Electronic Payment and Online Gaming

Gerald Draxler, Johannes Sametinger, Andreas Wiesauer

Johannes Kepler University Linz, A-4040 Linz, Austria
draxler@incert.at, johannes.sametinger@jku.at, andreas.wiesauer@jku.at

Abstract. We will evaluate electronic payment (ePayment) systems by employing a use-value analysis. The key success factors of ePayment systems are security and flexibility. Not surprisingly, it turns out, that there is neither a "best" nor a "most secure" ePayment system. The adequacy of these systems depends on the application context. A use-value analysis is an appropriate and easy to use evaluation method, because it allows the consideration of different application perspectives. In fact, many ePayment systems are available today, but there are still contexts that require a tailored solution. Online gaming will be given as an example. For this purpose, we will introduce *BetMPay*, an ePayment system that offers a high level of anonymity, payment guarantee for providers, as well as consumer protection. This system also suffers from drawbacks in comparison to other existing system. This again will be outlined by a use-value analysis.

1 Introduction

Today, transactions on goods, e.g., books or electronic devices are increasingly carried out over the Internet. Customers and merchants regularly face the problem of handling payments. Various payment systems are available that rely on different paradigms, e.g., credit cards, debit notes or payment via cell phones. Online store operators often have difficulties in selecting the appropriate systems for their needs. Criteria include usability, user acceptance or common usage in existing web shops. Many electronic payment systems are available and their use is constantly rising. But there are scenarios, where special requirements exist that are not sufficiently fulfilled by available systems. For example, online gaming clients often prefer to indulge their passion anonymously.

In this paper we present an overview on different electronic payment systems and evaluate their benefits from various perspectives. Additionally, we present a solution that had been implemented with the focus at customer anonymity. This system had been developed in the context of online betting applications and additionally aims at providing effective cost control for customers as well as paying guarantees.

In Section 2 we shortly introduce online gaming. Section 3 describes aspects of electronic payment and introduces a selection of ePayment systems. In Section 4 we focus on requirements that are important for any electronic payment system. We also depict criteria that can be used for evaluation. Section 5 provides an evaluation of ePayment systems by employing a use-value analysis. In Section 6 we introduce an ePayment system that is focused on customer anonymity, and we also compare it to the other systems. Related work follows in Section 7, and a conclusion is given in Section 8.

2 Online Gaming

In this context, "gaming" means the playing of games for something of material value like money. Games focus on an event with an uncertain outcome and the intent of winning additional material value [17]. The outcome of the game is typically evident within a short period of time, e.g., the final score of sports events. Online games are played for electronic money and require electronic payment systems.

An example provider of online gaming is *bwin* who is offering up to 30,000 bets daily with betting action in more than 90 sports [www.bwin.com]. Bwin offers a wide range of payment methods, including credit cards and online banking deposits. Reliable transfer of money is crucial. Above all, gaming providers need to be sure that money of their clients can actually be collected.

3 ePayment

Electronic payment or ePayment is the transfer of electronic means of payment from the payer to the payee through the use of an electronic payment instrument [11].

ePayment systems are used to transfer money from one account to another at the same or another financial institution. ePayment is an important part of eCommerce, as goods and services offered through the Internet are most conveniently paid in electronic form.

Several factors influence payment over the Internet [8]. For example, the Internet does not have an established security architecture. Both seller and buyer are not physically present in an online transaction. Goods are available only as virtual representations. And there is no synchronization between payment and delivery of goods.

3.1 Classification

Numerous ePayment systems are on the market. They can be classified based on several categories, see [1] and [11]. ePayment systems can be divided into electronic cash mechanisms and credit-debit systems. Electronic cash resembles conventional cash and is based on tokens. Electronic tokens represent value and are exchanged for payment.

Credit-debit systems are based on bank accounts. In credit-debit systems, money is represented by records in bank accounts. Payment information is sent over computer networks, e.g., the Internet. Electronic cash has several advantages like the potential for anonymity and the lack of the need to contact a central system. In *pre-paid systems*, the payer's account is debited before the payment. Pay-now systems debit the payer's account at the time of payment. In *post-pay systems*, the account of the payee is credited before the account of the payer is debited.

Another distinctive feature is *micro payment ability*. Micro payments typically amount to a value of less than 1 Euro or 1 Dollar. In contrast, macro payments start at an amount of 10 Euros/Dollars and small payments are in between. There can also be a limit on the amount of money that can be paid, e.g., the amount that had been prepaid or the credit card limit.

3.2 Available Systems

Too many ePayment systems are available to provide an exhaustive list. We have chosen a few that are widely available. Not all systems are offered world-wide; we have also included systems available in Austria, the home country of the authors. Additional ePayment providers and services can be found, for example, in [4].

Credit cards entitle their holders to buy goods and services based on the holders' promise to pay for these [5]. Credit card providers offer various levels of security in order to prevent fraud, e.g., the card security code. *Verified by Visa* and *MasterCard SecureCode* depict additional security measures for online transactions. When credit card information is entered online, the user has to authenticate herself, i.e., to confirm her identity with an additional password. *Debit cards* are used like credit cards for telephone and Internet purchases or like ATM cards for money withdrawal. In both situations, funds are immediately transferred from the holders' bank account. This is in contrast to credit cards, where users have to pay back on a later date. Maestro is an example for a widely known debit card service [www.maestrocard.com].

PayPal is an e-commerce business that allows worldwide payments and money transfers over the Internet [www.paypal.com]. *Paybox* offers payments via users' mobile phones in Austria. A user simply provides her phone number or, for anonymity, an alias number, gets an SMS (simple text message) from PayBox and confirms the payment [www.paybox.at]. *PaySafeCard* is a pre-paid system primarily for online shopping. It allows online cash payments without a bank account or credit card [www.paysafecard.com].

4 ePayment Requirements

Concerns on data security and on the misuse of private data are important factors for electronic payments. These concerns alone can hinder the development of e-commerce [15]. Security requirements will depend on the amount of money being transferred, i.e., macro payments require higher security than micro payments. Smaller risks and cost considerations lead to the acceptance of less security. However, concerns about security are key factors in discouraging consumers from online payments [9].

Security comprises integrity, availability, and confidentiality [8]. For online gaming, anonymity is an additional important security aspect. ePayment providers have to make sure that all these facets are considered sufficiently, including e.g., software security, network security and organizational security. The payment card industry data security standard helps organizations of payment cards to prevent fraud [6]. This can be achieved through increased data controls and decreased exposure of data to potential compromise. Evaluating the security of systems is a difficult and time-consuming task. In order to make this task manageable for our purpose, we will use the following properties that can be assessed with reasonable effort.

Passwords. How many characters must users enter in order to enter the system? We use a qualitative measure – high if a minimum length of eight characters and compliance to defined rules, e.g., use of special characters, are required; medium if passwords are used but do not comply with rules and low if no passwords/PINs are employed.

Password renewal. Password renewal defines whether users are asked to change their passwords periodically.

Login brute-force. Login brute-force prevention addresses effective measures for preventing brute-force attacks, see [12].

Certificates and SSL. Certificates and the use of SSL/TLS address the security of the communication channel, e.g., whether communication is encrypted and authenticity of the counterpart can be determined.

Authentication. We again use a qualitative measure – two-factor authentication, one factor authentication and authentication that is solely based on information that cannot be considered as sufficiently secret, e.g., account information or credit card numbers. Two factor authentication means that authentication is based on knowledge, e.g., passwords, and the possession of artifacts like cell phones. As access or transactions codes are sent to these cell phones, their possession is crucial for payments. One factor authentication is based on knowledge or possession.

Lock-out. Systems may lock out a certain user upon request. A lock-out can be initiated by users whenever they realize that authentication information had been lost or stolen in order to prevent malicious transactions.

Anonymity. We differentiate between information that is easily linked to identities like credit card numbers and information that is more difficult to use to reveal identities, e.g., phone numbers. Thus, we use yes/no values.

Additional security features address the fact whether critical transactions are secured by certain measures, e.g., use of transaction authentication numbers (TAN). Additional non-security requirements include micropayments, guaranteed payments, cross-border payments, offline payments and market penetration.

5 Analysis

As ePayment systems rely on different paradigms, they are difficult to compare. Our analysis does not aim at determining the best or most secure system. Instead, we want to provide a comprehensive overview on functionalities and security aspects of different systems.

5.1 Methodology

An evaluation determines the value or usefulness of a solution with respects to given objectives. Use-value analysis does not only cover quantitative but also qualitative criteria [7]. It involves the following steps [2]:

- Identification of evaluation criteria
- Assessing values of criteria for each system (quantitative or qualitative)
- Quantification of qualitative values (scaling)
- Weighting of criteria depending on importance

For the analysis, we use criteria outlined in section 4 together with requirements concerning system flexibility, e.g. micro payment or cross border payment ability.

5.2 Results

Table 1 shows the parameter values of the different systems. The values were retrieved by literature analysis, statistics, interviews of ePayment system providers and self-experimentation. We have to quantify our qualitative measures. We rank "high" by 3, "medium" by 2 and "low" by 1 and further "yes" by 3 and "no" by 1. Therefore, systems with higher use-values will be preferable. We can compare the systems based on these values. The adequacy of the values depends on the point of view, e.g., seller or buyer. We can reflect this by assigning different weightings to the chosen criteria. These weightings are calculated as follows: We use a base of 100. Since we have 14 criteria, we get an average weighting of 7 (100/14 rounded). We almost triple the average weighting and use 20 as a maximum weighting factor for eminently significant criteria. Since less important criteria shall not be completely disregarded, we use 3 as minimum weighting factor. Different points of views can be reflected by assigning different weightings in the range of 3 to 20.

A user study has shown that it is important from the perspective of customers to guarantee anonymity, ease of use and security. Furthermore, customers prefer systems that they already use or that they can use in other contexts too, i.e., flexible systems with high market penetration [3]. Given these considerations, Table 2 shows the results of our use-value analysis from a customer perspective. *Click & Buy* emerges as the preferable system. In contrast, providers demand payment guarantees as well as high market penetration in order to prevent customer distraction [10]. *Click & Buy* is also preferable from a provider perspective. This table is not shown due to space limitations.

An advantage of such use-value analyses is that they are easy to adjust according to requirements in a given context. For example, if it is central to provide high flexibility, we can adjust the weightings of micropayment ability, cross-border payment ability and offline payment ability and conclude that Paybox is our first choice.

6 BetMPay

Although there are many ePayment systems available, there can be application contexts in which requirements cannot be fulfilled by existing systems. In this section, we will describe *BetMPay* – a system that has been developed to support special needs of online gaming companies. These special needs are anonymity, prevention of customer addiction and a high level of payment guarantees.

Table 1: Values of Payment System Criteria

Criteria/ System	Credit Card using SSL	Verified by VISA	Paypal	Paysafecard	Paybox	Click and Buy	Debit Card
Password Strength	Low	Low	Med	Med	Med	High	Low
Password Renewal	No	No	No	No	No	Yes	No
Login Brute Force	No	No	Yes	No	Yes	Yes	No
Certificates	Yes	Yes	Yes	Yes	Yes	Yes	Yes
SSL/TLS	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Authentica-tion Method	Low	Med	Med	High	High	Med	Med
User Lock-out	Yes	Yes	No	No	Yes	Yes	No
Additional Security	No	No	No	Yes	Yes	No	Yes
Market Penetration	High	Low	High	Med	Med	High	Low
Anonymity	No	No	No	Yes	Yes	Yes	Yes
Micro-payment	No	No	Yes	Yes	Yes	Yes	Yes
Payment Guarantee	Low	High	High	Low	Med	High	Low
Cross border Payment	Yes	Yes	Yes	Yes	Yes	Yes	No
Offline Payments	Yes	Yes	No	No	Yes	No	Yes

Table 2: Use-values from a Customer Perspective

Criteria/ System	Credit Card using SSL	Verified by VISA	Paypal	Paysafecard	Paybox	Click and Buy	Debit Card	Weighting
Password Strength	3	3	6	6	6	9	3	3
Password Renewal	3	3	3	3	3	9	3	3
Login Brute Force	6	6	18	6	18	18	6	6
Certificates	15	15	15	15	15	15	15	5
SSL/TLS	15	15	15	15	15	15	15	5
Authentication Method	10	20	20	30	30	20	20	10
User Lock-out	15	15	5	5	15	15	5	5
Additional Security	5	5	5	15	15	5	15	5
Market Penetration	30	10	30	20	20	30	30	10
Anonymity	15	15	15	45	45	45	45	15
Micro-payment	10	10	30	30	30	30	30	10
Payment Guarantee	3	9	9	9	3	6	9	3
Cross border Payment	30	30	30	30	30	10	10	10
Offline Payments	30	30	10	10	30	30	10	10
Use-value	**190**	**186**	**211**	**239**	**275**	**257**	**216**	

6.1 Context

Online gaming is a sensitive area, since it may impose dangers on customers, e.g., getting addicted. We can therefore identify three main requirements: At first, customers need anonymity. They may not want that others know about their activities. Furthermore, we need a mechanism that helps to prevent addiction. Finally, providers demand payment guarantees. They may regularly get in contact with (addicted) indebted or insolvent customers. *BetMPay* supports all three major requirements.

6.2 Scenario

Anonymity is one critical success factor of ePayment systems. *BetMPay* operates according to the following paradigm: Customers can buy vouchers for bets (offline) in gaming offices, kiosks or petrol stations. These vouchers represent a fixed value which can be used for gaming activities on online platforms. For this purpose, the customer has to register at a web application when she uses the payment system for the first time. The only information needed for registration is a valid cell phone number.

The system does not store any names, addresses or bank account data. If buyers do not disclose their cell phone number, e.g., by enlisting in phone directories, their identity cannot be determined using common methods.

After registration, the customer can enter a 16-character code printed on the voucher. The amount of the voucher will be credited to her account and can be used for gaming activities. Whenever customers win a game or decide to withdraw money credited to their account, they can create a payment ticket. The ticket consists of a security code which is sent to the customer via SMS. Afterwards she may go to gaming offices or kiosks, where the payment ticket is validated by cell phone number and the security code. The amount will get cashed out.

Together with a high level of anonymity, this paradigm further supports the other major requirements. On the one

hand, it provides better cost control for customers. As many customers of online gaming companies are compulsive gamblers, the system requires them to buy additional vouchers offline. This is not as comfortable as transferring money from bank accounts by means of credit cards, but it gives gamblers a chance to rethink their decision ("cool down phase") and can prevent them from making overhasty investments. On the other hand, the system provides guarantees for gaming companies: Customers can only bet with payments already made (pre-payment). As compulsive gamblers are often heavily indebted or even insolvent, companies do not have to fear losses or costly legal processes in order to recover debts.

6.3 System Architecture

The architecture of *BetMPay* is conceived in a classical three layer approach**.** The client is designed as a thin client using HTML in order to omit installation of software on the client side. Business logic is realized by ASP.NET components, which are operated by an IIS server. Data logic is realized using SQL databases. Since we do not use stored procedures, views or triggers, we support almost any relational database product.

6.4 Risks and Countermeasures

We will outline *BetMPay*'s major risks and countermeasures from the perspective of design and implementation.

System Design. The system faces two fundamental security risks. At first, malicious users may fake vouchers by auto-generating the 16-character code and therefore be able to transfer credits, for which they never paid. To mitigate this risk, special measures for creating the code are used. The code is separated into an application number, a ticket number and one part of a ciphered message. The other part of the ciphered message is stored in a database when the code is generated. Whenever a user redeems a voucher, the two parts of the message get assembled, deciphered and compared to the template. Thus, the validity of the voucher can be checked.

The second fundamental risk is the fact that cashing out requires the possession of a specific cell phone. If the cell phone gets lost or stolen, other persons may retrieve money from the account. The risk gets reduced primarily by the circumstance that users have to create payment tickets. Users can create such tickets only with the password of the account. We have a two factor authorization in this case, i.e., possession of the cell phone and knowledge of the password. In addition, payment tickets are sent to the cell phone via SMS. Customers can ask their cell phone provider to lock the phone as soon as they recognize their loss. The cell phone will not be able to receive SMSs anymore. This provides further protection even in the case when a malicious person has the phone and knows the account password.

Generated payment tickets could be used when a cell phone gets stolen or lost. In case the malicious person only has the cell phone but does not know the account password, the customer may lock the account and therefore prohibit any cashing outs. If the malicious person also knows the account password, he can change the password and prevent logins by the regular customer. This risk can only be overcome by instructing users to use their payment tickets carefully. For example, they should be generated only shortly before a cashing out is requested.

System Implementation. *BetMPay* uses several strategies for mitigating common security risks, like brute forcing, SQL injection, or man-in-the-middle attacks. In order to prevent login brute force attacks, the number of login attempts within a certain time frame is determined. Whenever a certain threshold is exceeded, the user gets locked. SQL injection attempts can be mitigated by input validation. We use a double strategy and validate input on the client as well as on the server side. On the client side, a configurable AJAX component is used whereas the server side validation is done by .NET methods. For preventing man-in-the-middle attacks, communication between client and server is encrypted by means of HTTPS and the use of a certificate signed by a trusted certificate authority.

Password policy. A configurable AJAX component on the client side informs users whether their password complies with defined rules (minimum length, special characters). Additionally, passwords are checked on the server, e.g., if passwords have been used before. Users have to update password periodically.

6.5 Evaluation

Table 3 shows the results of the use-value analysis of *BetMPay* that have been gathered from a usability study. *BetMPay* is ranked third from a customer perspective and fourth from a provider perspective. This comes from restrictions regarding cross-border payment ability and the market penetration of this system. The aspect of preventing overhasty decisions has not been considered in our analysis. We can therefore conclude that if market penetration can be increased and cross-border support will be added, *BetMPay* will be a good choice for online gaming.

7 Related Work

Benefits and costs of ePayments as well as a tool for system comparison are given in [16]. There are also evaluations and comparisons of electronic payment systems.

Table 3: Use-values of BetMPay

Criteria	Weighting Customer Perspective	Value Customer Perspective	Weighting Provider Perspective	Value Provider Perspective
Password Strength	3	9	3	9
Password Renewal	3	9	3	9
Login Brute Force	6	18	3	9
Certificates	5	15	6	18
SSL/TLS	5	15	7	21
Authentication Method	10	30	5	15
User Lock-out	5	15	5	15
Additional Security	5	15	3	9
Market Penetration	10	10	15	15
Anonymity	15	45	5	15
Micro-payment	10	30	10	30
Payment Guarantee	3	9	20	60
Cross border Payment	10	10	10	10
Offline Payments	10	10	5	5
Use-value		**240**		**240**

Wright evaluates privacy, traceability, transaction cost, and the ability to build up the customers purchasing pattern of credit card payment systems, an electronic check system and digital cash systems. He evaluates advantages and disadvantages to customers, merchants, service providers as well as financial institutions [13]. Wright suggests a new system for increased user acceptance, which allows payments over telephone networks for purchases made over the Internet. Yu et al. explore advantages and limitations of online credit card payment, electronic cash, electronic checks, and small payments. Systematic and detailed comparisons of alternative systems are provided [14]. Their analysis was targeted at companies planning to adopt or to improve an ePayment system.

8 Conclusion

We have shown an evaluation of various ePayment systems by employing a use-value analysis. Key success factors of ePayment systems are security and flexibility. There is no "best" or "most secure" ePayment system. The adequacy of these systems depends on the application context. Use-value analysis is an appropriate and easy to use evaluation method, since it allows the consideration of different application perspectives. Despite the fact that many ePayment systems are available, there are contexts that require tailored solutions, as is the case with online gaming. We have introduced *BetMPay*, an ePayment system that offers a high level of anonymity, payment guarantees for providers, as well as consumer protection. One major drawback of *BetMPay* is that it requires an established selling infrastructure, i.e., concluding contracts with gaming offices or kiosks.

References

1. Abrazhevich D.: Electronic Payment Systems: a User-Centered Perspective and Interaction Design, 2004. http://www.idemployee.id.tue.nl/g.w.m.rauterberg/publications/PhD-Thesis%20%28Abrazhevich%202004%29.pdf
2. Heinrich L.J.: Informationsmanagement, 7th Edition, Oldenbourg 2002.
3. Leibold K., Stölzle R., Stroborn K.: ePayments und die Meinung der Konsumenten – Online-Survey; in Handbuch ePayment. Zahlungsverkehr im Internet: Systeme, Trends, Perspektiven (Ketterer K.H., Stroborn K.). Fachverlag Deutscher Wirtschaftsdienst, Köln 2002, p. 109-118.
4. NACHA – Electronic Payments Association. Electronic Payments Review & Buyer's Guide 2009. www.nacha.org
5. O'Sullivan, A., Sheffrin S.M: Economics - Principles in Action, Prentice Hall, 2003.
6. Payment Card Industry (PCI). Data Security Standard Requirements and Security Assessment Procedures, Version 1.2.1, July 2009. www.pcisecuritystandards.org/security_standards/pci_dss.shtml
7. Pahl G., Beitz W., Wallace K., Feldhusen J., Blessing L.: Engineering Design: A Systematic Approach, 3rd Edition, Springer 2007.
8. Slay, J., Koronios, A.: Information Technology, Security and Risk Management John Wiley & Sons, 2005.
9. Sumanjeet S.: Emergence of Payment Systems in the Age of Electronic Commerce: The State of the Art, Global Journal of International Business Research Vol. 2. No. 2. 2009.
10. Tan, M.: E-Payment – The Digital Exchange, Singapore University Press, 2004.
11. Tsiakis T., Stephanides G., Pekos G.: Trust and Security in Electronic Payments: What We Have and Need to Know? www.waset.org/journals/waset/v5/v5-36.pdf, 2005.
12. Viega J., McGraw G.: Building Secure Software, Addison-Wesley Professional Computing Series, 2002.
13. Wright, D., Comparative Evaluation of Electronic Payment Systems, Infor -Ottawa-, Vol. 40, Part 1, pages 71-85, 2002.
14. Yu H.-C., Hsi K.-H., Kuo P.-J., Electronic payment systems: an analysis and comparison of types, Technology in Society 24, pages 331-347, 2002.
15. Electronic Payment Systems Observatory (ePSO), Building Security and Consumer Trust in Internet Payments, – The potential of "soft" measures, Background Paper No. 7, 2002
16. Electronic Payments, www.electronic-payments.co.uk.
17. Wikipedia,Gambling, http://en.wikipedia.org/wiki/Gambling