Building Privacy-preserving Administrative Processing Tracker with High SNR with Cryptographic Primitives

ustravelap.com

Abstract

To ensure strong security and privacy notion of personal information, we develop ustravelap.com - a website to securely keep the records of administrative processing of a U.S. visa. To guarantee the security even if the data resides in the server is stolen, the security mindsets and the cryptographic primitives are used to enforce the confidentiality. In this draft, we introduce the security mechanics adopted in our system, including the desensitization, encryption, and authentication.

1 Introduction

1.1 U.S. Border Security

Admitted or not, U.S. is the most open country, which can be seen from the millions of people applying for a visa. The processing speed (without administrative process) and acceptance rate is already high compared with other western countries. Known for sure, the illegal immigrant issue has been an overwhelming topic in the U.S. society. Therefore, due to **necessary** border security concerns, some visa applicants are subject to the administrative processing. To be honest, *security clearance* in our definition.

$$\text{Administrative Processing} \overset{\text{c}}{\approx} \text{Security Clearance}$$

The growth of the number of applicants, together with the difficult international circumstances, poses a threat to the border security of many countries. Some countries decide to follow a negative attitude towards non-immigrants, while the U.S. still opens the door. We should always remember that, it is the honourable visa officer who follows the regulations honestly, who protects you even during your short journey in the U.S.. The fact that your aeroplane is not hijacked is not something taken for grant. It comes from the people who protects the border security, routinely checks your name, and deals with people every morning.

You being subject to administrative processing does not mean the visa officer does not trust you, but mostly under your circumstance. And the visa officer is doing what he/she should do and actually what U.S. people demand the visa officers to do. You are not the reason the administrative processing is designed for. So before you being aggressive and anxious about *why I am subject to administrative processing*, you should understand that thousands of people are subject to this processing. It is a normal process. There is no way to expedite the visa processing *except preparing all possible materials for interview*. A good description of the border right can be a revised sentence from Canada IRCC.

Entering another country is a privillege rather than a right.

1.2 Tracker of Administrative Processing

The anxiety does not automatically dissipate. Therefore, a tracker for the status of administrative processing is needed, which helps benign persons consider and schedule their journey earlier. Especially, one ultimate reason of tracker website is to tell the newcomers that it is normal to wait for such a time, and no way to expedite. As the state-of-the-arts tracker "checkee.info" has the following issues, we decide to implement a different one. [1] Our system focuses on the privacy guarantee and the high signal-noise ratio (SNR).

[1] The website "checkee.info" is maintained by someone volunteer. We should always be thankful to the website developer.

- **(Traceability)**. Not all people reports that their cases are cleared when the visa is issued. Therefore, in the "checkee.info", there are many long-term cases with formidable 1000 days. However, such cases are resolved for a long time. To ensure that long-term cases can be cleaned and keep the accuracy of the history data, the traceability is needed. In our consideration, the notification by email is not realistic. Not only such emails are likely to be automatically labelled as spam, the email service can be used to DDoS someone, but also the effort to maintain a speedy and reliable mail service is enormous. Not to mention that previous email addresses may be discarded. To do that, we ask the user to provide the case number which can be tracked publicly in the ceac.state.gov. However, the case number is not public in our system. Instead, only the administrators can access to the case number of long-term inactive results which is not cleared. Even when the server is compromised, the secrecy of the case number is still guaranteed.

- **(Privacy-preserving)**. To keep connected to the information provider and allow the provider to update the information, the "checkee.info" requires the user to set a password. To the best of our knowledge, we still cannot make sure whether the "checkee.info" stores the password in the plaintext. However, there is much personal information in the website, including the email address, the password, and maybe some other personal information. The best way to keep the secrecy of such information is by simply not collecting them. In our website, we adopt a different way by not collecting personal information. The case number which can be regarded as personal, is well protected by the cryptographic methods in Section III.

- **(High Signal-Noise Ratio)**. Not only the long-term inactive results can cause confusion as described in *Traceability*, some false-check also influence the results of "checkee.info". Sometimes, people are told by the visa officer that the visa has been approved. When they go home and check ceac.state.gov at once, they find the status of their visa is *administrative processing*, and submits their cases into "checkee.info". However, that is a temporary status for everyone after the interview, and may not reflect an administrative processing. Such incorrect result confuses many people, and they are wondering *why someone else is cleared soon*, and *why someone is cleared within 4 days*. Such noise is needed to be removed. In our system, we use a wizard-like system for case submission, which will teach the newcomers to understand our definition of administrative processing and take a rest. It will ensure the high quality and clarity of the records in the website.

- **(Strong Security Notion)**. Only when the administrator of the website and the server is together taken down, can the case number stored in the website be leaked. In other words, even if the server is compromised, the case number remains secret. The proof is in Section III.

- **(Simple Authentication)**. The website "checkee.info" uses the email address and the password as the authentication credentials. Consider that the storage of the password would be likely leaked and served as the database for social engineering. Our system does not require the user to leave a password in any form. Instead, we consider the case number (starting with AA) as the sufficient authentication secret for the case. The conclusion for this is due to the nature of public submission of the system.

- **(Helpful)**. There are many common mistakes in understanding especially in counting the processing days. To make the website helpful, we provide the counting of working days instead of calendar days. A simple anticipation is also provided to the user to persuade the user to believe that *Your case is impossible to be completed this week*. The convenient calendar, the wizard-style submission system, the lightweight update system are what we are trying to be helpful.

To satisfy the above goal, we implement the system with security mindset and cryptographic primitives, in the order to answer the following question.

Can we have an administrative processing tracker system with strong privacy guarantee and high SNR?

2 Security Clearance

There is no need for visa applicant to understand what the detailed procedures of security clearance are. If that detailed procedure is leaked, it is subject to be abused by terrorists and spies, then very comprehensive investigation techniques will have to be introduced. As follows, we provide the basic necessary information.

For you, administrative processing means waiting. However, for the visa officer, it means documentation. Whether you are a classified person or not, is only known by the Washington D.C. rather than everyone in the embassy or the consulate, so a request for security advisory option (SAO) would be filled by the visa officer after necessary materials are collected.

Then several governmental institutions in Washington D.C. will start to handle your case, together with millions of other cases. Due to the high volume of application materials, and the impossibility of ignoring any suspicious trace, it will take a long time.

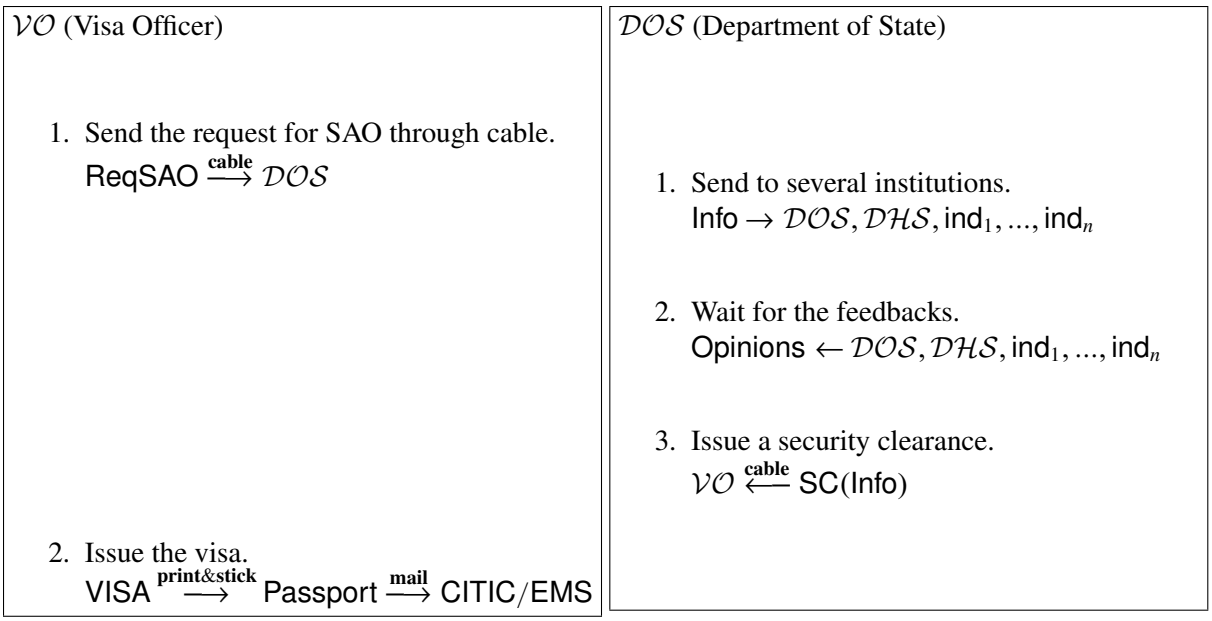

Figure 1: A sketch of security clearance processing.

After the SAO, a security clearance is provided to the visa officer, who is generally starting to issue the visa. In the stamped visa in your passport, you will see "clearance received". The officially reported waiting time for administrative processing is 30-60 days.

Lessons from Section II. Security Clearance

- It is of no use to inquire the details of your case if it does not exceed 30 days in general.
- Unless the security clearance is issued, the embassy/consulate has nothing to do with your case.
- The case is handled by those with the access to confidential database, rather than the embassy/consulate.
- The consuls has to interview in the morning, you can track your status in the afternoon.

3 Encryption and Authentication

To ensure the secrecy of the case number, we adopt the asymmetric encryption with RSA-4096. It is well-understood that incorrect usage of RSA, especially the textbook version, would make it easy to decipher. In our system, we use the library of OpenSSL to generate and provide encryption/decryption with necessary padding. For interested readers, we simply introduce the asymmetric encryption in our system.

1. **(Initialization)**. The website administrator generates a pair of public key and private key.

$$\mathsf{pk}, \mathsf{sk} \leftarrow \mathsf{RSA.KeyGen}(1^{\lambda})$$

   The public key is given to the website server, while the private key is kept secret by the administrator.

$$\mathsf{pk} \xrightarrow{\textbf{outsource}} \mathcal{S}$$

2. **(Encryption)**. The website encrypts the case number upon receiving. It will not store the plaintext case number.

$$\mathcal{C}(\mathsf{caseNumber}) = \mathsf{RSA.Enc}(\mathsf{pk}, \mathsf{caseNumber})$$

3. **(Decryption)**. The administrator retrieves the case number of a waiting case.

$$\mathcal{C}(\mathsf{caseNumber}) \xrightarrow{\textbf{retrieve}} \mathcal{A}$$

   The administrator then performs a decryption.

$$\mathsf{caseNumber} = \mathsf{RSA.Dec}(\mathsf{sk}, \mathcal{C}(\mathsf{caseNumber}))$$

4. **(Cleanup)**. When a case is labelled as clear, the server will remove the case number. It ensures that only pending case numbers are stored.

$$\mathcal{C}(\mathsf{caseNumber})' = \perp$$

Another work is on the authentication which we uses only the case number. We try to ensure that the authentication credentials $\mathbf{F}(\mathsf{caseNumber})$ is one-way, i.e. hard to guess $\mathsf{caseNumber}$ from $\mathbf{F}(\mathsf{caseNumber})$. The function we choose is a secure hash function SHA-256.

1. **(Hashing)**. The website hashes the case number upon receiving.

$$\mathcal{H}(\mathsf{caseNumber}) = \mathsf{SHA256.Hash}(\mathsf{caseNumber})$$

2. **(Verifying)**. The website can verify whether the entered case number is corresponding by the comparison of hash.

$$\mathcal{H}(\mathsf{caseNumber}) \stackrel{?}{=} \mathsf{SHA256.Hash}(\mathsf{caseNumber}')$$

4 Conclusion and Future Work

In this draft, we briefly describe the building of ustravelap.com, a privacy-preserving administrative processing tracker website with high SNR. When more information is available for the website, the machine learning mechanisms can be used for case-specific prediction of clear date.