Security overview for m-payed virtual ticketing

Gianluigi Me
Dipartimento di Informatica Sistemi e Produzione
Università di Roma "Tor Vergata"
Roma, Italy
me@disp.uniroma2.it

Abstract— **The use of wireless and mobile devices is expanding worldwide; with a growing eagerness to find new and useful ways to apply mobile technologies. New applications, as mobile ticketing, can benefit of mobile-payment facility. This paper aims to provide a mobile ticketing system design for PDA, scalable to other mobile devices, presenting a wireless weaknesses overview and security building blocks for mobile ticket and mobile payment relying on**

Keywords: m-payments; PDA; encryption; wireless security

I. INTRODUCTION

The explosion of Internet-based information has made consumers much more familiar with nontraditional ways to shop for goods and services, (e.g. Amazon.com, eBay and Expedia.com) attesting that consumers are very much interested in shopping and transacting via electronic media.

The progression of these two phenomena has very naturally led to a converged idea: the desire to initiate and complete transactions via a mobile device. The concept is a very easy one for many mobile users to accept; there is almost a knee-jerk response that such a portable means of shopping and payment would be much more convenient than traditional cash-based or card -based methods.

Based on these parameters, it is expected that the transaction value of m-payments performed follows Figure 1.

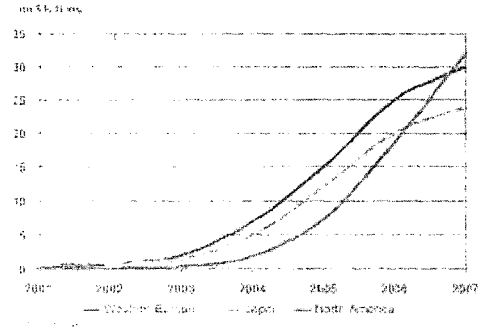

Figure 1. Projected M-Payments Geographic Market Size by Transaction Value (Gartner Research)

One of new mobile applications, possibly relying on mobile payment, is represented by mobile ticketing. Following the definition in [1], a ticket is a proof of access/usage rights to a particular service and mobile ticketing is its electronic realization with the help of mobile device. Potential applications of this service include transportation (flights, trains, boats, ferries, buses, trams), events (Concerts, theatres, fairs, museums, sports events), facilities (Gyms, solariums)

Mobile ticketing is mainly composed of 2 building blocks: mobile ticket provider application and payment system facility relying on. The payment choice mainly depends on payment size and expected target client mobile equipment.

One of the most important issues is related to the security mechanism underlying the enabling technologies for mobile application underlying financial transaction, actually big concern for e-commerce consumers, merchant and issuers [2]. Security, with ease of use, costs and universally availability, is absolutely critical to the success of any mobile ebusiness. A number of technologies and solutions already exist that can form the basis of a wireless security architecture: on these, new threats and risks of mobile e-business are pending.

Even if payment aspect of ticketing has to be considered independent by the ticketing aspect, this paper focuses on security layer viable for both application building blocks.

II. CONTRIBUTION OF THIS WORK AND ROADMAP

The contributions of this paper are the following: (1) present a mobile ticketing application system design, based on cellular network and Bluetooth, with regard to payment system (2) identify the vulnerabilities of such an architecture, (3) address the security issues that arise with regard to the payment system, showing different possible solution viable for actual mobile systems focusing on the GSM/GPRS link, based on state of the art mobile payment standards (e.g. VISA 3D, MeT, Radicchio); Finally, I will draw conclusions.

III. WIRELESS SECURITY THREATS

Mitigating design flaws in a security architecture is hard work. While mitigating implementation flaws, such as buffer overflows, usually involves only few lines of code, mitigating design flaws often involves redesign of the system architecture.

For this reason it's important to address security issues with a detailed analysis of vulnerabilities of the architecture chosen in system design phase. As noted in [3] adding security or fixing poorly design security in wireless networks after the fact is often impossible.

0-7803-7822-9/03/$17.00 ©2003 IEEE.

The range and nature of the threats will vary hugely depending on each application and the environment in which it operates. As rule of thumb, it is difficult to assure the confidentiality and integrity of data as it is exchanged over wireless data networks involving many different third parties. At the moment, mobile devices security capabilities, as new interfaces to e-business applications, are severely restricted. Furthermore the rapid development of new mobile technology means that it is not always mature or suitably verified for security. There is also a lack of standards for user and device authentication, as detailed further, executable content security and stored data security.

However, the Figure 2. illustrates some of the typical threats and challenges that mobile e-business presents:

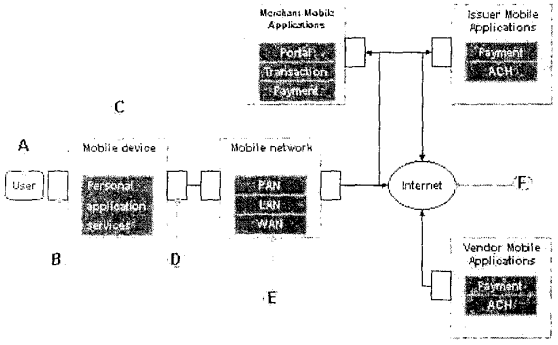

Figure 2. Wireless vulnerabilities

Malicious or careless behaviors pose first vulnerability on A-point. Lesson learnt from military security experience teaches that even the highest quality locks offer virtually no protection against the hands of a legitimate user. For this reason and for Personal Digital Assistant (PDA) individual use these concerns are likely the most difficult to solve, as confirmed by Gartner research, saying that, through 2005, 85 percent of wireless security incidents will be device-related rather than over-the-air related.

Than, on B point, weak user authentication controls, as password, can be a threat. In fact, initial access code or password on wireless devices can often be deactivated by the user and allow unauthorized access to applications and data. Furthermore, password authentication has at least 10 vulnerabilities (Dictionary Attack, Van Eck phreaking, Social engineering etc). The C point denotes that the ,devices is insecure, because of many weaknesses as

- Over The Air (OTA) remote configuration facilities, undocumented APIs or software bugs that could be exploited and abused.
- Virus risks due to variety and immaturity of wireless devices, operating systems, applications and network technologies as well as the size of the user base increases the threat of virus and malicious code attacks;
- SIM card duplication risk. If application security is based on user authentication to the device (from the SIM) then it will also be possible to masquerade as a genuine user;
- Device or theft or loss risk, since mobile devices generally have very limited security features built in, losing them also means that sensitive corporate or personal data may be disclosed;
- Loss of data risk, if a device malfunctions, is lost, or if its data is accidentally deleted and there is no recent data backup combined with restore capability, the data will be lost forever.
- Always on risk, because mobile devices can be accessed even when they are not actively in use, users are less likely to know if they have been a victim of an attack

On D point focus wireless link threats. In fact, as in E, radio frequency signal jamming in the proximity of the device or a base station can lead to disruption and non-availability of wireless devices and networks. Furthermore, the combination of data being transmitted over public radio frequencies and the weaknesses in the cryptographic algorithms (e.g. GEA, A3, A5, A8) pointed in [4] gives rise to digital RF scanning equipment capturing and decrypting data, leading to loss of confidentiality and information disclosure. Denial of Service Attacks are also possible, as in F, by continuously transmitting large amounts of data to the attack point, network bandwidth may be saturated and, in the case of D point, the battery on the device drained leading to performance degradation or non-availability. These threats are to be considered over the usual threats for fixed networks.

Moreover, for the sake of completeness, further vulnerabilities have to be considered in the overall mobile ticket application, regarding Bluetooth security, as PIN Attack, Location Attack, Limited Authorization Levels, Random Topology, as noted in [5].

IV. MOBILE TICKETING APPLICATION

As rule of thumb, mobile ticketing support two distinct application architectures:

1. the proof may reside in a ticket issuer's server, in which case the redemption of the ticket consists of user authentication to the server. This requires an online connection to the ticket issuer's server at the usage point (according to MeT, defined as virtual tickets).
2. the proof may reside in a personal device, as in the case of the presented project, in which case the redemption of the ticket consists of user authentication to the server and ticket download. Afterward, an appliance on access gate to the service (i.e. theatre) checks ticket stored in Personal Trust Device (PTD). According to MeT, this second architecture is referred as PTD tickets.

As shown in 0a PDA connects via GSM/GPRS/UMTS (label 1) cellular network infrastructure to a Ticket Store Web

site (label 2) with Pocket Explorer. As rule of thumb, it's possible to consider this server valid for every kind of mobile device connecting to, meaning that it's capable to offer, via a transcoding service, content with appropriate text/graphics format, as presented in [6].

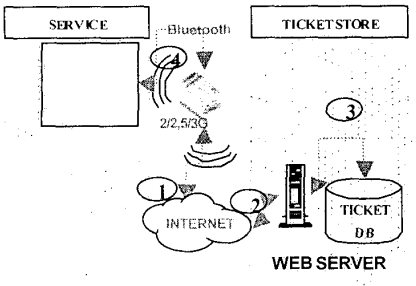

Figure 3. Mobile ticketing (PTD) architecture of project

After ticket selection phase, whose commit is due to its availability, m-payment starts. For the sake of simplicity and without lack of generality (any third m-payment third party can be enclosed) on Figure 3 Web server and payment server coincide, even if the two services have different perimetral security requirements (out of the scope of this paper). On payment commit, ticket can be released to PDA (label 3). Prior to send, ticket securization happens. This can be done in multiple ways, possibly with regard to security model adopted for m-payment, detailed in next sections. For example, possible ways include encryption (i.e.. symmetric or asymmetric keys to cipher) or Hash Message Authentication Coding (HMAC). The ticket needs to be securized for reason explained in previous section and because of lack of user authentication methods in Bluetooth 1.0. As the ticket has been sent, it resides on PDA until event occurs. This time range presents most security concerns because strictly related to user behaviour in managing PDA. Ticket sending back and cancelling facilities (e.g. due to stealing, loss) could be implemented to provide to the customer added value service not available for analogous paper tickets.

- On date event (label 4), ticket is used to access the event. A Bluetooth appliance is posed on gate, performing authentication and checking integrity and validity of ticket.

This application has been implemented using

- on mobile side, a Pocket PC Compaq iPAQ 3860, equipped with ARM SA1110, 64MB, Bluetooth and Windows CE Pocket2002,
- on appliance side, a COTS laptop equipped with Anycom Buetooth PCCard Type II emulating the appliance.

The connection between appliance and PDA has been implemented using Bluetooth virtual ports, without use of IP layering sockets (not yet implemented at time of develop).

A more detailed description of Bluetooth interaction system can be found in [7].

V. REMOTE PAYMENTS

As well as the presented application can benefit of Secure Socket Layer (SSL) as web application do, it's my intention to present secure layer viable for wide variety of mobile devices.

Remote payments can be performed with embedded SIM Toolkit application or via WAP protocol, whose secure layer is Wireless Transport Layer Security protocol. WTLS 3.0 provides transport layer security between a WAP client and the WAP gateway similar to those of the SSL protocol used on the Web. WTLS certifies that the data sent has not been manipulated by a third party, it accounts for privacy, and it also guarantees that the author of a message can be identified Figure 4. . To avoid man in middle attack, a WTLS Class 3 should be used, which requires the user to be issued a client-side public/private key pair. WTLS uses RSA's RC5 or ECC to encrypt data and transport it over wireless link: the protocol works in conjunction with PKI, to secure application platforms with digital certificates, and wireless cookies, to provide session management.

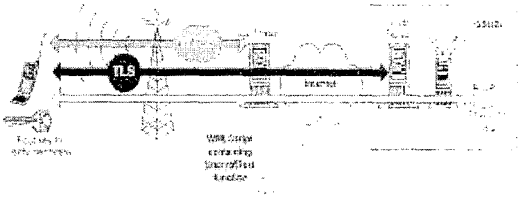

Figure 4. WAP 2.1 security

Under TLS Figure 4. , both the server and the client are authenticated using public/private keys stored on the handset, on a Subscriber Identity Module (SIM), as detailed in the next paragraph. Use of end-to-end TLS/SSL (using EncryptText() script function) complies with Internet protocol standards and ensures that the cardholder password is never in the clear at the gateway level. The Issuer therefore receives the same level of security for password authentication as is available with any TLS/SSL Internet connection [8]. Alternative approach, also with WPKI, uses so-called "roaming" or zero-client schemes where the users' private keys are stored on a secure server or the WAP gateway, and pulled into the transaction to support end-to-end encryption and digital signing. In WAP versions until the 2.0, gap between WTLS and SSL/TLS offered vulnerabilities for two attacks: 1) Man in the middle, because during the conversion there are fraction of seconds when the message is not encrypted and therefore susceptible to eavesdropping or packet sniffing, 2) Because of the gap Cardholder and Issuer cannot be guaranteed that messages are not forged by an impostor.

WAP 2.0 resolved the WAP gap issue by defining a secure tunnel through the WAP gateway, which now acts as a "proxy" server, to maintain a TLS/SSL session all the way from the phone to the server. In conclusion there is a lack of reliability

due to power consumption, with actual batteries, during encryption phase.

VI. SECURITY BUILDING BLOCKS

Macropayment schemes are modeled on real world payment instruments. Each of macropayment systems based on credit cards, cheques and cash instruments have a minimum transaction overhead, usually imposed by the issuing bank, which prevents them being used for micro payments. A second heavy-use inhibitor factor is their heavy use of computationally expensive cryptographic operations, such as public key cryptography. Computational overhead makes macropayments too inefficient for repeated frequent transactions such as making a payment per second for a telephone call.

In contrast, micropayment solutions are designed to allow the efficient frequent transfer of very small amounts, in a single transaction. The increased efficiency is obtained by slightly relaxing the security, which is acceptable due to the small amounts involved [9].

A. Wireless Public Key Infrastructure (WPKI)

In order to fulfill its purpose, a WPKI must be able to ensure the following services:1) Authentication: communicating parties must be able to confirm the identity of the other party; 2) Confidentiality: communication between two parties must remain private; 3) Integrity: the information that is transferred between the parties must remain correct and unaltered; 4) Non-repudiation: the merchant needs to be sure that sometime in the future the payer cannot deny having purchased that ticket and demand a refund.

A PKI is considered wireless when at least the front-end devices that are employed by end-users to communicate with other parties (such as service providers and trusted third parties) are wireless. Mobile payments WPKI, at state of the art, can rely on two different algorithms of asymmetric cryptography: RSA and Elliptic Curve Cryptography (ECC), whose detail can be referred to [10]. While RSA represents a reliable industry standard, included by most manufacturers, an extremely valid alternative for this scheme is ECC with advantages as improved performance [11], smaller memory and processing requirements, and generally lower cost of implementation.

End users benefit from longer battery lifetimes on mobile devices and lower messaging costs for wireless communications. ECC brings similar benefit to smart cards, such as strong security, increased speed, lower costs and high performance. This strength and performance is delivered without requiring a cryptographic co-processor as used in RSA. The small size of ECC key pairs, certificates, and implementation efficiency enables the use of inexpensive smart cards with low memory requirements.

1) Smart cards

M-payment smart cards, following the standard specification ISO 7816-X and ISO/IEC 14443-1, should provide 1) Tamper-resistant storage for protecting private keys and other forms of personal information (even if vulnerable to optical probing attack [12]), 2) Isolate security-critical computations involving authentication, digital signatures, and key exchange from other parts of the system that do not have a "need to know", 3) Enable portability of credentials and other private information between computers at work, home, or on the road. As rule of thumb, Figure 5. shows various strategies to store cryptographic keys needed for strong authentication.

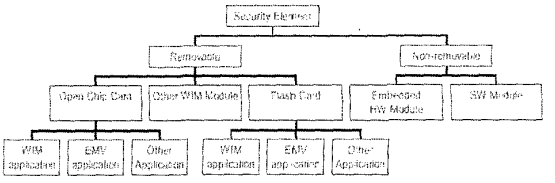

Figure 5. Preferred Payment Architecture strategies

For example, the keys can be stored in mobile device HW module as well as in a WAP Identity Module (WIM) resident in the SIM (SWIM) or in a removable smart card that can be inserted in a dual slot phone.

A typical smart card chip for mobile payments includes a microprocessor able to provide sym/asym encryption, ROM (operating instructions storage), RAM (data during processing storage), and EPROM or EEPROM memory for non-volatile storage of information. Asymmetric encryption, and therefore smart card equipped with embedded crypto processor, is the only provider of nonrepudiation service, needed for macropayments and remote transactions. Tradeoffs between symmetric and asymmetric cryptography choice, with requirements achievable by both, resides on scalability of architecture and cost of computation speed (e.g., RSA needs a coprocessor, raising the cost of the card).

B. Authentication

Authentication, information used to verify an identity claimed, is generally the second step of a two-step process: 1) Identification-The user claims an identity, usually by supplying a user ID to the security system, 2) Authentication- The user supplies or generates authentication information that corroborates the binding between the person and the identifier.

An authentication service using only one authentication factor [13] may be vulnerable: combining two or more factors provides greater security (strong authentication). Even if mobile device has to be considered a PTD, mobile payments requirements cannot afford to these mechanisms. For this reason different user authentication mechanisms are implemented, so the Issuers can choose preferred authentication method, mostly related, at the moment, to the too vulnerable password mechanism. These are valid until access to mobile phone will be driven by biometrics trait (e.g. voice, thumbprints).

1) Asymmetric Authentication

Using asymmetric cryptography will enable the exchange of authenticated messages and secret data without exchanging the secrets needed for performing authentication. Typically, as for WTLS, TLS, SSL, a public-key authentication mechanism follows a challenge-response mode. The user, or rather software on the computer, can use the user's private key to digitally sign a challenge from the authentication server to generate the

response. The user sends this back to the server together with the PKC. The authentication server validates the PKC and, if this is successful, verifies the digital signature using the user's public key from the PKC, so authenticating the user. This handshake can be performed on different channels, as shown in Figure 6. .

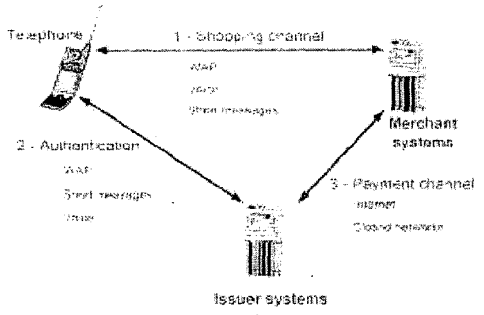

Figure 6. Shopping and authentication channel in VISA 3D Secure™

As rule of thumb, to authenticate cardholders using asymmetric signature, the Issuer needs to consider the following: 1) Key storage: generation, storage, and PIN access to the private key in the cardholder's system (SWIM, WIM in dual slot etc.), 2) Certificate issuance: the type of certificate employed, 3) Device/subscriber certificate: the certificate contains information related to the phone hardware such as SIM ID, and possibly subscription information, 4) Cardholder certificate: the certificate contains information about the cardholder, such as the name, 5) Authentication channels: the channel (e.g. WAP) selected to exchange challenge and signature. These elements can be combined in different ways to form full authentication solutions.

2) Symmetric key authentication

Symmetric key cryptography is used for on-line transactions and to protect the authenticity and integrity of data by generating message authentication codes (MAC). Most vendors use a standard authentication protocol using cryptographic hash functions based on the ANSI X9.9 standard for Macs (e.g. SHA-1, MD5); others use a proprietary protocol. Authentication Modes with MAC can be Asynchronous (Challenge Response) or Synchronous (Response only, Time/Event synchronous): in some implementations, the token and authentication server recalculate the user's shared secret after each authentication event. In these cases the central authority, or issuer, generates a key or key pair that is placed on the card during personalization. The card generates the MAC by performing the specified algorithm over a defined set of data that is known as the "challenge". This challenge is defined for the application to be unique for each transaction. The MAC (and any necessary transaction data) is then delivered to the issuer, which must verify the MAC. The issuer determines the correct key based on the card account number, then validates the received MAC by generating a MAC using the same data and algorithm. If the received and generated MACs match, then the issuer can be certain that the data was not altered and was provided by the card's application. Issuer can adopt a synchronous authentication mode based on authentication tokens (of any kind), something that only the user possesses, rather than something that only a user knows. All OTP-generating tokens use symmetric cryptography: each user's token has a unique, personal, shared secret key that is used to encrypt some data (depending on the mode) to generate the OTP. This secret key is shared with the authentication server, allowing the server to duplicate the encryption process and generate the OTP that it expects from the user: a match authenticates the user.

VII. CONCLUSION

Mobile ticketing and mpayments, due to diffusion of PDA and mobile phones, can represent a spread-use application in the mobile world. This paper aimed to provide a general overview of mobile ticketing security, based on open standard models, focusing on security weaknesses and holes present in literature, relating to choice rationales regarding to security levels and adaptability to actual limited mobile device computational resources. Security design has to be linked to client equipment, payment size and possibly to related m-payment issuer and provider: it's possible to adopt countermeasures so the big concerns can focus on PTD owner behavior and transaction actors perimetral security. In the future, biometric trait, on mobile device, can solve most concerns related to user behavior.

ACKNOWLEDGMENT

I gratefully acknowledge the support provided by Dr. I. Santodonato.

REFERENCES

[1] MeT, MeT White Paper on Mobile Ticketing (MeT-WPMobTick-v1_0-20030122), www.mobiletransaction.org, 22-01-2003

[2] C.S.I., "Cyber crime bleeds U S. corporations, survey shows; financial losses from attacks climb for third year in a row", http://www.gocsi.com/press/20020407.html

[3] N. Petroni Jr, W.A. Aurbaugh, "The dangers of Mitigating Security Design Flaws",IEEE Security & Privacy,Jan-Feb 2003, Vol.1, n.1 pp. 28-36

[4] R. Di Pietro, G. Me, "Military Secure Communications Over Public Cellular Network Infrastructure", Proceedings of the IEEE/AFCEA Milcom 2002

[5] R. K. Nichols, P. C. Lekkas," Wireless Security: Model, Threats and Solutions", McGraw-Hill TELECOM, 2001, pp. 402-415.

[6] B.N. Schilit, J.Trevor, D.M. Hilbert, Tzu Khiau Koh, "Web interaction using very small Internet devices",IEEE Computer,Oct 2002, Vol.35, n.10 pp. 37-45

[7] G. Me, "A secure mobile local payment application framework", 2003 Int'l Conf. on Security and Management (SAM'03)

[8] 3-D Secure ™Mobile Authentication Scenarios, VISA International ,http://international.visa.com/fb/paytech/secure/main.jsp

[9] Michael Peirce, "Multi-Party Electronic Payments for Mobile Communications", http://citeseer.nj.nec.com/peirce00multiparty.html

[10] B. Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", 2nd Edition, Wiley, 1995

[11] Certicom, Remarks on the security of the elliptic curve cryptosystem, www.certicom.com, 2000

[12] S. Skorobogatov, R. Anderson, "Optical Fault Induction Attacks", www.cl.cam.ac.uk/users/rja14/faultpap3.pdf.

[13] NCSC-TG-017 "A Guide to Understanding Identification and Authentication in Trusted Systems", U.S. National Computer Security Center