The privacy risks of RF technology in e-Passports

Privacy and Identity

2533 words

September 1, 2018

Radio frequency identification and e-Passports

Radio frequency identification, RFID for short, is making an appearance in almost every aspect of our daily lives. A lot of products we carry with us have RFID tags in them including our clothes, phones and passports. Not all RFID tags are the same, there is a wide variety of them. We mainly divide them by their used frequencies. Tags that use a lower frequency have a longer range and vice versa. Another key difference is whether the tag requires a battery or not. Some tags are passive and do not require a battery because the reader provides the energy for them. Other tags have a battery included and can thus send out signals without a reader. These tags are called active. In this paper we will look at the tags that are present in e-Passports[1]. Governments want to keep up with the current latest capabilities and requirements and thus decided to put passport data in a chip. This data is protected with a key that is printed on the passport (or ID card) itself. This way customs can unlock the chip with the key on the passport and read out the information that it stores. Initially, the passport chip only stored a digital facial image but later, also fingerprints were added to the chip. There have already been some issues with the e-Passport in the past. One of these issues allowed one to determine the country of origin of a passport without a valid key. Another issue allowed one to guess the key and access all information stored upon the chip. We will investigate the privacy and identity aspects of RF technology in e-Passports and try to come up with some solutions for the issues that e-Passports cause.

Privacy and identity issues

We have already seen that e-Passports are not always as secure as promised. We will now look at the privacy and identity issues that arise when enrolling e-Passports.

Biometrics

Sensitive data is stored upon the chip present in the e-Passports. Not only is your face stored in the chip, also biometric data, namely fingerprints, are saved upon the chips memory. Specifically, this fingerprint data is stored as an image. This means that if one could access the chip, this data could be stolen and reused for other purposes. As stated by the authors in *Finn, Wright, and Friedewald's Types of Privacy*, biometric data should be kept private. The storage of this biometric data upon a chip thus violates the *Privacy of the person.*

Unique identifier

Another issue arises when looking at the protocol that is used by the RF chips in e-Passports. The ISO14443 standard defines the rules for communication to and from the chip. These rules specify that at protocol initiation, the chip ID is send to the reader. Most of the RFID chips have

[1]The tags that are present in e-Passports are a different version of RFID tags, a more advanced one with more capabilities. They will be called *tag* or *chip* from now on.

a unique identifier. If the chips that are present in the e-Passport all have a unique ID, this could be used to track individuals without them even knowing. Placing multiple readers on a specific location could allow someone to precisely track your movement. This unauthorized tracking is a major privacy breach and threatens the *Privacy of location and space*. This type of movement tracking is very similar to Wi-Fi tracking that is already used in stores now. Tracking an RFID tag through a store is even more dangerous than Wi-Fi tracking because most of the times, a Wi-Fi enabled device can be turned off. RFID tags lack the existence of an on/off switch and once rolled out, will always be "on".

Infinite lifespan

This brings us to the next issue. This insecurity issue has to do with the lifespan of the chips. The chips in e-Passports do not have a battery and, once rolled out, have an infinity lifespan. The data that is stored upon the chip will thus be stored forever. This means that encrypted data stored upon the chip is not secure anymore. When the encryption gets broken, a lot of vulnerable e-Passports are still in regulation. This is not the only problem with the encryption. With a normal passport, identity theft occurs when someone steals your passport or makes a copy of it physically. Most of the times, the victim knows that it has happened and goes to the corresponding authorities to revoke the passport. This totally differs from the way e-Passport data could get stolen. With broken encryption a passport could be read out at a distance without the victim knowing it occurs. This way the victim only knows his data has been stolen after the attacker has used it for malicious purposes.

Bad cryptography

Another insecurity issue arises when looking at the cryptographic key used by the reader to communicate with the e-Passport in combination with the storage of fingerprint data. The key is optically stored on the passport. A reader thus looks at the passport to derive the key and can then communicate with the chip. Once the key is known to the reader, the reader has infinite access to the passport. Together with the storage of biometric (fingerprint) data, this creates an insecurity issue. Someone traveling to a foreign country gives them access to all their personal data stored upon the passport including the fingerprint data. Parties that also use the passport (like a car rental company) have access to the data stored upon the chip because anyone with physical access to the passport can read out its entire content.

The Laws Of Identity

In the previous chapter, we have identified some issues that arise when using the e-Passport. In this section, we will look at *The Laws Of Identity* and how they apply to e-Passports.

In the previous chapter, bad cryptography was stated as an insecurity issue. This issue can also be applied to the second law in *The Laws Of Identity*. This law states that information should only be given to a party on a "need to know" basis. For a car rental company, only some of the information on the passport is needed. Fingerprint data, for example, is definitely not needed. The chips in e-Passports however are designed to give access to all information stored when the correct key is used. The collection of personal data by a specific party (almost) always requires consent of the victim where the data is gathered from. This consent is normally given by the passport holder when handing the passport to another party for identification purposes. However, with tags in passports, reading can occur at any moment without the user knowing. The tag present in the e-Passport is encrypted so information stored upon that tag can not be read out by random individuals. However, as we have already seen, information can leak from the tags. An example of this has already been discussed. Tags present in the earlier e-Passports did send out specific error messages that related to the country of origin of the passport holder. This

information can be obtained without the users consent. This was a bug but it relies heavily upon how RF technology works. RF technology is designed to always communicate to everything that asks for it without notifying the user or in other ways making the user aware this is happening. This violates the fourth law of *The Laws Of Identity*. RF tags emit an omni-directional public beacon. The usage of these tags for a passport holder breaks the fourth law. The e-Passports should only respond to public beacons that are emitted by trusted readers. They should not be emitting signals to everything that asks for it. The final law we will discuss is the seventh law of identity. This law states that different identities must be used when dealing with different parties. We thus must choose what information we share with different parties. The implementation of the key into the RF chip on the e-Passport does not achieve this. When the key is revealed, all information stored upon the chip is accessible rather than parts of the stored information.

Data protection laws

Before looking at the data protection laws, we must first determine whether they apply on e-Passports. The data protection laws apply if personal data is being processed. Personal data is information relating to an identified or identifiable natural person. Most of the data that is present on an e-Passport can be used to identify someone (such as someone's name). The processing of this data occurs when any set of operations is performed on the e-Passport. This means that anyone interacting with the e-Passport is processing personal data and we can thus apply the data protection laws to e-Passports. For data processing to be legal, we must look through the GDPR and see whether e-Passports comply with this law.

Processing grounds

Every activity that is subjected to the GDPR should have a valid processing ground. One of the processing grounds that the GDPR allows is due to legal obligation. e-Passports fall under this legal obligation because the government is obligated to hand out passports (and you are obligated to have one). From the perspective of people using your e-Passport for verification or identification, other rules apply. Most of the time they rely on consent or also on legal obligation.

Data protection principles

The GDPR states that an organization that is processing personal data must comply to the data protection principles. We will take a look at some of them. One of the principles states that data should only be collected when its use is relevant. This is the point where some discussion arises. The storage of fingerprint data upon the e-Passport is, for some people considered to be not necessary. The old passports never had fingerprint data on them so why should the new ones contain this very sensitive data? Other people may argue that the government could use this data to provide a faster or more secure way of identification at, for example, an airport. The government should be really careful protecting biometrics as they are stated as very sensitive information under the GDPR.

Data subject rights

The data subject rights ensure that personal data of data subjects remain under the control of the data subjects. Because your passports is such a sensitive part of information, data processors that process your passport data should be aware of the rights stated in the GDPR. Most of these rights are rather straightforward because a lot of the data on your passport will not change over the years. Also you are obligated to have a passport so deletion of data is out of the question. These rights are thus either non applicable or already taken care of.

Accountability

The GDPR also states that the controller should be aware by what personal data it processes and how it should secure these types of personal data. This means that the government should, at all time, make the appropriate measures to secure our personal data.

Privacy enhancing technologies and other improvements

We have seen that there are a lot of issues regarding the new e-Passport. Some of these issues are caused by the usage of RF technology. Others are caused by the implementation of the RF technology into the e-Passport. In this section, we will look at some solutions for the problems we encountered in the previous chapters.

Hashing

The first issue we will address is the storage of plain data upon the RF chip. The storage of this plain data is a privacy issue because, if an attacker could get access to the chip, he could steal your face and fingerprint data. We could solve this issue by creating a hash of this data and, when verifying, creating a fresh hash and comparing the two. This brings some technical issues with it because if the data that goes into the hash function is not exactly the same as the prerecorded data, the hash function will yield completely different outputs. Luckily, a different type of hash functions exist that can also compare data that is almost the same as the prerecorded data. This type of hashing could thus be used for comparing fingerprints and facial images. This means that the storage of biometric information gets avoided and thus increases the privacy aspects while maintaining the current function. This means that the hash acts as a pseudonym for the original data. Someone with the hash can still copy that hash but your fingerprint data will remain safe.

Turning off your e-Passport

Another big issue with e-Passports is the lack of an off switch. Everyone that is in a close enough radius to you can interact with the e-Passport without you knowing. We need to create a situation in which the owner of the e-Passport can only activate its chip when he or she needs it and otherwise put it in "sleep" mode. This way, unauthorized and unwanted access to the chip gets avoided. This can be done in a couple of ways including Faraday cages and physical on/off switches on the chip itself. This solution results in an increase of sender anonymity due to the fact that the chip can not be read out at any moment anymore. Also link-ability from a passport the the passport holder decreases because it is physically turned off.

Information regulation

The implementation of the e-Passport in the way that is done now creates, in some cases, an overkill. When, for example, you only need to prove you are eighteen, or when renting a car, biometric data is not needed. The user however can not decide whether he wants to only give a birth date, or name. It is an absolute decision, the user gives out all information or the user gives out no information. The latter may result in exclusion of certain services (such as not being able to buy alcohol or renting a car). This situation must be avoided by creating a privacy friendly environment that gives the user the control over the data it is giving to other parties. This can be achieved by, for example, implementing an IRMA based system. This system could look like the following. The user has a smart card that has a chip on it and can interact with a special terminal. This terminal is present at each place where e-Passports must be checked. The card is placed in a terminal and the user enters its PIN. After that, the terminal gives the user the choice whether to hand over different types of information. This creates a more privacy aware environment because a lot of information is kept secret from parties that do not need that information. This PET will

increase the anonymity of the passport holder because not all data that is on the passport needs to be given to a verifier.

Conclusion

The enrollment of RF technology into the new e-Passports brings with it some difficult privacy and identity problems. The government should consider removing biometric data from the passport as it is very sensitive information that can not be changed when leaked. e-Passports are a leap into the future but the government should be more careful when enrolling such a privacy sensitive "device". In a privacy aware environment, information regulation should exists so that the user can decide whether he or she wants to give out certain pieces of information.

Bibliography

- Beugelsdijk, R. (2006). RFID, Veelbelovend of onverantwoord? Bijdrage aan de maatschappelijke discussie over RFID (CBP).
- Hoekman, J., Hubbers, E., Jacobs, B., Oostdijk, M., Schreur, R. W.. Crossing Borders: Security and Privacy Issues of the European e-Passport.
- Spiekermann S., Evdokimov S.. Privacy Enhancing Technologies for RFID – A Critical State-of-the-Art Report
- Information Commissioner's Office (2006). Data Protection Technical Guidance Radio Frequency Identification.
- Hennig, J. E., Ladkin, P. B., Sieker, B. (2004). Privacy Enhancing Technology Concepts for RFID Technology Scrutinised.
- Juels, A., Molnar, D., Wagner, D.. Security and Privacy Issues in E-passports.