lesquels nous collaborons.
Le système de Vote Electronique est en outre soumis à des audits publics réguliers, qui permettent une amélioration continue de la sécurité et de maintenir le système à jour contre les nouveaux scénarios qui pourraient émerger, ce qui n'est pas le cas ici.

Conclusion

Cette question n'est ni nouvelle, ni ignorée par les équipes du Vote Electronique à Genève et des contre-mesures pour s'en prémunir sont en place depuis 2003 et renforcées depuis 2015 avec la vérifiabilité individuelle.

Par ailleurs, selon les vérifications auxquelles nous avons procédées à ce jour, il n'apparait pas d'anomalie dans le déroulement de l'opération de vote électronique. La surveillance de celle-ci continue comme lors de chaque scrutin.