FINDING A BALANCE

Keiron Dalton *discusses the existing vulnerabilities in 4G mobile infrastructure and the way forward for customer authentication*

Many of us have become highly reliant on mobile banking by now as a means of managing our finances both quickly and efficiently, which is why we feel so anxious when a story about a security vulnerability hits the headlines. Sheer convenience, along with the ongoing closure of many high-street branches, have propelled us into the arms of mobile applications, facilitating a radical change from traditional banking and the long waiting times of old.

Such is the pace of change that mobile banking has now become the most popular method of managing finances in the UK, and research by the British Bankers' Association suggests that this momentum is expected to continue as applications alone will surpass all internet, branch and telephone use by 2020. Retail banks have moved fast to capitalise on this consumer trend, with the number of high street branches falling over 50 percent since 1988.

As the power of mobile banking continues to thrive, progress in dealing with its vulnerabilities seems somewhat stagnant, however. A study by Symantec found a 54 percent increase in the number of new mobile malware variants in 2017 alone, highlighting how the mobile channel is being seen as an increasingly lucrative source of revenue for unscrupulous hackers.

> SMS IS VERY EASY TO COMPROMISE AND CAN OPEN BACK DOORS TO A TARGET'S BANK ACCOUNT

One particular vulnerability was recently highlighted by researchers at Purdue University and the University of Iowa, which found a string of 4G network errors allowing hackers to hijack phone numbers and pose as familiar organisations such as energy suppliers and high-street banks.

This flaw enables spoof text messages and calls to be sent to customers, asking what seem like harmless and routine questions. In this way, fraudsters can easily trick users into giving up their personal information, leaving their bank accounts, credit cards and other sensitive services open to exploitation. Scammers can even attach these messages to an existing message chain on a victim's phone, making it virtually impossible to identify whether or not an enquiry is legitimate.

The ways hackers can exploit this vulnerability do not stop there. Scammers can use the same security flaw to pull off a range of mobile-based attacks, from connecting to a 4G network using another's identity, to intercepting messages and even forcing other devices to disconnect from a mobile network.

REMAIN CAUTIOUS

These scams can be extremely sophisticated and convincing, so users should treat any inquisitive message with caution. Typical red flags include any message that asks you to confirm your identity, reveal banking details, or hand over cash. Customers should hang up on these calls and ignore these messages immediately, and report any suspicious activity to their legitimate operator.

As diligent as individuals can be, however, it is impossible to ensure complete security by simply telling customers what to do in a given situation, as there will always be an element of human error, which could lead to users inadvertently clicking a malicious link or sharing their personal details. It is, therefore, up to banks, mobile operators and service providers to improve their authentication procedures in a bid to keep their customers safe.

The use of SMS for one–time password authentication is bearing the brunt of blame for these scams, which is understandable, as when used in isolation, SMS is easy to compromise and can open back doors to a target's bank account.

But solely blaming the limitations of SMS risks ignoring deeper issues that are inherent in modern mobile infrastructure. These flaws stem from the ability of criminals to hack into the LTE network that all major cell operators rely on. The LTE network is shared and connects cell operators to mobile devices worldwide, so the majority of modern devices will be affected if the wider network is not secure.

Operators have been aware of these issues for some time and are moving fast to strengthen their networks from a technology standpoint, but the main challenge is that an operator is only as strong as its competitors and vulnerabilities in networks can therefore be easily created and left unaddressed. Mobile stakeholders such as the GSMA are well aware of this, and there is a growing argument that global regulatory standards must be looked at, but this will be a long process that will require agreement from a number of interested parties, each of which has complex and differing needs.

The importance of multi-factor authentication increases as mobile banking continues to grow in popularity

WORKING TOGETHER

Luckily, the fact that many operators are treating this as a priority is enabling some of the bureaucracy to be eliminated, with collaboration taking place to strengthen the mobile ecosystem in numerous forms. Leading operators are proactively working together to share insights on these threats to find workable solutions. A good example of this is the GSMA Mobile Connect programme, a global collaboration of operators which aims to create secure ecosystems for data insight sharing across multiple sectors. This is enabling banks and other institutions to offer customers a wide choice of verification methods and better understand customer behaviour, by incorporating security insights from operators and sharing best practice.

These initiatives are gaining good momentum, but the unfortunate reality is that the current mobile networks that we rely on are still inherently weak, and that any move to banish the use of SMS authentication would fall short of providing a comprehensive and long-standing solution to the problems that we are currently faced with.

All channels of authentication have vulnerabilities, but there are other technologies that can be easily adopted in order to strengthen them. The key thing to understand is that SMS is a perfectly effective method of authentication, but only when it is employed in conjunction with others as part of a multi-factor approach.

By making greater use of multi-factor authentication, customer preference in terms of how they manage the security of their accounts is protected, while still upholding the highest standards of security. SMS banking, for example is highly regarded by many customers, as it can streamline timely and complicated tasks such as managing transfers and balance enquiries.

The disruption being brought to mobile banking

by challenger banks such as Monzo is also enabling the online customer experience to rival that of a traditional brick and mortar service. These applications are offering customers unprecedented insights into their spending habits with immediate and effective customer support available around the clock, so for many, the prospect of now regressing to a traditional service holds limited appeal.

Ridding the verification methods that these services rely on risks dampening the customer experience and may affect the relationship between clients and their banks. With this in mind, the secret to greater security lies in strengthening the systems that we already have, rather than depriving customers of methods of interaction that they have been familiar with for a long time.

MULTI-FACTOR AUTHENTICATION

By requiring users to verify their identity through more than one independent credential, the likelihood of a security breach is greatly reduced. If one factor, say a password, is compromised or broken, an attacker will be faced with at least one more layer of defence to deal with, such as a one-time valid pin or passcode. Adding additional layers of complexity can greatly deter hackers from

2017 SAW A 54 PERCENT INCREASE IN THE NUMBER OF NEW MOBILE MALWARE VARIANTS

pursuing a victim, while maintaining the useful verification methods that customers enjoy.

There are many multi-factor authentication technologies to choose from, so organisations must select the methods that best suit them or the specific needs of their customers. Biometric verification such as retina and fingerprint scans, facial recognition and even hand geometry is now becoming more mainstream, as awareness grows and consumer perceptions become more positive and welcoming of its benefits. The good thing about these technologies is that they can be easily scaled up or down, so those users that would prefer not to employ a particular method of authentication can choose not to do so.

These technologies are extremely sophisticated and difficult to bypass on their own, let alone in conjunction with other methods. By taking a multi-factor approach to customer authentication, organisations can make security processes much more watertight, without compromising on the convenience that their customers value so highly. The face of corporate engagement is drastically changing, as people increasingly expect to engage with the organisations that matter to them via an increasingly diverse number of channels. Customer engagement has now spilled over to the likes of WhatsApp and Facebook Messenger, and those organisations that can offer this while maintaining a commitment to powerful authentication can gain a real competitive advantage.

These threats will become much less of a concern if organisations take more responsibility in securing their services and operators retain their proactive approach to patching gaps in security, and then combine this with a steadfast commitment to multi-factor authentication. The popularity of mobile banking is only likely to grow, so any efforts to curtail its use at the expense of customer experience are likely to end badly. Consumer demand is greater than it ever has been, and failure to meet these expectations can cause irreversible damage.

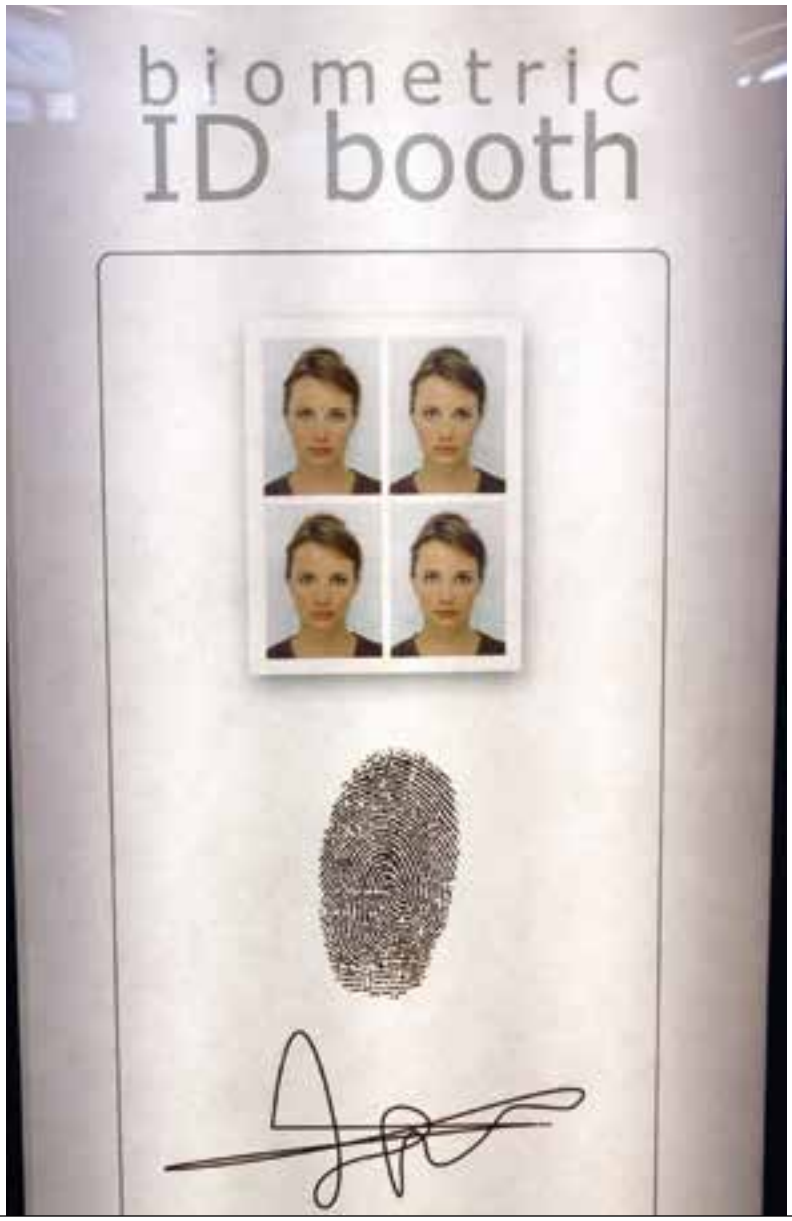
GETTING THE BALANCE RIGHT

Security should not come at the expense of customer satisfaction, and *vice versa*. Striking a balance is key. With a multi-factor approach, both attributes can be prioritised at the same time, as there is a wealth of verification tools that are both convenient to use and highly secure when used together.

By taking a personalised approach to security, and letting each individual choose the verification methods that they are most comfortable with, organisations can strike the perfect balance between security and usability. As the ever-changing nature of cyber crime reaches new heights, it's important that we do not lose sight of those that rely on our services ●

Keiron Dalton is responsible for the global strategic direction of Aspect Software's Verify mobile identity service. He possesses a wealth of experience of IT innovation, with mobile security being his key area of expertise.

Could biometric ID booths like this one replace regular photo booths in an effort to defeat the problem?



Picture credit: Getty