New Approach to Passport Authentication and Security: Self-Printed Passport

Abstract

Passports are legal documents that allow you to pass from one national to another. Technology developed on passports gained momentum after 9/11 attacks in United States of America [1]. Standards are being offered to all countries by the United States of America. These standards are accepted by almost every country today. Biometric photography, one-dimensional barcodes and RFID (Radio-frequency identification) technologies are among the technologies used in passports [1]. Yet these technologies do not change the fact that passports can be copied. In order to make it difficult to copy passports, create a self printed passports. This kind of passports are the only documents available on the printed copy from citizens. These works include the use of 2D barcodes, the detection of invisible colours on special paper, the use of public keys and private keys in encryption and decryption. In this paper we are going to create imaginary passports with these security technologies. We will compare the fictitious passport that we have created with the passport security technologies that exist in the day. We will then tell you how these technologies can cause security vulnerabilities in our imaginary passport. We will list the problems caused by these vulnerabilities and close the exploits.

Introduction

Passport is a basic identity document deemed valid to overcome international borders. Passports are generally considered to provide decisive evidence of a person's citizenship [2]. Passport is the state, the owner of the passport, and provide diplomatic protection for citizens connected to entering the citizenship country [2].

Security of the passport is really important since immigration is a huge problem in today's world. Specially after several conflict around the world increase immigrant number dramatically. In order to increase of migrations decide to improve their password uniqueness with several security addition. Actually before the 9/11 attacks in united states, passport security was not considered widely [1]. After terror attacks in USA, American federal governments defines passport standards for USA, foreign comers. Many special security technologies which increase also implemented on passports. After many different addition to security still security of the passports are issue in all around the world.

Let's continue with today's passport protection. Before 9/11 passports only include tracking id and image for the authentication of the foreign comers. It seems easy breakable, since many governments do not share any documents which related with their citizens, another country. Only possible to getting other countries citizen information is getting information from visa. Visa applications allows to investigating another countries citizens for accepting to pass border of the country. This kind seems valid authentication but this kind of human-involved protections always reachable. These weakness compared with our solution in comparison part of the paper [1].

After 9/11 US government sees that this kind of security is easily breakable. And they decide that to improve it with technology. But improving with technology is not enough. Every country should apply same technology for their passports. Reason of this US government, establish a company to spread to world [1]. These companies responsible to define standards of the passport and implement latest security measures.

This technological protections available and published for every country for spreading it out. Some of the technological improvements are using barcodes, special papers, standardised citizen photos (biometric photos) to face detections and RFID's.

These techniques fail some cases. In order to improve these techniques, alternative and self-printed passports might be used in future. Let's start with today's passport protection technologies.

Present Passport Security Technologies

Today's technology trends on security on the passports listed. Both advantages and disadvantages can be found below.

a) 1D Barcode

We are using barcodes everywhere. In shopping malls, cargo deliveries… etc. Simple 1D barcodes include black lines, with the barcode reader machine this black lines converted to desired numbers [Figure 1]. Each line's thickness define one number in the barcode. In almost every passport contains barcodes today. When border pass, border police read barcode data with barcode reader to getting information of the foreign comers. These barcodes uses for retrieving data from international databases.

Figure 1: *1D Barcode****

Barcodes are initially good way to accessing data. But they can be easily copied. Barcodes not related with the authentication they directly related with the retrieving data. Copying barcodes are not the case. Barcodes can be accepted as a confidentially in terms of security.

b) Biometric Informations

Biometric portrait photos are standardised for the face detection. In many airports in US, border checks have cameras which improved for face detection [Figure 2]. Today many countries passports include biometric photos. These photos compared with the foreign comers faces. This is one of the authentication technique for the passport. Also international databases include these biometric photos. As we mentioned barcodes used for retrieving data. With barcodes border police access database which include biometric photos. Also these biometric photos compared with the foreign comers himself and his

Figure 2: *Biometric Information (Canada Passports Standards)* [4]

biometrics photo which is present on the passport.

Biometric informations also include fingerprints. Increasing of the terror thread, finger print required on visa applications [Figure 2]. These kind of informations stored on international trusted databases and shared with the all governments databases for improving security measurements.

As figure illustrates that both finger prints and biometric photos can be required for both applying visa and taking passport.

c) RFID (Radio-Frequency Identification)

Radio Frequency Identification (RFID) technology is a method of recognising objects individually and automatically using radio frequency [2,3]. RFID basically comes from a label and reader. RFID tags can be programmed to receive, store and send object information such as Electronic Product Code (EPC). Information on supply chain management can be automatically recorded or changed as the reader reads the labels placed on the product [2].

RFID systems works like barcodes. Unless can't easily copyable since RFID chips are electronically coded. These chips can be read by RFID reader for retrieving data from international databases.

RFID technologies started used for national identifications cars in US in 2006. After that they standardised for the further uses. Again like barcodes they are widely used for passports around the world. And standardisation institutes defines standards of RFID uses on passports globally [1].

This technology not only used for retrieving information they can be also good way to validate passports are real passport or not.

d) Special papers, and UV lights

Special papers widely use for money. Reality of the money can be satisfied with special paper and materials. These materials interact with different colour spectrums to validate money. Same case applied to passports commonly. Many countries use these kind of papers to interact with UV light to show invisible validation numbers.

Why passport security needs new technologies

Globally immigration increase cause increase illegal actions to passing borders. People start to find a way to access globally improved countries. This is brings huge opportunity to people who earns money from illegal access such as creating fake passports. As we mentioned before governments spent huge amount of money to improve technologies behind passport security. But people can some how reach the security barriers to create fake passport. Due to lack of technology some countries cannot apply globally accepted standards of passports. Most of the illegal actions happened against to passports. Let's consider barcodes, barcodes can easily copied. RFID chips can be hacked or replaced with different chips.

We can categorise current passport threats as a three groups [1]. These threats are data leak, copying identity, biometric thread.

For preventing these threads. We can create case scenario for better understanding.

Assume that there is not passports exist like booklet. Citizens print-it out their passports themselves via printers. In our test case only validation techniques are fallowing techniques. These are, two-dimensional barcode scanner, colour monitor, cryptographic software, public keys of password authentication.

Methodology

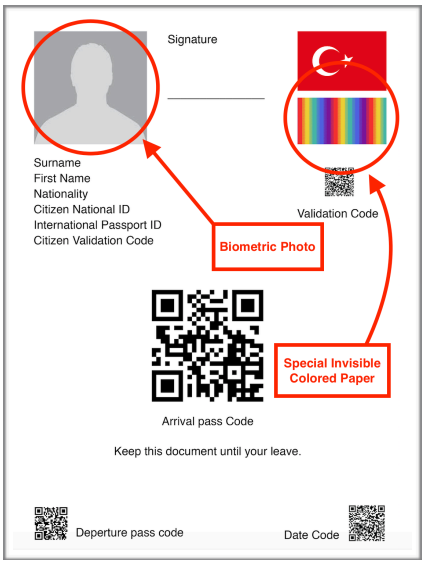

Figure 3: Self Printed Passport*

According to our case scenario to improving passports given left hand sided figure [Figure 3]. This figure illustrates passport which include technologies under limited technologies.

First our self printed paper is special. They can provided from governmental agencies. As you can see from figure 3, there was a special colour palette invisible with naked eye. This is security measurement agains the passports validity. With these special papers, the use of any paper as a passport is avoided.

This papers can be only read with colour monitor. Colour monitor is connected with device which can read invisible colours.

This monitors works like money validation systems. These systems also applied on current passports as we mentioned previously.

2D - Barcode:
In our case scenario and in real life unable to implement RFID to printed paper. For more usability using RFID is impossible to user on it. In our printed passport, 4 Different 2-D barcode can be used as accessing information from border leave and border entrance. Using 4 different 2-D barcode makes our self-printed papers more unique. As you can see from figure 3, there is 4 different 2-D barcodes available. Two barcodes exist for departure and arrival, one barcodes are exist for approving passport and lastly date barcodes are exits.

We are using 2-D barcodes since they are gives more opportunity to combine different barcodes than 1-D barcodes.

In our case scenario there was a 4 different 2-D barcode readers available for each barcodes. It increases the validity of the passport.

Digital Signature:
An electronic signature or digital signature is an electronic signature that has been added to another electronic signature or has a logical link with the electronic signature and is used for authentication purposes. Also known as e-signature[5]. It is a legal authentication system that can be used instead of a signature in electronic media [5]. Especially because of the rapid rise of e-commerce gains more importance. Signed by electronic signature, signed by whom and credibility is checked. Electronic signature; That the integrity of the transmitted information is not corrupted and that the information is transmitted by verifying the identities of the individuals.

Public key encryption is the part of the digital signature. Public key encryption is a cryptography system in which different keys are used for password and decryption operations. Each of the communicating parties has a pair of keys [5]. One of the keys forming these key pairs is the secret key and the other is the open key. When one of these keys is encrypted with one, the other is decrypted. These two key pairs are mathematically related to each others [5].

Private key is the crypto key that security threats will occur only when two people who are communicating with each other are aware of it and someone else's hand over it. The private key is used in symmetric encryption applications. In public encryption, the private key signature key is also called the "signature key" [6]. As the security is removed when the personal key is played, it becomes widespread to use both private and public encryption [6].

Public and private keys can't be imagine separately, They complete each others [5,6].

2-D barcodes should include hashed code. We are provide special readers but, in case of theft, we need to encrypt information which is present in 2-D barcode.

In our case scenario we are going to encrypt our barcode codes with private key and decrypt codes with public keys.

This operation requires authority which is trusted it may cause issue between governments. 4 different barcodes can be encrypted and decrypted with different authorities.

Comparison between self-printed passport and traditional passport

Self printed passports can be seems more secure with below arguments.

Traditional passports can be modified, but self-printed passports are disposable - only one time use -. This increase uniqueness and decrease changeability of the passport.

Moreover using encryption and decryption (digital signature) it increase confidentiality of the passport. But in this case trusted authority may cause problem. For the solving this issue, 4 different 2-D barcodes can be used for specified for the countries. 2-D barcodes increase variety of the barcodes.

Self-printed printed passports also include colour monitored paper. These papers provided by governments to citizens. These papers increase validity of the passports.

Conclusion

Passport is one important tool against uncontrolled immigration. Its importance increase after 9/11 dramatically. Governments spent millions of dolors for ensuring security on passport securities. But today's main security gap on passports are lack of standardisation. Due to technological gap between countries house this issue. With self-printed passports, it can be avoid to passport differences.

References

[1] Kundra, S., Dureja, A., & Bhatnagar, R. (2014). The study of recent technologies used in E-passport system. In 2014 IEEE Global Humanitarian Technology Conference - South Asia Satellite (GHTC-SAS) (pp. 141–146). IEEE. https://doi.org/10.1109/GHTC-SAS.2014.6967573

[2] Ezovski, G., & Watkins, S. (2007). The Electronic Passport and the Future of Government-Issued RFID-Based Identification. In 2007 IEEE International Conference on RFID (pp. 15–22). IEEE. https://doi.org/10.1109/RFID.2007.346144

[3] Radio Frequency Identification Technology in the Federal Government Components of an RFID System. (2005). Retrieved from www.gao.gov/cgi-bin/getrpt?GAO-05-551.

[4] CCA Standards, Figure 41~A, Canadian Biometric Photo Standards, http://www.cic.gc.ca/english/resources/publications/biometrics-eval/section6.asp, ACC, (2014)

[5] Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. Communications of the ACM, 21(2), 120–126. https://doi.org/10.1145/359340.359342

[6] Buchanan, W. J. (1999). Private-Key Encryption. In Mastering Networks (pp. 300–310). London: Macmillan Education UK. https://doi.org/10.1007/978-1-349-14966-7_18

* Imaginary passport designed by author.
** Barcode figure taking from web, with no copyright