IDEMIA

Cybersecurity and the Road to Biometrics

Blog post 1/3 - By Philippe Le Pape, identity and security expert, VP Partnerships and Presales within the Digital Security and Authentication Division of Safran Identity & Security (formerly known as Morpho).

 # PAYMENT
 # CONNECTIVITY

POSTED ON 06.30.16

Last February, not coincidentally on "Safer Internet Day,"US President Obama announced the **Cybersecurity** National Action Plan (CNAP), a new initiative intended to strengthen US government and private-sector cybersecurity. The announcement came after an epidemic of data breaches and cyber-attacks on government and private networks.

Online fraud in the form of malware and phishing is engulfing the internet. In 2015 security company **Kaspersky Labs** detected over 100m malicious objects such as scripts, exploits, executable files, and so on. A worrying aspect of the criminal activity behind online fraud is the ease by which stolen identities and compromised accounts can be monetized. What's more, there is considerable evidence of increased sophistication in the forms of attack used by fraudsters, as noted by security company **Symantec in their annual security threat report**.

Identity theft occurs when a criminal gains access to personal information to steal money or other benefits, such as access to tax refunds. Using false, or falsely obtained, **documents for identity** theft is not a new crime, and the **authentication** and protection of these documents is a long-standing problem. With the rapid growth of online services, digital exchanges and payments via the Internet have broadened the types of identifiers that can be used for impersonation and fraud. Accordingly, the needs of individuals, organizations and banks have changed and continue to evolve; security and convenience are essential for individuals when making **payment transactions**.

In recent history, the situation has been exacerbated by the all-conquering rise of mobile devices; today, the vast majority of **online transactions** are now initiated on a smartphone or tablet. **Research last year by the US Federal Reserve** found that 71% of US mobile phones are Smartphones and that over half of these use their phones to access banking services. In the EU, **KPMG** found that around 38% of those with a bank account use **mobile online services** to access it. In addition, eGovernment initiatives around the world (**spurred on by the UN eGovernment program**) – are driving citizens to access services from voting to tax returns online. And this is increasingly via a mobile device, which implies on-the-go, small screen, wireless connectivity and a host of other less than secure environmental conditions. Symantec state that data breaches in the financial sector alone accounted for 23% of all identities exposed by hackers. Security experts believe **identity theft** to be an even greater threat in the mobile world, as the constraints of the form-factor and continuous handset connectivity makes them more vulnerable to abuse.

How then, to stay secure in our mobile, connected, digital world?

Building Trust In The Digital Economy

In the digital world, trust is rooted in knowing precisely with whom or what you are interacting; **strong authentication** functions facilitate this by proving that the user – whether an individual, entity or object – is in fact who or what they claim to be. In order for **digital exchanges** and the digital economy to thrive, there must be trust between the players involved, namely individuals, organizations, as well as the hardware and software that connect them.

In other words, at what point is there sufficient evidence that the user's identity is really who they claim to be, enabling the transaction to proceed? While the CNAP Fact Sheet clearly refers to '**multi-factor authentication**', the US government's CIO has spoken specifically about two-factor authentication. This technique verifies user identity by means of combining two different components. These components may be something the user knows, something the user possesses or something inseparable from the user. An everyday example of two-factor authentication is the ATM; only the correct combination of a bankcard (something the user possesses) and PIN (personal identification number, something the user knows) enables cash to be withdrawn.

Two-factor authentication services have been extended to include verification by mobile phone. Several popular email and cloud storage providers now use this type of verification as standard. However there are still weaknesses with this system and the first is the humans involved: we simply aren't very good at creating or remembering passwords, even with the help of password management software. During the recent 'Star Wars' film hype, research found that 'starwars' became a worldwide popular password – but far more worryingly, '123456' and 'password' remain the two most used passwords. This reflects the constant battle going on in our lives between security and convenience.

The fundamental point is that the password is no longer the best way to authenticate users.

This raises two questions: Why do we still rely on the archaic alphanumeric password for authentication and what other method(s) could render it finally obsolete? This series examines those questions in the following two articles, **Look! No PIN! (2/3)** and **The Mobile-powered Planet (3/3)**.