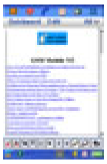
Few words about – why not SMS for Authentication

http://www.gsmmobile.co.nz/index.php?name=News&file=article&sid=253

News ASB Bank pushes ahead with RSA Mobile



By TOM PULLAR-STRECKER and AFR - ASB Bank is pressing ahead with a plan to use mobile phones and text messaging to improve the security of internet banking, despite a decision by RSA Security - the US specialist behind the technology - to stop marketing it.

IT manager Clayton Wakefield says the bank is expanding its trial of a "two-factor" authentication system and is likely to make the security option publicly available to at least some customers later this year.

ASB has been using software system RSA Mobile to send randomly-generated one-off access codes to customers' mobiles once they log on to its internet banking website using their regular password, under a trial which kicked off this year.

Customers rekey the one-off access code into a field in its website to authenticate transactions.

Two-factor authentication is designed to prevent criminals from initiating a fraudulent transaction without obtaining both their victim's log-on and password, and the requisite hardware device - in this case their mobile phone.

RSA Asia-Pacific vice-president Sebastian Moore says there are major flaws with SMS authentication services, including the cost to organisations of delivering millions of SMS messages every year and poor mobile phone coverage in some areas.

He says that when banks evaluated the technology they soon realised it was too costly. RSA had been forced to withdraw RSA Mobile from the market following poor take-up, "until such time as the market changes", Mr Moore says.

It will continue to support ASB Bank, as it is a current customer.

"Everyone is interested in SMS authentication but, once they start to evaluate it, take-up is low because of the cost of sending the messages," Mr Moore says.

"There's also no guarantee of getting SMS messages when you're overseas or at home in a valley."

Mr Moore says the cost of sending SMS messages could amount to tens of millions of dollars a year.

"If you assume it costs 25 cents a message and an organisation had a million internet users, SMS costs are going to add up quite considerably."

Mr Wakefield says ASB Bank was "a little bit surprised" by the decision.

"We think it is the way to go, going forward, and have been working with them on it."

Till now ASB has been trialling the system only with its staff, but Mr Wakefield says the pilot is now being expanded to include some other customers. Mr Wakefield doesn't believe Mr Moore's assumptions about costs and coverage are applicable to New Zealand.

"They are obviously having a breather for one reason or another."

In June, National Australia Bank became the first cab off the rank in Australia, announcing it would trial SMS authentication later this year.

NAB's manager of internet banking, Peter Bottomley, says estimates that it could cost $10 million a year just to send SMS messages to customers didn't ring true.

NAB would keep costs down, he says, by allowing customers who made regular payments to particular payees to pre-authenticate themselves with an SMS code only once, when they initially set up a payee account.

This would mean fraudsters wouldn't be able to siphon off people's cash to bank accounts under their control, but customers wouldn't have to use two-factor authentication to authorise payments to bank accounts into which they had previously transferred funds.

Customers who were travelling or knew they had poor mobile coverage from home could also opt to pre-authenticate themselves, which would get around some of the mobile coverage issues, says Mr Bottomley.

Mr Moore says RSA will concentrate its efforts on hardware and software tokens that also generate one-time access codes and push ahead with its "federated" security model whereby customers need only authenticate their identity once when visiting multiple websites.

Posted by webmaster on Tuesday, August 10, 2004 (18:46:50) (186 reads)

http://md.hudora.de/blog/guids/98/20/02112808460530 98.html

Thursday, 28. November 2002

SMS security risks highlighted by Friends Reunited hacking case

Breach of trust by two dismissed mm02 workers, rather than deeper problems, led to the release of private text messages to a jealous boyfriend that sparked a campaign on revenge against his cheating girlfriend. [...] Nourse obtained proof of his girlfriends' infidelity by persuading two friends, employees at O2, to intercept her text messages and pass them on to him. A spokeswoman for O2 told us this was only possible because of a breach of trust by two engineering workers who have subsequently been sacked and convicted for offences under the Data Protection Act. O2 is not prepared to release the names of the pair but tells us both were convicted and fined for DPA offences this July. The person who intercepted Nourse's girlfriend's messages worked in a "privileged position" at an engineer on 02's text platform. He was aided by another engineer. Cracker tools were not used to extract the text message, O2 told us. The firm said that, despite the incident, it is happy with its systems and users should feel comfortable about the using text messages.
Analysts Gartner said the case illustrates that SMS is not a secure environment suitable for sending confidential messages.
"The contents of SMS messages are known to the network operator's systems and personnel. Therefore, SMS is not an appropriate technology for secure communications. Most users do not realise how easy it may be to intercept," it warns.
Gartner added that the case also showed how important people issues - rather the technologies concerns - are in trying to prevent security breaches. [The Register]
08:46 | #

SMS Security flaw reported at Verizon.htm

Aug 12 2003

ThreeZee Technology, a security research firm say that they have located a bug within the Verizon Wireless Text Messaging system. The bug will allow any person to easily view mass lists of SMS messages sent to Verizon Cellular customers, including the telephone number and the text in the message.

The applications of the bug can be extended to signing the phone up for an online login at www.VText.com, thus gaining the ability to intercept messages sent to the phone, as well as the ability to make numerous charges to the customer's phone bill.

Verizon Wireless allows anonymous surfers to send text messages to their customers via their website. After sending the message, they are directed to a page in which they can view the status. The status page reveals a few things to the user: When the message was sent, the Tracking ID, the recipient's phone number, or @vtext.com email, the status, and when or if it was delivered to the handset.

This same page allows you to manually enter the tracking ID and the phone number or vtext.com email of the user who should be receiving it. By separating Message IDs with commas, you can submit a query only limited by the web server's maximum content limit.

Verizon states that you need to enter both the Tracking ID and the recipient of the message. This is where the bug comes into play. By simply entering a message ID, and omitting the phone number, you can track a single message, or hundreds. While the Tracking, or message ID may look foreign in ways, it's quite simple.

Think of the way an odometer turns on a car.. that is the basic idea of the ID.

Example 1: MsgID4_A54GKVHD
Example 2: MsgID4_3M5GKVHD

Starting after the "_", the message ID will progress in the order of A - Z, and 0 - 9. There seems to be no association with the time sent, or who it was sent to. Like the odometer, when a character/digit of the ID reaches the end (9), it will restart at A, and the preceeding character will increase by 1.

i.e:
MsgID4_A59GKVHD
MsgID4_A6AGKVHD

By submitting a query to the server with message IDs separated by commas, you will receive a huge list of telephone numbers and email addresses on the Verizon wireless network.

It's quite easy to discover a list of valid message IDs and the phone numbers associated with them. This in itself could be extremely useful for SMS spammers to gather a list of people which actively receive messages. Verizon also offers a service to members which allows them to view the text in a message they've sent. This only requires the message ID to view. Using this list of gathered valid message IDs, combined with the other service, you can spy on the full text of any message sent either via email, via vtext.com, or even messages sent from Verizon to its users.

When a customer signs up for a login at vtext.com for their phone, the password is then sent to the phone in a text message. Using a combination of the available bugs can lead a person to take partial control of the customer's account, opening the door to many different possibilities. This is including, but not limited to: Making charges to a customer's account, sending messages from their phone, and intercepting messages to the phone.

Verizon has not yet fixed this problem, which is why ThreeZee has not disclosed the full details of the bug, just the overview above.

http://www.articon-integralis.com/en/media_en/press_releases/2004/ai_150604en.html

Articon-Integralis' operating company Integralis warns of Hotspot vampires

Mobile handsets leaving users vulnerable to WLAN hacker attacks

15th June, 2004 - **Articon-Integralis' brand Integralis, Europe's Leading Security Systems Integrator, today warns that unwitting WLAN Hotspot users risk having their account details, including passwords, 'hijacked' by Hotspot hackers because of a serious security flaw found in the SMS validation process used by T-Mobile and Vodafone.** The flaw affects users signing up for the WLAN service via insecure Bluetooth enabled mobile phones, or potentially anyone using a vulnerable mobile phone in public when Hotspot hackers sign up for the service invisibly on behalf of the user.

Users face astronomical phone bills as hackers target this simple SMS validation process to gain unlimited Internet access from WLAN hotspot venues across Europe and the United States. Potentially, hackers could also open multiple Internet accounts which they could 'tout' in online forums. A key aspect of this 'hijack' is that the perpetrated fraud is untraceable.

Hotspot Access
Hotspot users wishing to surf the Web from a PDA or notebook PC can register

Latest News...

Articon-Integralis AG reports Q1 2005 results

Articon-Integralis AG preliminary Q1 2005 with that particular outlet's Internet provider from their mobile phone, via SMS. All they have to do is send a simple code word to their mobile phone operator or log onto a Hotspot web page to receive an SMS message containing their personal login data. This Internet account, which could have an unlimited validity period, can be used at Hotspots compatible with that mobile operator across Europe and the United States. Costs for accessing the Internet are billed automatically to the user's mobile phone.

"Hackers are in the process of racking up hundreds of pounds worth of illicit WLAN Internet access in less than the time it takes to buy a cup of coffee. We were astounded with just how easy it is to poach a Hotspot users' identity, particularly as our tests involved two of the country's most trusted mobile operators," says Tim Ecott Manager, Integralis S3 [Ethical Hacking] Team UK. "With the trend towards mobile working and roaming ever increasing this should be a wake-up call to the operators providing these services and a warning to consumers to start thinking about protecting themselves from the wireless threat in the same way that they would think about protecting their handset from a pick pocket on the street."

Hotspot Piracy

As documented by Integralis in May, several mainstream Bluetooth handsets have a weakness in their Bluetooth interface. Hackers can take advantage of this and gain unlimited WLAN Internet access from Hotspots worldwide.

Hackers use their laptops or PDAs at public places to scan for susceptible handsets with activated Bluetooth interfaces. Once the hacker has identified a handset, they then identify the type of operator and then initiate SMS communication with the target handset, submitting a request for personal Internet access login data or register the victim's mobile number on the operator's Hotspot web page.

After receiving the login data, the hacker can delete the SMS message from the target phone, erasing all traces of the fraud. In theory, they can use these devices to open as many anonymous accounts as desired – some with unlimited validity periods – from which they can attack web servers and cause other damage without being detected. All costs are accrued by the mobile phone owner. The entire process takes just a few minutes and victims only discover the damage when they receive their phone bill. The victim has practically no way of proving that this fraud has occurred.

How to prevent these attacks – recommendations from Michael Müller and Andreas Bröhl, Bluetooth and WLAN experts at Integralis:

Mobile operators should discontinue their SMS authentication checks for Hotspot users because it doesn't provide protection from attacks.
Handset users should only activate the Bluetooth functionality in a secure environment, under no circumstances in public places such as railway stations, airports or trade fairs. Furthermore, visible mode should also always be deactivated, although this will not guarantee 100% attack protection.
Last but not least, users should ask their manufacturers about new firmware versions

results and management board change

Articon-Integralis AG Annual Report 2004