Secure Communications for Mobile Verification Platforms

Emmanouil Kafetzakis*, Nikolaos V. Boulgouris†, Emmanouil Panaousis‡ and Anastasios Kourtis*

*National Center for Scientific Research "Demokritos"
Institute of Informatics & Telecommunications
{mkafetz, kourtis}@iit.demokritos.gr

†Brunel University, London
Department of Electronic and Computer Engineering
nikolaos.boulgouris@brunel.ac.uk

‡Queen Mary, University of London
School of Electronic Engineering and Computer Science
panaousis@eecs.qmul.ac.uk

***Abstract*—This article discusses security issues of passenger verification platforms, deploying mobile and portable devices, which will enable authorities to conduct fast, secure and reliable checks at land/railway border crossing points. The automated passengers verification facilitates the efficient, high-speed processing of biometric information and documentation at border control points without compromising security or requiring major infrastructure investments. From the passengers point of view, faster cross border checking increases convenience by eliminating the need of waiting in long queues.**

I. Introduction

Every year, millions of visitors enter the European Union (EU) by cars, buses or trains [1]. Several EU regions near borders attain significant economic and benefits from these visits and, as a result, the established EU policy is to encourage and facilitate cross-border travel. For this reason, EU has embarked on signing agreements allowing visa-free travel within an area which includes EU's Eastern neighbours. These agreements, however, are expected to increase dramatically the passenger flows that EU land border authorities have to control, introducing major implications in the security of all European countries. Concerns about these issues have been officially expressed by several countries during the finalisations of the visa-free travel arrangements.

The lack of pre-travel screening of passengers under the visa-free travel regime necessitates interoperable CCTV and video archive installations [2], as well as high-security identity control at the borders. To overcome this, new border check procedures must be developed in order to expedite border checks without degrading the existing well-established security levels. An appealing way for the expedition of border crossing is to conduct checks using mobile equipment while passengers remain onboard, as specified in the Schengen Border Code [3], [4]. The benefits of using mobile equipment, however, should not come at the expense of lower quality (in terms of efficiency and reliability) passenger control. Instrumental for ensuring efficiency and reliability is the use of biometric identification techniques in combination with reliable (in terms of Quality-of-Service (QoS)) wireless connections that allow secure communications connection to EU large-scale centralized databases (e.g., Visa Information System (VIS) [5], Schengen Information System -SIS- II [6], EURODAC [7], etc.). Such mobile identification systems, the deployment of which is of high priority for EU [8], should overcome existing technological limitations (e.g., mobility support, low cost devices) while respecting current legal frameworks and prevailing social/ethical considerations in order to perform fast and secure checks.

The potential benefits of mobile border checks are expected to be substantial as under the current border control procedures passengers must leave their vehicles and queue. Thereby, any portable and easily-customized devices that can conduct fast, secure and reliable controls, could drastically reduce waiting times by allowing passengers to remain inside their vehicles (cars, buses, trains) during land border controls. For example, 3.42 millions of passengers crossed the Narva crossing point in Estonia [9], which is one of the major land routes linking the EU and Russia, in 2011. This means about 10,000 passengers crossed the border each day. If authentication for each of the crossing passengers could take place 1 minute faster than today, then 6.5 years of queuing time could be saved in a year. Considering all Schengen land border crossing points, it is clear that the potential impact on the cumulative waiting time during land border controls can be very beneficial.

This paper discusses data and communications security issues of passenger's verification platforms when mobile identification devices are deployed. Such devices can be equipped with biometric features allowing authorities to conduct fast and reliable checks at land/railway border crossing points. The main advantage of using mobile and wireless technologies is the supported mobility of the border officials, allowing them to use the devices outdoors or while passengers are still in

ISBN 978-3-8007-3529-7

their vehicles. The wireless connections can be supported by IEEE 802.11 and Long Term Evolution (LTE) technologies to achieve high data throughput with suitable level of security using low-cost commercial devices.

The rest of the paper is organized as follows. Section II briefly reviews the status of land border checks and describes operational scenarios for passenger's identification platforms. Section III focuses on relevant wireless network security aspects, while Section IV discusses security measures in mobile identification devices. Finally, conclusions and future work are drawn in Section V.

II. Definition of Operational Scenarios for Border Checks

The deployment of mobile biometric devices for fast and reliable identification of passengers at land border crossing points can bring substantial benefits. Mobile biometric devices may use heterogeneous wireless technologies in order to exchange data with the core (backend) identification platform. The core platform usually has access to large passenger databases and exploits existing infrastructure and connections of the Border Control Centre (BCC). In addition, mobile devices could use recognition techniques and radio frequency identification readers.

A. Current Status

For land border checks, mobile devices have been increasingly used as they permit controls without the need to verify passengers at a control booth. Such devices can only check the physical security of passports/visas and access the information stored in the chip of an e-passport/e-visa. Thus, current mobile devices are not able to perform biometric controls; following travel document scanning, the procedure is fundamentally the same as that when a control booth is used. In most cases, the task of a passengers identification, i.e., checking if a passport/visas photograph matches the passengers face, remains a task conducted manually by a border officer. In addition, the land border official can be deceived in plenty of ways, for example due to disguiser look-alike fraud. Further, since existing mobile identification devices lack network connectivity, the border official cannot check the passengers profile against the corresponding EU databases. Scenarios I and II, presented below, allow the officers to be always connected to the BCC and therefore with EU databases.

B. Scenario I - Check At the Land Border Crossing Point

Scenario I takes place near to the BCC (see Fig. 1). Due to the short proximity between the mobile identification devices and BCC, the connection between them could be established via a reliable IEEE 802.11 wireless network.

In this scenario, border officials use mobile devices to check the passengers onboard (inside either cars or buses). By using a reliable, fast and secure wireless connection supported by the IEEE 802.11 technologies, each passengers information will be sent to the wireless access point located in BCC and from there to the core platform.

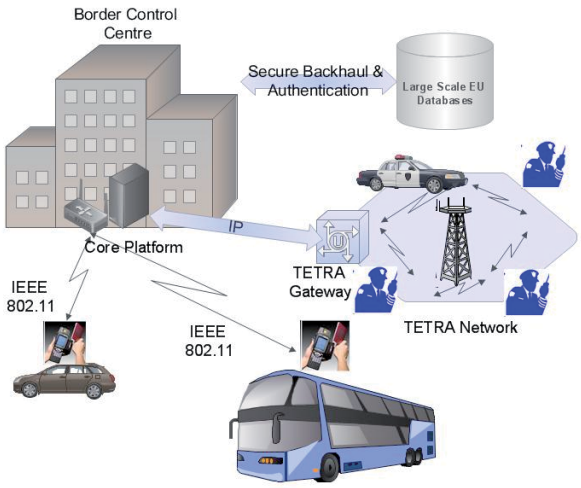

Fig. 1. In Scenario I, due to the short proximity between the mobile identification device and the BCC, secure WiFi communications can be used.

In case that one or more passengers are identified as suspects or perpetrators by the identification platform, then BCC will wirelessly communicate with the border official that performs the control in the field, as well as emergency responders in the surrounding area (through their TETRA terminals) to coordinate the security officers' actions. In order to send group alerts/messages to holders of both mobile identification devices and Professional Mobile Radio (PMR) terminals, a TETRA to IP network gateway is required. The interoperability of PMR systems and IP based telecommunication networks has been largely studied [10], [11], [12] and different commercial products implement interoperability features between the different radio communication systems. Although interoperability has been proved to be feasible in terms of signaling and user registration/management, a remaining problem is the lack of a standardized way of providing services.

C. Scenario II - Check Before the Border Crossing Point

Scenario II takes place inside trains, during transit. In a typical situation, the land border control takes place by disembarking the passengers from the train, which results in long waiting times. Another more convenient way for checking passengers efficiently is to perform the border control inside the train on the move.

For this case, the mobile identification devices could exchange information with the core identification platform in BCC by using Long Term Evolution (LTE) wireless networking technologies (see Fig. 2). To this end, the mobile identification devices are connected to a public network and therefore every security measure should be applied in all levels [13].

III. Security in IEEE 802.11 and LTE networks

The use of WiFi (IEEE 802.11) networks in public places requires a higher level of security based on strict network access

ISBN 978-3-8007-3529-7

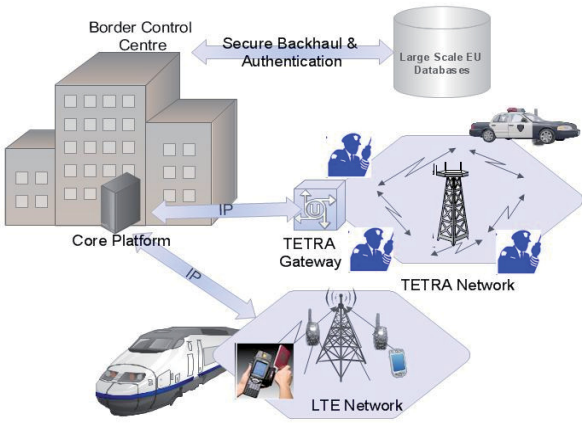

Fig. 2. In Scenario II, targeting a more convenient way to check passengers' flow, land border checks take place inside trains during the journey. The LTE technology is used to enable communication with the BCC.

control and data communication encryption. These requirements were specified in the IEEE 802.1X standard [14], which implements the media-independent Extensible Authentication Protocol (EAP) [15]. The authentication and access control process involves two entities: a wireless users device and an Access Point (AP) that plays a role of authenticator. For key management, the IEEE 802.11i security amendment [16], [17] specifies the key generation and distribution scheme. The unlicensed nature of WiFi creates some uncertainty over the possible application of this technology in border control cases but as argued in [18], [19] there is probably room for unlicensed wireless technologies to be used even in emergency cases.

On the other hand, the licensed technology of LTE makes things more reliable for security-sensitive applications. LTE security is based on an Authentication and Key Agreement (AKA) protocol [20], which enforces network access security and provides compatibility and interoperability with legacy networks such as 2G and 2.5G networks (GSM/GPRS). In LTE, encryption and integrity protection algorithms are based on Snow 3G and Advanced Encryption Standard (AES). Although the security level provided by LTE is high, LTE networks are public and thus are not directly controlled by land border authority. This might lead to situations, where security is compromised. Therefore, careful consideration should be given to the application on LTE in land border control cases.

To address potential vulnerabilities introduced by the commercial nature of WiFi and LTE technologies, we envisage the development of higher layer security policies which guarantee the integrity of the data transmitted to and from the mobile identification devices. Policies should include measures for the authentication of border officials to the mobile identification device and also of the mobile device to the core platform. Device authentication mechanisms will ensure that only registered devices will have access to the servers of the core platform. The security policy should also specify the procedure used by the mobile device in order to identify itself to the core platform servers.

In this context, the identification platform should provide a unified wireless security solution, applicable to both types of wireless connections; LTE and WiFi. This solution has to be applied on top of the existing security mechanisms. It has to satisfy the three main security requirements of integrity, availability and confidentiality for each of the involved technologies.

In this direction, encryption mechanisms at the Internet Protocol (IP) layer (Layer 3) can be implemented, specially tailored to the needs mobile identification. The secure exchange of data can be ensured via the exploitation of Virtual Private Network (VPN) technologies based on IPSec and/or SSL protocols. According to the specialties of each type of wireless network, (technology used, bandwidth requirements, static/mobile conditions), the most suitable parameterization of the encryption solution should be located.

We envisage devices that will be loaded with software implementations of different modules including *3D face biometric authentication* and checks against fraud passengers' documentation (such as passports and visas). These would facilitate different border control procedures, but they would require *fast*, *secure* and *costless* multimedia communications services (such as video, voice and data exchange – texts and images) as well as connection to web-based services.

Multimedia communications will also be provided in a peer-to-peer (P2P) mode when infrastructures (such as 3G/LTE) are not available. Due to the decentralized nature of such a network, different types of attacks can be launched against the devices. We have carried out some initial work with the realm of security for mobile peer-to-peer networks in [21], [22], [23], [24]. Decentralized mobile networking can also reduce cost of mobile data traffic compared to existing *Public Protection and Disaster Relief* (PPDR) technologies imposing no operational cost by using license exempt parts of the spectrum. Therefore, devices can use long-range versions of IEEE 802.11 radio technologies with reduced radiation levels and health hazards for humans and other living entities. Also, the low-power nature of such communications highlight them as a "greener" solution compared to the current PPDR systems (i.e., TETRA).

IV. Security Measures in Mobile Identification Devices

Apart from secure communications, the identification platform should make provisions for additional security functionalities in order to protect the device itself from unauthorized usage. An administration function has to allocate devices to border officials, authorize different roles and, therefore, load different processing modules or give different access to different users. This administrative function should also report and remotely locate, lock, and disable the mobile device when this is stolen or lost [25]. Furthermore, remote operation commands may be issued to change or modify the software of a mobile device that has been lost or stolen, to delete any

ISBN 978-3-8007-3529-7

sensitive data including access codes or authorizations that may have been saved on it.

The mobile identification device selection and a series of other factors affect the architectural decision of the identification platform. Specifically, assuming that reliable and fast ubiquitous network connections exist and that biometric algorithms should be kept secret even in case of theft or loss of the mobile device, it is desirable that biometric matching operations take place on the core identification platform (located at the BCC) rather than the mobile device itself. Subsequently, the cancelable biometrics (i.e., the intentional distorted biometrics) could be transmitted to remote secure servers that will further process the biometric samples and finally match the extracted biometric features with those stored in the passport/visa or EU databases (Scenario 4 in NIST Best Practice Recommendations [26]). Such a distributed IT architecture requires high QoS connections that link the mobile identification devices with the core platform.

V. Conclusions and Future Work

A passenger's verification platform uses mobile identification devices, biometric verification algorithms, and secure wireless networking technologies in order to achieve effective land border control. Considering the mobile and the distributed nature of the presented platform, the article explored aspects of the system in order to allow fast and reliable connections between the different mobile identification devices and the core platform. Our future work will discuss the different types of devices that could be used in the discussed scenarios. Such devices are likely to be vastly deployed in commercial environments thus modifications towards the achievement of an adequate level of security and privacy must be determined. Another important aspect to be examined is the passenger's information exchanged among the different modules along with a message sequence diagram for both Scenarios I and II, during a passenger's verification. Last but not least, emphasis will be given in the different kinds of fraud that can be incurred in such an environment and how these could be identified and mitigated.

Acknowledgment

The authors from National Center for Scientific Research "Demokritos" are partially funded by the European Union Seventh Framework Programme through the SAVASA project, under grant agreement No 285621.

References

[1] BEST Network, "D1.1 Inventory of biometrics enabled registration processes for immigration purposes", 2010.

[2] FP7 SEC SAVASA Project: "Standards based Approach to Video Archive Search and Analysis", [Online]. http://www.savasa.eu.

[3] "Regulation (EC) No 562/2006 of the European Parliament and of the Council of 15 March 2006 establishing a Community Code on the rules governing the movement of persons across borders" (Schengen Borders Code).

[4] European Commision. "The Schengen Area". [Online]. http://biblio.ucv.ro/bib_web/bib_pdf/EU_books/0056.pdf

[5] "2004/512/EC: Council Decision of 8 June 2004 establishing the Visa Information System (VIS)".

[6] European Commision, "Report on the global schedule and budget for the entry into operation of the second generation Schengen Information System (SIS II)", 2010.

[7] Directorate-General Justice, "Freedom and Security", EURODAC Information and communication unit, B-1049 Brussels, 2004.

[8] European Security Research Advisory Board, "Meeting the challenge: the European Security Research Agenda", 2006.

[9] B&S, EUROPEAID/129783/C/SER/multi, "A Study on Common Border Crossings Points Management between Schengen Area and Russia / Belarus", 2012.

[10] ETS 300392-3-1 ETSI TETRA specification, "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 3: Interworking at the Inter-system Interface (ISI); sub-part 1: General design", 1999.

[11] ETSI TETRA specification, "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 3: Interworking at the Inter-system Interface (ISI); Sub-part 3: Additional Network Feature Individual Call (ANF-ISIIC)", 2000.

[12] ETSI TETRA specification, "Terrestrial Trunked Radio (TETRA); Voice plus Data (V+D); Part 3: Interworking at the Inter-system Interface (ISI); Sub-part 3: Additional Network Feature Group Call (ANF-ISIGC)", 2004.

[13] G. M. Haslestad, T. Koien, "Security aspects of 3G-WLAN interworking", IEEE Communications Magazine, vol. 41, no. 11, pp. 82-88, 2003.

[14] IEEE, Standards for local and metropolitan area networks: "Standard for port based network access control", IEEE Standard P802.1X, 2001.

[15] B. Aboba et al., "Extensible Authentication Protocol (EAP)", Request for Comments 3748, June 2004.

[16] IEEE 802.11i, "WLAN MAC and PHY Specifications, Amendment 6: MAC Security", June 2004.

[17] Z. Yang , A. C. Champion, B. Gu, X. Bai, D. Xuan, "Link-layer protection in 802.11i WLANs with dummy authentication", in Proc. Second ACM Conference on Wireless Network Security 2009, pp. 131-138.

[18] E. A. Panaousis, C. Politis, K. Birkos, C. Papageorgiou, T. Dagiuklas, "Security Model for Emergency Real-time Communications in Autonomous Networks", (Springer) Information Systems, Frontiers Journal, 14(3): 541-553, 2012.

[19] E. A. Panaousis, T. A. Ramrekha, G. P. Millar and C. Politis, "Secure Decentralised Ubiquitous Networking for Emergency Communications", in Proc. International Conference on Telecommunications and Multimedia (TEMU), IEEE, Jul 30 - Aug 1, 2012.

[20] (2008, September) 3GPP system architecture evolution (SAE), "3GPP TR 23.882 V8.0.0: Report on technical options and conclusions", [Online]. http://www.3gpp.org/ftp/Specs/archive/23_series/23.882.

[21] G. P. Millar, E. A. Panaousis and C. Politis, "Distributed Hash Tables for Peer- to-Peer Mobile Ad-hoc Networks with Security Extensions", Journal of Networks, Special Issue: Recent Advances in Information Networking, Services and Security, 7(2): 288-299, ISSN: 1796-2056, Feb. 2012.

[22] E. A. Panaousis, G. Drew, G. Millar, T.A. Ramrekha and C. Politis, "A Test-bed Implementation for Securing OLSR in Mobile Adhoc Networks", International Journal of Network Security & Its Applications, 2(4): 1-26, ISSN: 0975-2307, Oct. 2010.

[23] E. A. Panaousis, L. Nazaryan and C. Politis, "Securing AODV Against Wormhole Attacks in Emergency MANET Multimedia Communications", in Proc. 5th Mobile Multimedia Communications Conference (MobiMedia), ACM, Sep. 2009.

[24] E. A. Panaousis and C. Politis, "A game theoretic approach for securing AODV in emergency Mobile Ad Hoc Networks", in Proc. 34th Conference on Local Computer Networks (LCN), Oct.2009.

[25] National Institute of Standards and Technology (NIST). Guidelines on Cell Phone and PDA Security (SP 800-124). [Online]. http://csrc.nist.gov/publications/nistpubs/800-124/SP800-124.pdf

[26] NIST. (2009, July) Mobile ID Device Best Practice Recommendation, Version 1.0. NIST Special Publication 500-280.

ISBN 978-3-8007-3529-7