Electronic services for tourist destination reservations

Milos Ilic
Electrical and Computing Engineering
University of Pristina, Faculty of Technical Science
Kosovska Mitrovica, Serbia
milos.ilic@pr.ac.rs

Zaklina Spalevic, Mladen Veinovic
Singidunum University
Belgrade, Serbia
zspalevic@singidunum.ac.rs, mveinovic@singidunum.ac.rs

Zeljko Spalevic
University Donja Gorica
Donja Gorica, Montenegro
zeljko.spalevic@udg.edu.me

Abstract—**Internet and other electronic and mobile services have changed business industry, and also have significantly revolutionized travel industry in the last decade. In travel and tourism industry, travel products and services appear to be well suited to Internet marketing, based of their distinctive high-priced, high involvement, intangible, heterogeneous, high-risk, and well-differentiated characteristics. Online booking represents important service for end users, travel agencies and hotels. Online accommodation and transportation reservation and payment need to be secure as much as possible. Authors in the paper present technologies that are in use for this kind of electronic services, security mechanisms for online booking, online card payment, and a law regulation for costumer protection.**

Keywords-e-booking; e-payment; SSL security; tourists protection; legal regulations;

I. INTRODUCTION

The rapid development of information and communication technologies in recent decades has resulted not only in drastic increase in speed of the information flow, but also in the number of users of mobile devices. This trend has been recognized and used by many industries, including tourism. The use of specialized application software, compatible with the modern electronic devices, the interaction between tourists and tourist destinations received a whole new dimension [1]. For the purpose of interaction between tourists and tourist destinations different applications are in use. To get basic information about specific tourist destination, user can download application with the help of which he will obtain the necessary information. Benefits of these applications are manifold because they contain information about other tourist destinations too, and can be reused. Through the network, applications update their database with newer information about historical sites, hotels, restaurants, the best way of transportation to destination, and etc.

Hotel search and booking is one of the services provided through these applications, and that is something that is done by everyone who wishes to travel and stay. This process of finding the finest hotel is time consuming, overloaded with information, overwhelming and in some cases poses a security risk to the client. Hotel booking systems have been around for decades and over the years have become more interactive, providing clients of hotels worldwide to book a reservation without having to physically walk into the facility [2]. In 1946, American Airlines installed the first automated booking system, the experimental electromechanical Reservisor. A newer machine with temporary storage based on a magnetic drum. This system proved successful, and was soon used by several airlines for inventory control. It was seriously hampered by the need for local human operators to do the actual lookups. Ticketing agents would have to call a booking office, whose operators would direct a small team operating the Reservisor and then read the results over the telephone [3]. There was no way for agents to directly query the system. Today the online booking system became a trend. Many companies have its own booking API (application programing interface). They are even selling their API to other small companies. To buy or sell the API, the registration and documents should be signed under the rules of the countries e-commerce policy.

The major shift to the online-based hotel booking system generated several advantages for the industry, as it built high possibility of global distribution due to the accessibility of twenty-four hours a day and seven days a week. Self-serving website could help hotel to less stress relying on staff for tasks like accommodation information and booking [4]. In addition, hotel amenity and accommodation information provided online has been often more accurate and consistent than telephone sales due to the lack of human interaction, and online information could be updated faster than training employees in policies and procedures [4].

Online booking services for accommodation reservation in touristic destination must be safe and secure. Client personal information about reservation and online payment transactions must be protected. This kind of information can be known only to the client, booking service provider and to the hotel or transport company. To secure communication between two sides, and which is most important credit card payment transaction, booking service must encrypt all communication.

Beside encryption, both sides must pay attention in each reservation. The goal of this paper is to look at online applications that are in use for different tourism reservations from three points. First point is application security on different levels, the second point is recorded frauds, and the third point is legal regulations that must be applied for costumer personal data protection.

Paper is organized as follows. The second section describes different electronic services that can be used in tourism. The third section describes security mechanisms behind booking applications, their advantages, disadvantages and improvements propositions. The fourth section represents recorded frauds, and fifth section represents legal regulations for costumer data protection. The sixth section presents main conclusions and ideas for future work.

II. TYPES OF ELECTRONIC APPLICATIONS IN TOURISM

Different applications for desktop computers and mobile devices are in use in tourism. Some of them are in use for marketing and tourist destination promotion, and some of them are used by clients for different kind of reservations and information gathering. According to [5], some types of applications are numbered in continuation.

- Transport planning applications. These applications allow users to track flight information in real time, helping them to share information on travel disruptions with other users and to make alternative arrangements.
- Travel planner applications. These types of applications perform the traditional function of the tour operator and allow users to have an easy to manage online itinerary. They perform management functions including flights and car hire, hotel and restaurant reservations, and meetings. Another function is synchronization between mentioned functions and users calendar on the electronic device.
- Accommodation planning applications. Through these types of applications users are able to locate hotels within their current location and compare prices, quality levels and other features, as well as book accommodation. These types of applications assist with users information search processes, enabling shorter planning times and increased flexibility and choice. These applications request the highest level of security.
- Tour guide applications. Generally consist of city guides containing recommendations for restaurants, shopping, attractions, nightlife and possibly some augmented reality services. These applications can replace paper guidebooks and add value since the information is constantly updated, often includes the reviewers of other visitors as well as sponsored information, which is easy to use and relatively cost effective.
- Attraction applications. These types of applications have often been developed to deliver an enhanced visitor experience at a particular site or attraction.
- Company specific applications. These applications allow users to view and manage their bookings and other information that the company may hold about them. Airlines can provide customers with boarding cards to their mobiles, and these applications are very useful for companies to manage their customer relationships.

Different types of applications provide different costumer services. In online markets users can often find applications which are a combination of two or more thereof tips, which are more convenient and provide more services in one place. Common to all types of applications is that need to run on different platforms. In that case application needs to be customized for different devices on which it might finally run.

III. TOURISM APPLICATIONS SECURITY

Previously mentioned types of applications can be divided in two groups based on security level that must be implemented. For some of them there is no need for implementation of complex encryption algorithms, which is the case for example with tour guide applications. Here there is no need for protection more than is provided by network security, because it does not use client's personal information. Relevance of the information that is presented to the client is much more important here. Based on this fact, from the aspect of security, we have paid special attention to second group of applications that require personal client data.

This group represents applications for accommodation, flight and transport reservation. Some of these applications do not require reservation fee payment, but some of them require payment of reservation fee or the entire amount of reservation. Common to all types of reservation applications is that they require the input of personal client data. In both cases applications must provide a higher level of protection.

The level of protection for application which, in addition to personal user information, require electronic payment or data from credit card must be the highest possible. In order to fulfill this task clients and booking services must give their contribution. Each of them is responsible for implementation of security measures on their side.

A. Security measures provided on the client side

Electronic booking services for different types of reservations require from the potential clients to create an account before any reservation. This is the step where clients must fill the form with their personal data. Some of the fields on the input form are mandatory, while there are optional fields also. The clients should take care of information which they provide about themselves. For example their confidential information may be personal ID, Social Security Numbers, Credit Card Numbers, CVV Numbers, and information such as birthdates and mothers' maiden names etc.

Another important step provided by users is password creation. Passwords are the first line of defense against cyber criminals. To create strong passwords users need to use a unique password for each of theirs important accounts like email, online booking and online banking, and it is good practice to update passwords regularly. Password could be long and made up of numbers, letters and symbols [6]. The best practice is to create password made up of phrases that clients only know, and make it be related to a particular website. For example for accommodation booking service client could start with “My hotel for perfect vacation twice a year all over the world” and then use numbers and letters to recreate it. “Mhfppv2ayaotw” is one of the possible password combinations. In this way created passwords are unique and users can easily remember different passwords for different websites.

When the account is created and client starts using booking service, with each reservation he/she must pay attention to many facts. One of the first facts is the network connection security. For example the service provider of some free Wi-Fi can monitor all traffic on their network, which could include client personal information. If the client uses a service that encrypts connection to the web service, it can make it much more difficult for someone to snoop on his activity. When the connection is started, the good practice for the client is to look at the address bar in web browser to see if the URL looks real. Client should also check to see if the web address begins with https:// – which signals that connection to the website is encrypted and more resistant to snooping or tampering. Some browsers also include a padlock icon in the address bar beside https:// to indicate more clearly that connection is encrypted and clients are more securely connected.

Beside strong passwords and secure network connections booking service clients like all other internet users are potential victims of the hackers. Two most popular ways within which hackers attempt to manipulate users via the Internet are phishing and pharming [7]. Phishing involves getting a user to enter personal information via a fake website. They send out e-mails that appear to come from legitimate websites or other banking institutions and booking services. The e-mails state that client information needs to be updated or validated and ask that client enter his/her username and password, after clicking a link included in the e-mail. Some e-mails will ask from client enter even more information, such as full name, address, phone number, social security number, and credit card number. In this way phisher may be able to gain access to more information by just logging in to client account. While phishing attempts to capture personal information by getting users to visit a fake website, pharming redirects client’s to false websites without them even knowing it [8]. One way that pharming takes place is via an e-mail virus that poisons a client's local DNS cache. It does this by modifying the DNS entries, or host files.

Clients can apply some of the basic methods to protect them from phishing and pharming attacks. They should avoid opening links that arrive by email, and that direct them to their booking website. If client wants to visit the site to see if there is a need to confirm, update or verify their account, they should open up a browser and type the link or retrieve it from their favorites. If the client suspects that an e-mail is part of a phishing scheme he should report it. One more measure for protection is browser, antivirus software, and any other security software updating. The latest versions of such software have phishing filters that detect attempts and warn client if it suspects that client have surfed to a site that isn't legitimate. Perhaps the most important and easiest method for application is that clients should not use public computers to access private information.

B. Security measures provided between client and service

Network communication between client and booking service is the same like any other communication with online services. OSI (Open Systems Interconnection model) is responsible for communication between clients and online based booking services. The OSI model is a conceptual model that characterizes and standardizes the communication functions of a telecommunication or computing system without regard to their underlying internal structure and technology [9]. Its goal is the interoperability of diverse communication systems with standard protocols.

Transport layer contains group of protocols named TCP/IP protocol. TCP/IP (Transmission Control Protocol/Internet Protocol) is responsible for communication between clients and online based booking services. TCP/IP uses the client/server model of communication in which a computer client requests and is provided a service by another computer in the network. One of the protocols from the TCP/IP protocol stack group which is responsible for security is SSL protocol. SSL is a protocol that provides privacy and integrity between two communicating applications using TCP/IP. SSL is the secure communication protocol of choice for a large part of the Internet community. There are many applications of SSL in existence, since it is capable of securing any transmission over TCP. Secure HTTP, or HTTPS, is a familiar application of SSL in e-commerce or password transactions.

An SSL connection is always initiated by the client. At the beginning of an SSL session, an SSL handshake is performed. This handshake produces the cryptographic parameters of the session. This part of the SSL protocol provides necessary encryption through MAC (Message Authentication Code) algorithm. Besides that handshake provides cryptographic keys that are needed to protect data that is sent via SSL records. For this job HMAC (Keyed-Hash Message Authentication Code) can be used. HMAC can be used in combination with any iterated cryptographic hash function. MD5, RC4 and SHA-1 are examples of such hash functions. An iterative hash function breaks up a message into blocks of a fixed size and iterates over them with a compression function. For example, MD5 and SHA-1 operate on 512-bit blocks on the input. On the other side the size of the output of HMAC is the same as that of the underlying hash function, 128 or 160 bits in the case of MD5 or SHA-1, respectively. HMAC also uses a secret key for calculation and verification of the message authentication values. The cryptographic strength of the HMAC depends upon the size of the secret key that is used. HMACs are substantially less affected by collisions than their underlying hashing algorithms alone. Therefore, HMAC-MD5 does not suffer from the same weaknesses that have been found in MD5.

The current SSL version 3.0 encryption uses either the RC4 stream cipher or a block cipher in CBC mode. The most severe problem of CBC encryption in SSL 3.0 is that its block cipher padding is not deterministic, and not covered by the MAC, thus, the integrity of padding cannot be fully verified when decrypting. The SSL 3.0 vulnerability stems from the way blocks of data are encrypted under a specific type of encryption algorithm within the SSL protocol. One of the last attacks named the POODLE (Padding Oracle On Downgraded Legacy Encryption) takes advantage of the protocol version negotiation feature built into SSL/TLS to force the use of SSL 3.0 and then leverages this new vulnerability to decrypt select content within the SSL session [10]. The decryption is done byte by byte and will generate a large number of connections between the client and server. Browsers and websites need to turn off SSLv3 and use more modern security protocols as soon as possible, in order to avoid compromising user's private information. One of the recommendations to avoid attack is the SSL 3.0 protocol disabling in the client or in the server (or both). Disabling SSL 3.0 entirely right away may not be practical if it is needed occasionally to work with legacy systems.

IV. PROTECTION OF PERSONAL DATA

Client data collected through the any kind of electronic and other services must be protected. Protection is regulated by the law of personal data protection. This law declares that every natural person shall be entitled to personal data protection regardless of their nationality and residence, race, age, gender, language, religion, political and other affiliations, ethnicity, social background and status, wealth, birth, education, social position or any other personal characteristic [11]. The legal acts defines how to protect the rights and freedoms of persons with respect to the processing of personal data by laying down the key criteria for making processing lawful and the principles of data quality.

Different booking travel online services create their own legal notes based on rights and obligations which are defined by appropriate law. For the purpose of this paper authors compared data protection legal notes from the three booking accommodation services. First one is online booking service which is an intermediary between the clients and the hotels [12], second is online booking accommodation through the hotel website form [13], and the third is service for mobile devices [14]. All these services define what kinds of personal client information are used, and why they collect and share personal data. Data that they collect are similar (names, e-mail addresses, credit card numbers, etc.). List of third parties that can get personal client data vary between services. Observed intermediary service declares that they share personal data with hotels for which client make a reservation, with local booking office for technical support, with competent authorities (law enforcement and other governmental authorities), and with business partners. In the case of the website reservation personal hotel does not share personal information with anyone, except with law enforcement. When a booking is made through the application for mobile device [14], to the chosen hotel service sent client contact details, booking information and, if appropriate, client credit card details (only for bookings made using a credit card), as well as any additional information for the hotel that client entered. Apart from the relevant hotel, no other third party receives any data, except in the event of a specific legal obligation. In the event of a criminal investigation, such as if it is suspected that a crime has been committed, all necessary data will be passed on to the authorities.

In accordance with European data protection laws, all services observe reasonable procedures to prevent unauthorized access and the misuse of personal client data. First observed service declares that they use appropriate business systems and procedures to protect and safeguard the personal data which clients give to them. They also use security procedures and technical and physical restrictions for accessing and using the personal data on their servers. Only authorized personnel are permitted to access personal data in the course of their work. Client credit card details are stored on the system for a maximum of ten days. After that, credit card data will be either permanently deleted from the systems or will remain hashed in the system for fraud detection purposes. However, if client stores his credit card details in his account, credit card details will be stored in hashed form, but without the last four digits of credit card number.

The second observed service do not define how safe data protection is, and which techniques they use for client personal data protection on their servers and networks. The third service define that their servers and networks are protected from outside access by the latest IT security components. These regulations specify legal requirements for the protection of personal data. From a client requires to keep his personal log in details confidential and not to make these details available to unauthorized third parties. The provider accepts no liability for misused passwords unless the provider is responsible for this misuse. All three services retain the right to use cookies. The first service defines fourth types of cookies: technical, functional, analytics and commercial cookies. Each type provides specific information, and each cookie can be used in different situations. The second service does not define which type of cookies they use. Third service uses the similar types of cookies like first one. All services do not obligate client to accept the cookies. Quite to the contrary, client can configure web navigator either to accept or reject the cookies that he receive or to advise him when the web server wishes to store any in his computer. That is just one more technique for faster client identification.

V. FRAUDS BEHIND BOOKING TRAVEL ONLINE SERVICES

Booking travel online offers the ability for the clients to compare prices and scour online reviews among them, but it also comes with some risks. Recently, certain frauds that target consumers booking travel online have been popping up more and more. Fraud relating to holiday accommodation is among the most common. Fraudsters are making hundreds of thousands of euros each year through fake websites, false advertising, bogus phone calls and email scams, often leaving their victims without a flight or holiday, or even stranded in another country with nowhere to stay. Most scams occur on sites where owners advertise their accommodation directly, but not uncommon and fraud through official services.

The most common fraud is false reservation and payment. This happens when a third-party site claims to have booked travel and takes a client's money in payment for that, but the hotel or airline has no record of them having done this. Another problem is inadequate accommodation. This happens when users get the accommodation that have not booked, or when furniture and rooms are not the same as on the booking site.

From this point another problem appears. This fraud is named a bait-and-switch, and happens when a consumer believes that the online travel booking site has a certain refund or return policy, when in fact it has no returns money. In the cases of travel cancelation or modification booking service requires an exorbitant fee. For example if a consumer decides to change or cancel the trip, they will lose their money entirely or be charged an exorbitant fee. Unfortunately, avoiding this one often comes down to reading the much-dreaded fine print, which many consumers don't do. Even if the site says something like satisfaction guarantee or refunds available clients still need to read the fine print before booking to fully understand the refund policy.

One more fraud or "technical problem" is multiplication of same reservation. This kind of problem appears when client places an order, but did not get confirmation email for that order. After the consultation with booking technical support employee, the client places a new order for the very same travel. Based on credit card details, travel agency charges double amount once for each reservation. In such cases booking services remove all responsibility from them, and does not refund money. Some online travel booking sites are changing travel dates on clients and not telling them beforehand. So, for example, a consumer would book a travel package with the company with a flight on a Monday; the flight would change times or dates and the company would neglect to tell the consumer. This can create a snowball effect where other parts of the trip get messed up too.

One common and in the same time illegal practice in the world of electronic booking systems are private individuals who offer accommodation. Online booking services that work like provides between travelers and people who offer accommodation does not have possibility to check all their clients on both sides. For registration on some booking service private individual who wants to rent a room, house or villa must input certain information. The most sensitive information is bank account information. All other are contact information and information about accommodation description. In this way anyone who opens an account can offer accommodation via these services.

Booking services does not have a mechanism to check the accuracy of information related to the user and information about conditions in the offered accommodation. Authenticity of all pictures, videos other forms of advertising that represent accommodation description booking service can't check. The mechanism of accommodation assessment comes down to users evaluation and users comments after accommodation use. Because of that travelers are not secured, and sometimes accommodation pictures are from the period when villa or hotel was new, but in the time when traveler come furniture is old and ruined.

One more type of a fraud associated with personal individuals is related with taxes payment. Private individuals set bank accounts in the bank whose locations are in another country or they use electronic bank or electronic wallet services for booking accounts creation. In that way they don't register their accommodation services in any touristic organization or in the government agency for business registers, and as they are not registered anywhere they do not pay taxes. If they have some villa or apartments in frequent touristic destinations they can earn large sum of money on the basis of unpaid taxes. In that case, their guests are not insured. In larger number of cases guests do not have that information and they pay amount for insurance on hand to the hoteliers. Electronic payment methods, especially payment in advance for such accommodations provide more space for frauds with taxes and insurance. Electronic money goes from one account to another and in most cases ends in banks located in countries that do not charge tax.

Online booking of airline tickets or accommodation is essentially online shopping. Internet security experts strongly recommend the adherence to the same measures to protect consumers from becoming victims of credit fraud. The rule of thumb is to trust only reputable service providers and to skip over too-attractive travel promo deals. The best way is to skip all online payments and credit card details sharing, but what if client must purchase plane tickets or accommodation online. Experts agree that credit cards offer more security than debit cards. Note that the latter is directly connected to a consumer's bank account, which means any transaction automatically deducts an amount from the person's bank account. Credit cards can also cushion the impact of a potential fraud. A required clearing-time of the previously transacted credits acts as a buffer for later disputes [15].

One more real example about hotel website booking vulnerability is posted online about a year ago. British security researcher finds an array of security issues using Hotel Hippo website. This service emailed to clients a link to their booking confirmation. It includes lots of personal information, and dates and details of where client will be staying. Unfortunately, what the page doesn't do is authenticate that person is authorized to access the information. Indeed, this part of the HotelHippo.com website is guilty of one of the easiest to exploit and most prevalent vulnerabilities found in website designs: insecure direct object references. The mentioned link contains account number based on which client's account page opens. With a little alteration of the number, attacker can start walking through the booking information of other customers too [17]. At this point, an attacker has everything they could possibly need to launch a highly effective phishing attack against a user. From the aspect of connection security another problem appears. The server only supports SSLv2, SSLv3, and TLSv1.0. There is no support for newer protocols like TLSv1.1 or TLSv1.2 and also no support for Perfect Forward Secrecy. They have ECDHE cipher suites available on the server, but they're just buried below other, less secure, cipher suites. Vulnerability like this could have left thousands of other customers, dangerously exposed. The huger problem is that booking service does not response about this disadvantage, and does not solve the problem.

Another, recent example of misuse of data from credit cards used for payment and reservation is detected in hotels which belong to “Hayat Group” corporation. The hotel corporation "Hayat" announced in late December that the computer systems for payments processing in hotels operating under this name had revealed PoS (Point-of-Sale) malware. ”Hayat" published a list of locations where the virus is found, the malware, revealing that 250 of 627 objects who had been operating under this name worldwide were affected by this attack. 99 of affected hotels were in USA, 22 in China and 20 in India. According to foreign media, the presence of the virus was discovered in late July, but these buildings were the first whose systems were infected with malware. In most cases, malware was present in the hotel's system in the period between 13 August and 8 December last year. The malware collected data for credit cards - the owner's name, card number, expiration date, and internal verification code. However, it seems as if the other user information are not stolen.

It’s important for all clients to report a fraud so that the criminals can be stopped and that others don’t fall victim to the same scam. In many countries there are special organizations that deal with these types of frauds. For example police of UK advise that clients could report fraud to Action Fraud center, or they can also use the online tool if they suspect that they have been targeted [16]. For the credit card payment frauds client need to report the fraud to card issuer.

VI. Conclusion

Tourists and travelers all around the world look for various types of accommodation and transportation to their touristic destination. Electronic booking services and mobile devices in last decade have upgraded travel and accommodation search and reservation. One online booking service gathers thousands of hotels, apartments and villas for tourist accommodation. On the same way, booking services for airlines companies gather different companies and provide the best prices and quality of service. The most important in all travel bookings is client security and quality of provided service. To secure client personal data and to reduce frauds and problems, users and booking provider must work together. They must pay attention, each on his side of application. Users need to report recorded frauds to the authorized institutions, in the purpose of prevention, and the booking providers need to secure clients personal data as much as possible. Tourist could provide useful information about some accommodation to the booking service and to other future tourists through the appropriate online evaluation of used accommodation. If we summarize all advantages and disadvantages, we can conclude that this kind of services has many benefits, makes everyday life easier and saves time and money. On the other hand, all participants have to pay attention to ensure mutual satisfaction.

Acknowledgment

This work has been supported by the Ministry of Education, Science and Technological Development of Republic of Serbia within the projects TR 32023 and TR 35026.

References

[1] I. Miskovic, V. Holodkov, I. Radin, “Upotreba mobilnih aplikacija u promovisanju turisticke ponude zasticenih delova prirode”, Pregledni clanak, Fakultet za sport i turizam, Novi Sad, TIMS Acta 9, pp. 75-86, 2015. DOI: 10.5937/timsact9-7219.

[2] W. Lawrence, S. Sankaranarayanan, “Application of biometric security in agent based hotel booking system – Android environment” International Journal - Information Engineering and Electronic Business, vol. 3, pp. 64-75, July 2012. DOI: 10.5815/ijieeb.2012.03.08.

[3] Computer reservations system, Retrieved from: https://en.wikipedia.org/wiki/Computer_reservations_system.

[4] R. Rust, P. Kannan, “The era of e-service,” in P. K. Kannan ed., e-Service, New Directions in Theory and Practice, M. E. Sharpe, New York, NY, 2002.

[5] G. Bendon, S. Hundson, Our mobile future: how smartphones will transform visiting experiences. London: Horizon Digital Economy Research, 2010.

[6] T Srivastava, “Phising and Pharming – The Evil Twins”, Sans Institute InfoSec Reading Room, pp. 1-32, 2007.

[7] Phishing and Pharming Information Site, Retrieved from: http://www.pharming-phishing.com/,2015.

[8] Pharming, PC.net, Retrieved from: http://pc.net/glossary/definition/pharming, 2015.

[9] McNub C. Network Security Assessement, O’Reilly Media, Inc., 1005 Gravenstein Highway North, Sebastopol, CA 95472, 2nd edition, pp. 102-196, 2007.

[10] B. Moller, T. Duong, K. Kotowicz, “This POODLE Bites: Exploiting The SSL 3.0 Fallback”, Google, 2014.

[11] P. Boillat, M. Kjaerum, Handbook on European data protection law, Publications Office of the European Union, Belgium, 2014.

[12] Privacy and Cookies, Booking.com, Retrieved from: http://www.booking.com/content/privacy.en-gb.html.

[13] Data Protection Legal Note, The Queen’s Gate Hotel London, Retrieved from: http://www.thequeensgatehotel.com/en/protection-legal-note.html.

[14] Data protection, Hotel info, Retrieved from: http://www.hotel.info/About/DataProtection?lng=EN.

[15] T. Mohn, “How to avoid ATM and Credit Card scams when traveling”, Retrievad from: http://www.forbes.com/sites/tanyamohn/2011/11/16/how-to-avoid-atm-and-credit-card-scams-when-traveling/4/

[16] A guide to holiday booking fraud, Everyting you need to know, Retrieved from: http://www.actionfraud.police.uk/sites/default/files/3395%20Holiday%20Fraud_v4.pdf.

[17] S. Helme, “HotelHipo Insecure, so I’ve herd”, Retrievad from: https://scotthelme.co.uk/hotel-hippo-insecure/