E-PASSPORTS AND AUTOMATED BORDER CONTROL KIOSKS: A RECIPE FOR HACKING

Kelsey Wheatley
(Postgraduate Student, MA IREL Global Program, Webster University, Missouri, USA)

Publication date: 17 September 2017

The flow of people around the globe has become a heightened concern for international security analysts. While ease of travel is an advantage of a developing world, the logistics of international migration can threaten the security of the borders. To combat these risks, airports began using advanced technology to not only decrease the time travelers spend in Customs, but to simultaneously make the borders more transparent, yet stronger.

It has become imperative that states track the influx of foreigners to monitor both who enters and exits the country. This development came from the need to ensure those who are supposed to be exiting the region per visa limitations or other regulations are actually leaving the country. U.S. Customs and Border Protection (CBP) implemented the Automated Passport Control (APC) program in conjunction with the pre-existing e-Passport technology to more effectively and accurately monitor this movement. The new machines debuted in the United States in 2013, but the United Arab Emirates, Australia, the United Kingdom and several other states have begun to use the automated border control (ABC) systems.

Travelers enthusiastically traded in filling out the paper customs declaration forms for simply scanning their passport, taking a picture and tapping a few buttons on the automated passport kiosks. The new technology uses biometric data including facial recognition, iris scanning or fingerprint matching, but not all travelers worldwide are required to submit this data when applying for a passport (Kephart 2013). Therefore, some question whether obtaining this data is aiding with transparency (Knaus 2017).

Are these machines secured?

The U.S. Department of Homeland Security states on its website that passengers' biographic data is not stored in the APC technology. It also says, "Travelers' passport information and answers to the declaration questions are submitted directly to CBP via secure encryption protocols" (U.S.

Customs and Border Protection 2017). Therefore, one could assume that these machines are not particularly intrusive. While this may be true in the United States, however, not all airports use the same technology, so the ability for hackers to gain access to stored data in other airports seems probable.

In the Philadelphia International Airport, there was a glitch in the automated kiosks soon after they were installed, which angered passengers who were promised a speedy and secure experience upon arrival (Loyd 2014). Since the technology is relatively new, cyber hackers can take advantage of these weaknesses to expose its vulnerabilities.

There are two main risks concerning the ABC kiosks right now. The first is the potential for hackers to penetrate the ABC kiosks. Although improbable, the possibility cannot be ignored. Hacking into "secure" data happens almost on a frequent basis. University of Wollongong biometrics expert Professor Katina Michael said, "recent threats to the security of government-held data such as the [Australian] census failure should raise real concerns about the storage of biometric data en masse" (Knaus 2017). Last week, the credit reporting company Equifax also reported that it suffered a security breach earlier this year (Yurief 2017). Where there is computerized technology, there is hacking.

The duplication of passports is another issue that stems from their digitalization. Lukas Grunwald, a German computer security consultant, explained how he easily cloned the data from the e-Passport and then demonstrated how he could scan the cloned passport chip instead of the original chip (Zetter 2006). *Therefore, someone with a forged passport could easily circumvent security protocols and enter a country with ABC kiosks (Zetter 2006). This would grant terrorists the ability to enter a country of their choosing virtually undetected.*

Ultimately, each airport that employs the APC kiosks maintains that the technology is secure and that the data is transmitted from the kiosk to the border patrol agent through an encrypted server. However, with any new technology, there are legitimate risks that must be considered.

Who is at risk?

Individually, each traveler that enters his or her information into a kiosk could be at risk. Even though various security professionals confirm that the kiosks operate under the highest security standards, Professor Michael said the automatic border control plan "posed a risk to individual privacy and raised ethical dilemmas that had not been properly explained to the public" (Knaus 2017).

Refugees and asylum seekers will also feel the ramifications if this data were to be compromised. In that case, states would prioritize border security over allowing foreigners into their countries, so gaining approval for relocation or asylum would be difficult for refugees.

With the refugee crisis surmounting all over the world, it has become increasingly important that borders remain secure to ensure the current immigration restrictions can be enforced. Leakage of this data would not only harm the individual passengers and compromise their personal security—it would threaten the security of the respective country. Passports could be replicated

and sold on the black market, where refugees would eagerly buy them because of the potential to escape a tumultuous and dangerous situation.

Concluding Remarks

Since the automated passport kiosks are relatively new, there have been no known instances of attempts to hack the systems. However, even though there have been no detected attempts that do not mean that they do not exist. At a time when refugees are willing to risk their lives simply to leave their homes, illegally obtaining a foreign passport to give them a chance at a new life is arguably morally excusable in their minds.

Therefore, passport security is a priority not only to ensure the security and integrity of the current passport holders, but to confirm that the border controls are functioning properly and can welcome those returning home, embarking on travel or seeking asylum. If this technology is compromised, the security of a country will be at risk and states might be less willing to expose themselves to the vulnerabilities of accepting refugees. Closed borders would only exacerbate this current international crisis. Therefore, it is imperative that security officials constantly monitor the ABC kiosks to promote international security.

Bibliography

Kephart, J. (2013). Biometric exit tracking. *Center for Immigration Studies.* Retrieved from https://cis.org/Report/Biometric-Exit-Tracking

Knaus, C. (2017). Biometric recognition at airport border raises privacy concerns, says expert. *The Guardian.* Retrieved from https://www.theguardian.com/technology/2017/jan/24/biometric-recognition-at-airport-border-raises-privacy-concerns-says-expert

Loyd, L. (2014). Snag at PHL's Customs kiosks angers travelers. *The Inquirer Philly.com.* Retrieved from http://www.philly.com/philly/business/20141002_Temporary_snag_at_PHL_s_automated_passport_kiosks_angers_travelers.html

U.S. Customs and Border Control. (2017). Automated Passport Control (APC). *Department of Homeland Security.* Retrieved from https://www.cbp.gov/travel/us-citizens/apc

Yurief, K. (2017). Equifax data breach: What you need to know. *CNN Tech.* Retrieved from http://money.cnn.com/2017/09/08/technology/equifax-hack-qa/index.html

Zetter, K. (2006). Retrieved from http://www.wired.com/news/technology/1,71521-0.html