A MODEL FOR SECURE VALUE-ADDED SERVICE SUBSCRIPTIONS IN CELLULAR NETWORKS

Stephen Perelson, Jacobus Ophoff and Reinhardt Botha

Centre for Information Security Studies,
School of ICT,
Nelson Mandela Metropolitan University,
South Africa

{stephen,jophoff,reinhard}@nmmu.ac.za, +27 (0)41 5043669, PO Box 77000,
Nelson Mandela Metropolitan University, Port Elizabeth 6031, South Africa

ABSTRACT

The current trends in South African cellular Value-Added Services are a melting-pot of consumer dissatisfaction. Only recently have regulations begun ensuring consumer protection. However recent experiences with subscription-based Value-Added Services have shown that the stricter regulations do not protect the consumer in a timely manner.

The authors review Value-Added Services and the problems therewith and then go on to examine recent regulations dealing with these issues. The authors propose a procedural solution, which addresses the lack of compliance with the regulations regarding subscription-based Value-Added Services, to ensure customer protection.

The proposed solution intends to implement customer authorization prior to a successful service transaction and in so doing avoid many of the existing problems with subscription-based Value-Added Service.

KEYWORDS

Cellular communications, Value-Added Services, Security

A MODEL FOR SECURE VALUE-ADDED SERVICE SUBSCRIPTIONS IN CELLULAR NETWORKS

Our case study begins with Tim, an IT professional. Tim is a long time subscriber to a cellular phone network in South Africa. Due to his interest in mobile technology he has followed the trends in cellular Value-Added Services (VAS) as they have developed. Tim makes a point of not purchasing any VAS that he can easily get free. He is also rather distrustful of how others may use any personal information that they may get – including his phone number. He is especially wary of the now common trend of subscription-based VAS offerings.

It came as a surprise then when he received an unsolicited text message, illustrated in Figure 1, from a company he had never heard of. Tim is no fool and being distrustful of any spam decided to save it but ignore it.

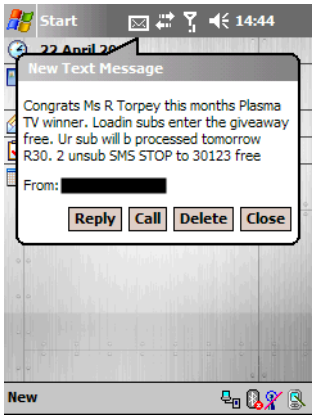

Figure 1: First Text Message

A few days later Tim was shocked to receive another text message, shown in Figure 2, from the same company. His shock stemming from the fact that the message was purportedly claiming to have successfully billed him for a subscription service he never wanted or asked for.

Tim decided to let his contact at the network operator know that something bad may have happened and then waited to see if the money was actually taken off his account.

Tim was furious when he noticed the deduction on his monthly statement. He immediately unsubscribed – thankful that he had kept the first text message – and let his contact at the network operator know how he felt about what had happened. He then continued to fill out and submit a detailed complaint to the Wireless Application Service Providers' Association (WASPA) [1]. The reason he did this is that the company that offered the subscription-based VAS stated clearly on their website that they adhere to the WASPA Code of Conduct.

In this article we examine VAS offerings, first giving a general overview and highlighting some potential risks for subscribers. We then review consumer protection mechanisms that are currently being employed before going on to propose a procedural model to prevent subscription service fraud. We conclude with a look at related risks using the Short Message Service (SMS) after which we summarise our contribution.

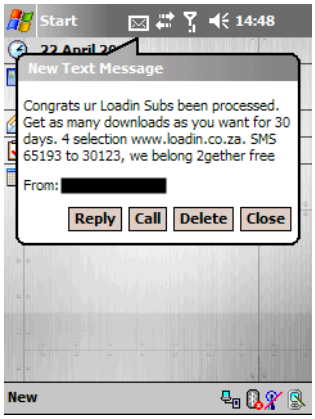

Figure 2: Second Text Message

1 A DESCRIPTION OF VALUE-ADDED SERVICES

In today's competitive cellular market network operators are continuously searching for ways to increase their Average Revenue Per User (ARPU). In addition to standard voice calls the use of SMS, Multimedia Message Service (MMS) and data services such as General Packet Radio Service (GPRS), Universal Mobile Telecommunications System (UMTS) and High-Speed Downlink Packet Access (HSDPA) provide a major source of revenue. These additional services are examples of what are generally considered to be VAS offerings [2].

The provision of VAS offering can be done by the network operator themselves or by a VAS provider. In the latter case the VAS provider connects to the network operator using standard protocols or gateways, allowing the operator to control and charge for the content appropriately [2]. The different VAS demonstrate and share many of the same characteristics. Classification of different VAS offerings can be done according to the following criteria [3]:

- Not a core network service but utilizes existing services to add value to the total service offering.
- Operationally independent from other services and can be used alone.
- Independent in generating revenue and/or stimulates an increasing demand for core network services.
- As an add-on to a basic service and possibly sold at a premium rate.

Table 1 provides an example of some of the more popular VAS offerings, namely MMS and ringtones, and classifies them according to some of the criteria defined above.

Table 1: VAS Offering Examples

VAS	Core Service	Operationally Independent	Premium Rate
MMS	No	Yes	No
Ringtones	No	No	Yes

An MMS is not generally considered a core network service although with increased use it might become one in the future. It does not however rely on any other services to operate and is charged at a fixed rate. Ringtones also add value to the total service offering but rely on other services, such as SMS, to operate. It is also charged at a premium rate, varying according to the specific provider.

Using the above examples a distinction can also be made between once-off and subscription-based VAS offerings. An MMS can be seen as a once-off service where the customer is charged once for the service and the content is delivered immediately, thus terminating the transaction. Although ringtones could work in the same manner it is much more common nowadays to find them packaged as a subscription-based service where the customer pays a monthly fee and content is continuously delivered until the subscription is stopped. Such subscription-based VAS are seen as a large source of potential revenue with providers marketing their product offerings widely to a large prospective customer base.

Currently a big concern with VAS offerings is the lack of regulation regarding the proper operating procedures for VAS providers. Subscription-based VAS suffers from a lack of authorization, thus putting all the power in the hands of the VAS provider. Additionally VAS advertising is often ambiguous and misleading resulting in unwary customers being charged for services they do not really want.

In the next section we will examine the attempts that have been made to regulate the industry and protect the consumer by the WASPA Code of Conduct.

2 CONSUMER PROTECTION

WASPA was launched in August of 2004 with the support of South Africa's three network operators. As stated on their website, WASPA aims to

> "uphold public perception of these [mobile] services and to protect against bad practices... with an appropriate Code of Conduct, representing the interests of its members and consumers, by enforcing the good practices established by this Code." [1]

WASPA acts as an umbrella organization, representing the interests of the consumer as well as protecting the liability of its members. At the core of WASPA is their Code of Conduct which sets the standards according to which its members should operate [4]. When examining the applicable sections to our introductory scenario the Code of Conduct states very clearly that

> "any request from a customer to join a subscription service must be an independent transaction, with the specific intention of subscribing to a service." [Section 11.1.2]

Tim played no part in the transaction that caused him to be subscribed to the VAS. In this case, because the offending VAS provider was a member of WASPA, he was able to lodge a complaint against the VAS provider which would be evaluated and responded to by WASPA. Similar complaints have also been lodged in the past with successful complaints resulting in heavy fines for the VAS provider as well as requirements to refund complainants or remedy breaches [5].

Even though such regulations exist consumers still need to undergo lengthy procedures before their complaints are heard and acted upon. For consumers unaware of WASPA their network operator is probably the only place for them to turn to. In the next section we propose a solution which attempts to eliminate the need for such lengthy procedures by adding an extra authorization step to subscription-based VAS.

3 PROPOSED SOLUTION

Our solution attempts to enforce a strict procedure before a customer is subscribed to a VAS. This subscriber authorization procedure, as shown in Figure 3, will rely upon the network operator enforc-

ing rules that the VAS provider must follow. It is important that the inconvenience that the verification process introduces to the customer is outweighed by the inconvenience of being subscribed to a service they do not want.

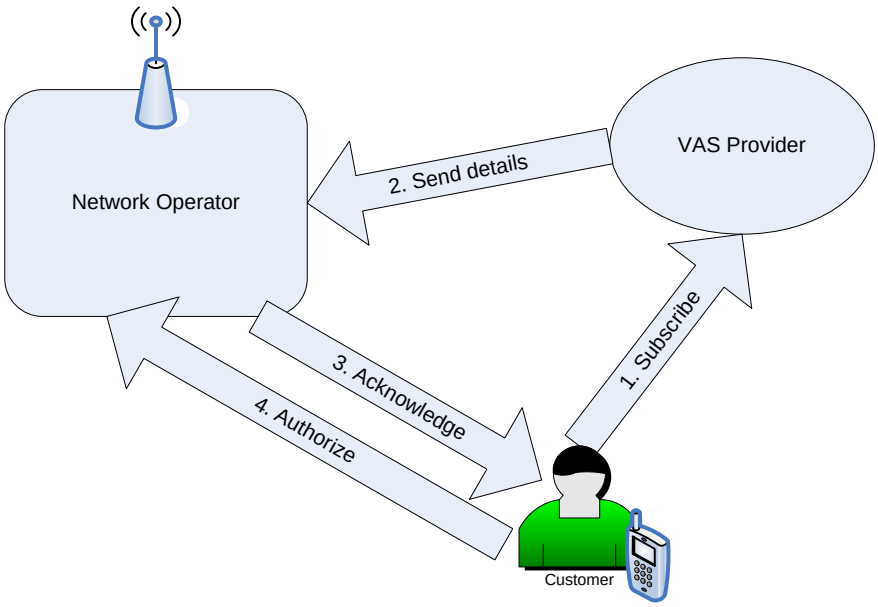

Figure 3: Subscriber Authorization Procedure

The subscriber authorization solution demands that the network operator verifies the customer's subscription. The VAS provider will not be allowed to bill the customer until the subscription has been verified. It is important to note that this proposed solution is only applicable for subscription services and not for preventing SMS spoofing, as discussed in Section 4.

This solution would work as follows:

1. Customer acknowledges VAS service through some means (SMS, email, website, etc).
2. VAS provider sends customer and service details to network operator.
3. Network operator sends the details of the particular subscription VAS to the customer in a text message asking for acknowledgement.
4. Customer responds with the correct code and gets subscribed or ignores the message.

The first step involves the customer subscribing to a subscription-based VAS through a text message or website. The customer may have discovered the service through advertising or some other method. It is possible that through miscommunication in a badly designed advert, or through word of mouth, that the customer is not fully aware of the financial implications of the subscription service.

The second step involves the VAS provider collating the details and sending them to the network operator for validation. The network operator, acting as a trusted third party, then asks the user to authorize the transaction.

This authorization is outlined in the third step and would involve sending a text message as depicted in Figure 4 to the customer. This text message could be paid for by the VAS provider as part of doing business.

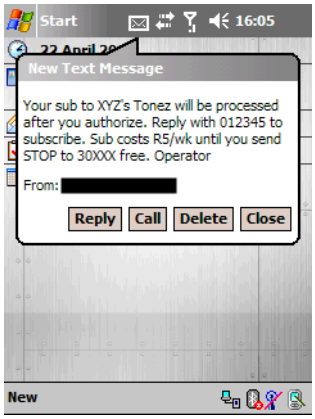

Figure 4: Confirmation Text Message

The customer then has the option of replying with the provided code as the text message body as mentioned in step 4. The network operator would then use this code from the customer as authorization for the particular VAS provider's service offering. If the customer does not send a reply then the network operator will cancel the subscription after a set amount of time has passed as decided upon by the VAS provider. The network operator will not bill the customer until the successful completion of this authorization process.

It is possible for the customer to subscribe to many different services from the same VAS provider or from other VAS providers. In such a scenario the network operator would maintain a unique authentication code for each service for the particular customer.

The VAS provider may also unintentionally send the same subscription request as outlined in step 2 to the network operator. The network operator should prevent the customer from getting multiple authorization requests. The VAS provider may be charged for every request sent to the network operator to protect against abuse of the service.

The subscriber authorization procedure we are proposing aims to ensure a customer is only subscribed to services they want. In essence this solution places the final choice in the customers hands. The solution is modelled on what is currently possible with the given limitations in the Global System for Mobile Communications (GSM) network. These limitations include authentication in the GSM architecture and are outlined in the next section.

4 RELATED SECURITY ISSUES

In addition to VAS subscriptions other services, such as the ubiquitous SMS service, can also pose privacy issues to users. In this section we will highlight some of the security concerns associated with SMS technology.

The SMS has become truly ubiquitous with millions of messages being sent daily. The SMS has also been incorporated in other applications, forming an indespensable part of many systems. An increasingly popular example is online banking, where text messages are used to transmit a secret authentication code that users need to enter before a transaction can be completed succsessfully. It is also interesting to note that some companies have used text messages to notify employees of their dismissal [6, 7]. Although the circumstances under which this has occured are controversial it raises interesting moral questions about the extent to which this technology should be used.

With such a reliance on text messaging by individuals and companies alike it is important to ascertain whether there are any risks involved with the use of this technology. In a recent news report a woman was apparently sent a message by her spouse asking for help and money. As the message appeared to be coming from the correct number she immediately gathered some money, only to be attacked and robbed as soon as she stepped out of her front door [8].

As already mentioned, the lack of authorization is a serious problem with regards to VAS offerings. In a similar way the lack of SMS authentication can be abused to pose a serious security threat to a user. It is well noted that the GSM system is highly secure regarding the validation of a mobile station, the handset, on the network [9]. This is done through a well documented protocol which has remained secure despite numerous attacks against it. However assuming the same level of security regarding text messaging can be a catastrophic and costly mistake. This is due to the lack of authentication when a message is sent. Text messages are not bound to a caller's number as voice communications are, but rather to an identifier which could be almost any value (although most commonly the mobile number of the sending user is used). It is well documented that spoofing a text message is a trivial exercise and that distinguishing such spoofed messages from legitimate ones can be very difficult [10]. This has lead to a large increase in phishing attacks [11, 12] against mobile users and impersonation attacks by third parties using such methods [13].

Should individuals just blindly accept text messages from seemingly legitimate numbers, and for that part any other message they receive, or should some consideration be paid as to the validity of each message. Finding a solution to such problems is not a trivial task as text messaging is a well established service that is used in a standard way by millions of users worldwide. Filtering software, similar to spam email filtering, could be a potential solution but would also prevent some legitimate messages from reaching the recipient. Another problem is evident in our case study; Tim would have missed the messages informing him of the VAS subscription and would only have noticed something suspicious on his next billing statement and would not have been in an informed position to do something about it. This could be solved if an SMS could be used for non-repudiation and there were mechanisms in place for guaranteed delivery and guaranteed reading [14].

Changing user habits or making a fundamental change to the system infrastructure is an almost impossible task, leaving user vigilance as the most likely short term solution to such risks. The conclusion proposes future research to address such issues.

5 CONCLUSION

After a while the network operator contacted Tim to say that the money would be refunded. Tim is still waiting for the refund to appear on his statement. . . .

Tim's story is not unique. Shady practices with regards to VAS operators abound and there is little consumer protection. WASPA has the power to enforce practices and to fine violators; however, the consumer is still largely unprotected.

In this article we have examined subscription VAS and pointed out the security risks that unsuspecting cellular users could face. Furthermore we have discussed the efforts that have been undertaken to regulate the industry and protect the customer, namely the WASPA Code of Conduct. Even though this Code of Conduct is very comprehensive and provides for a reasonable level of consumer protection, many VAS providers fail to comply fully with these regulations.

In an attempt to address this lack of conformation we presented a procedural solution to protect the customer from being unwillingly subscribed to a VAS. Even though our process involves some extra work for the customer and the VAS provider, we feel that the benefit to the customer makes this worthwhile. If the network operator charges the VAS provider for the acknowledge and authorization steps they are guaranteed an extra revenue stream and the charge to the VAS provider can be considered an incentive for adhering to the Code of Conduct. This charge to VAS providers should help

ensure that more care is taken when submitting prospective customer details to the network operator.

We also briefly overviewed similar security concerns regarding SMS technology. It is clear that SMS spoofing will become an increasing problem for cellular users and will not be an easy problem to solve. Future research will be necessary to analyse the extent of the security risks and establish the best practises to deal with this problem.

In conclusion, we hope that our solution finds favour with network operators and VAS providers, and that Tim's experience will not have been in vain.

6 ACKNOWLEDGEMENTS

The financial assistance of the National Research Foundation (NRF) is hereby acknowledged. Opinions expressed and conclusions arrived at, are those of the authors and are not necessarily to be attributed to the NRF.

7 REFERENCES

[1] Wireless Application Service Providers' Association. WASPA Website [online]. 2006 [cited 21 April 2006]. Available from: `http://www.waspa.org.za`.

[2] Wikipedia, the free encyclopedia. Value-added service [online]. 2006 [cited 21 April 2006]. Available from: `http://en.wikipedia.org/wiki/Value-added_service`.

[3] Mobile in a Minute. Value-added Services [online]. 2006 [cited 21 April 2006]. Available from: `http://www.mobilein.com/what_is_a_VAS.htm`.

[4] Wireless Application Service Providers' Association. Code of Conduct [online]. 2006 [cited 21 April 2006]. Available from: `http://www.waspa.org.za/code/codeconduct.shtml`.

[5] Wireless Application Service Providers' Association. Complaint Reports [online]. 2006 [cited 21 April 2006]. Available from: `http://www.waspa.org.za/code/complaint_idx.shtml`.

[6] Bonnie Malkin and Sherrill Nixon. U R out: man fired by SMS [online]. 2003 [cited 23 April 2006]. Available from: `http://www.smh.com.au/articles/2003/04/14/1050172541832.html`.

[7] ABC News Online. Woman sacked by SMS, union says [online]. 2006 [cited 23 April 2006]. Available from: `http://www.abc.net.au/news/newsitems/200604/s1609997.htm`.

[8] Indiatimes Infotech. The new phony crime: SMS spoofing [online]. 2004 [cited 23 April 2006]. Available from: `http://infotech.indiatimes.com/articleshow/msid-776694.cms`.

[9] Chii-Hwa Lee, Min-Shiang Hwang, and Wei-Pang Yang. Enhanced privacy and authentication for the global system for mobile communications. *Wireless Networks*, 5(4):231–243, 1999.

[10] Denis Pankratov and Dmitri Kramarenko. SMS spoofing – Q&A with CCRC staff [online]. 2004 [cited 22 April 2006]. Available from: `http://www.crime-research.org/interviews/sms-spoofing-intro`.

[11] Steven M. Bellovin. Spamming, phishing, authentication, and privacy. *Communications of the ACM*, 47(12):144, 2004.

[12] David Geer. Security Technologies Go Phishing. *Computer*, 38(6):18–21, 2005.

[13] Claude Castelluccia and Gabriel Montenegro. Protecting AODV against impersonation attacks. *ACM SIGMOBILE Mobile Computing and Communications Review*, 6(3):108–109, 2002.

[14] Tom Coffey and Puneet Saidha. Non-repudiation with mandatory proof of receipt. *ACM SIGCOMM Computer Communication Review*, 26(1):6–17, 1996.