CommsWire

Essential daily reading for the communications industry executive

An iTWire publication www.itwire.com Editor: Stan Beer Thursday 13 September 2018

FUTURE OF MOBILE AUTHENTICATION UNVEILED

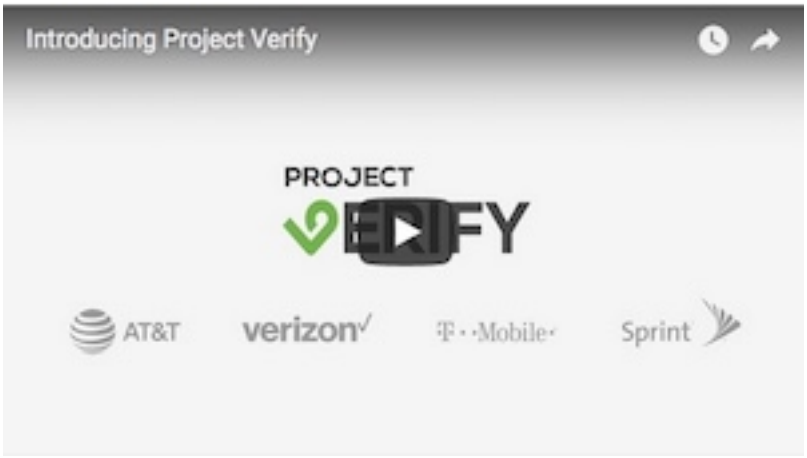
CommsWire (ISSN 2202-4549) is published by iTWire Pty Ltd. 907/151 City Rd, Southbank, Vic, 3006
CommsWire/Telecommunications Editor: Stan Beer
Staff writers: Peter Dinham, Alex Zaharov-Reutt, Sam Varghese. Columnist: John de Ridder
Advertising: Director of Digital Media, Andrew Matler: andrew.matler@itwire.com • Tel: 0412 390 000

FOUR BIG US CARRIERS UNVEIL MOBILE AUTHENTICATION PROJECT

US mobile carriers AT&T, Sprint, T-Mobile, and Verizon have announced they are setting up a Mobile Authentication Taskforce that will implement an initiative named Project Verify which will, according to them, be the future of mobile authentication.

The initiative, announced at the **Mobile World Congress Americas** which is taking place from 12 to 14 September in Los Angeles, aims to use a phone number, IP address, account tenure, phone account type and SIM card details for multifactor authentication.

The information will be loaded into a Verify app, which will log the user into other apps or online websites without the need for entering authentication details. The app will also be able to handle second-factor authentication.



The device-based ID will serve as an user profile during the authentication process.

A site devoted to Project Verify says the four carriers together serve 98% of the American mobile user population, adding that the Taskforce "will also work with service-oriented businesses that require high levels of user authentication and verification, to develop the technology and its applications".

The platform will share consumer data with other companies only with their consent, according to the site.

Plugging the project, the site says: "Despite the rise of online fraud and data breaches, consumers and businesses still rely on easily-forgotten and weak usernames and passwords.

"It's time for a comprehensive solution that reduces friction, combats fraud, and builds trust."

"This initiative expands upon our global operator initiative, Mobile Connect, to bring standardised authentication and identity services to the US market," said Alex Sinclair, chief technology officer, GSMA, in a statement.

"The solution aims to deliver a seamless experience for service providers from many sectors, helping to drive rapid adoption and scale."

Sam Varghese

AUSTRALIA, WORLD HIT BY SHARP RISE IN MOBILE FRAUD ATTACKS

Fraud attacks on mobile transactions in Australia have increased 26% this year compared to 2017, with a new report also revealing that attacks have risen sharply globally.

According to the **report** from security firm ThreatMetrix - a LexisNexis Risk Solutions Company - mobile fraud has reached 150 million global attacks in first half of 2018 with attack rates rising 26% year-over-year in Australia alone.

The report also reveals that Asia Pacific countries including Australia, Japan and Singapore featured in the top five target destinations among countries perpetrating the highest number of attacks globally - UK, US, China and Canada.

Other key findings of the ThreatMetrrix report for the Australia-New Zealand region, and globally, include:

- Growth in attack rate for financial services transactions coming from ANZ in Q2 2018 higher than any other region at 138%, compared to last quarter
- Bots are booming: 1H 2018 registered a total of 2.6 billion bot attacks, with a 60% step up from Q1 to Q2 2018.
- Bot attack rate from ANZ grew 33% in comparison to last quarter, indicating a ramping up of cybercrime activity in the region, coinciding with the advent of the New Payments Platform (NPP)
- Globally, 58% of digital transactions now originate from mobile devices
- Globally, mobile attacks are increasing, with one third of all fraud now targeting this channel
- 85% of transactions on social networks and dating sites now come from mobile devices, where identity spoofing is rife

And in the last three years the proportion of mobile transactions versus desktop has globally almost tripled, with one third of all fraud attacks now targeting mobile transactions.

ThreatMetrix says the fraud attacks on mobile devices have risen as consumer behaviour increasingly embraces mobile for virtually all online goods and services, with fraudsters starting to close the gap on this channel.

Globally, one third of all fraud attacks are now targeting mobile transactions. This means that although digital companies do need to prepare for increasing attacks, mobile remains the more secure channel compared to desktop.

“This means that although digital companies do need to prepare for increasing attacks, mobile remains the more secure channel compared to desktop,” the report says.

The security firm says the rise of mobile is undisputedly the key change agent in digital commerce currently.

In the last three years the proportion of mobile transactions versus desktop has almost tripled – with mobile transactions, which include account creations, logins and payments, reaching 58% of all traffic by the middle of 2018.

The report also reveals that mobile fraud rates have tended to lag behind the channel’s overall growth, however in the first half of 2018 mobile attack rates rose 24%, when compared to the first half of 2017.

According to ThreatMetrix, mobile offers organisations unique opportunities for accurately assessing user identity, thanks to highly personalised device attributes, geo-location and behavioural analysis.

“It offers strong customer authentication options that require no user intervention, including cryptographically binding devices for persistent authentication (“Strong ID”),” ThreatMetrix notes.

“The number of Strong IDs for mobile devices on the ThreatMetrix network has more than doubled in the first half of 2018, improving both customer recognition rates and the efficacy of identifying trusted transactions.”

“Mobile is quickly becoming the predominant way people access online goods and services, and as a result organisations need to anticipate that the barrage of mobile attacks will only increase,” said Alisdair Faulkner, Chief Identity Officer at LexisNexis Risk Solutions.

“The good news is that as mobile usage continues to increase, so too does overall customer recognition rates, as mobile apps offer a wealth of techniques to authenticate returning customers with a very high degree of accuracy.

“The key point of vulnerability, however, is at the app registration and account creation stage.

“To verify users at this crucial point, organisations need to tap into global intelligence that assesses true digital identity, compiled from the multiple channels that their customers transact on.”

Peter Dinham

WHY IT WILL BE WORTH UPGRADING TO THE NEW IPHONE XR

COMMENT: I am not a moronic consumer who eagerly lines up to spend his hard earned money each time Apple makes a new product announcement. That said, one feature of the new iPhone XS and XR phones launched today has made me consider upgrading.

After more than three years, I am still happily using my iPhone 6, which has proven to be an excellent and reliable product.

I don't really care about having a better camera, more storage or a faster chip because my phone does everything I need it to – almost.

These days I am spending a lot of time overseas and this has been somewhat of an irritant when it comes to using my phone.

My provider Vodafone does offer a very reasonable $5 a day international roaming plan but this becomes prohibitively expensive for those of us who spend a good part of the year abroad.

My solution until now has been to swap SIMs when I'm abroad. Where I am currently I use a very good prepaid unlimited data plan for about $20 a month.

This however has the disadvantage of cutting off access to my Australian phone calls and SMS messages.

Consequently, if I want access to my home phone while using an overseas SIM I have had two choices.

I could carry two phones or move over to a dual-SIM Android device. I have never found an Android phone that I like and carrying two phones is a drag so for me neither solution is viable.

And this is exactly why the new IPhone XS and XR models have made me sit up and take notice.

Buried in among all the guff about the new chip, better camera, improved screen, increased storage and fabulously stylish design in today's announcement was the fact that for the first time Apple has introduced dual SIM to its phones through the use of the usual nano-SIM slot and an embedded digital eSIM chip.

An eSIM is an embedded chip in the phone that is software writable so in future users could switch mobile operators without changing a physical SIM.

For us overseas travellers, we could retain our Vodafone, Telstra or Optus nano-SIM and activate our eSIM with whatever mobile operator we choose to use abroad.

Or conceivably, our Australian operator might be housed on the eSIM and we could simply insert a cheap local physical SIM while overseas.

eSIM is new and requires mobile carrier cooperation but the good news for me is that my provider Vodafone is a strong supporter of this technology.

For those of you with Telstra and Optus, don't worry because there is no way they will risk losing iPhone customers by not jumping aboard. Although one wonders why they have still not implemented visual voicemail.

As far as my choice of new phone is concerned, it will almost certainly be the iPhone XR 128GB model for $1299, which is just about at the limit I'm prepared to spend for any type of mobile handheld device.

Yes it's still pricey but I know it will last me at least three years – and who knows, I'm might even be able to trade-in (or sell) my iPhone 6.

So will I be lining up for the new iPhone XR when the Apple Store throws open its doors on 26 October?

No, but I will certainly go down to a store after the din has died down and take a look at one. If I like what I see, then I will seriously consider ugrading.

Stan Beer

LABOR UNWILLING TO COMMIT EITHER WAY ON ENCRYPTION BILL

The Labor Opposition appears hesitant about ruling out support for the Government's Assistance and Access Bill, a draft of which was put up for comment on 14 August.

Labor Shadow Attorney-General Mark Dreyfus (below) said in response to queries from ***CommsWire***: "Labor is carefully considering **the exposure draft** of the Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018 that was released by the Turnbull Government in early August.

"Labor is determined to ensure that our law enforcement agencies and national security agencies have the powers that are necessary to keep Australians safe."

The last date for public comment on the bill was Monday (10 September).

The Australian Greens have **strongly opposed the bill**, with the party's Digital Rights spokesperson Senator Jordon Steele-John saying cyber security would be "significantly diminished by undermining the fundamental principles of end-to-end encryption – which is exactly what this legislation proposes".

A number of groups have **spoken out** about the legislation, pointing out that adopting it would be a mistake.

Dreyfus said: "As well as defending our nation's security, Labor also strongly believes in the importance of upholding the rule of law and the rights and freedoms that define us as a democratic nation."

As per the draft bill, telecommunications and Internet companies and makers of digital devices will **face fines** of up to $10 million if they do not help law enforcement agencies gain access to data needed for investigating terrorism offences.

The government has also left open the door **to crack encrypted messages**.

"We, in Labor, understand that in passing laws designed to protect the Australian community it is essential that we always work to uphold the rights and freedoms that our nation has proudly defended since Federation," Dreyfus added.

"It is with this in approach in mind that Labor is committed to engaging in a constructive manner with the government on the Telecommunications Legislation Amendment (Assistance and Access) Bill 2018."

Sam Varghese

MICROSOFT'S 'GERMANY-ONLY' CLOUD SERVICE BEING WOUND UP

Microsoft's provision of cloud services in Germany through T-Systems, a subsidiary of Deutsche Telekom, appears to be over, with the software firm announcing it would now deliver cloud services from new data centres in Germany.

The stopping of this service could have been prompted by the massive losses that the service incurred, with one German publication, Handelsblatt, **reporting back in March** that the Windows manufacturer has been set back by more than €100 million (A$162 million).

Microsoft said in **its blog post** that the reason for winding up the Deutsche Telekom service was because "customers' needs have shifted, and the isolation of Microsoft Cloud Germany imposes limits on its ability to address the flexibility and consistency customers desire."

The **setting up** of the Deutsche Telekom deal was prompted by data security fears; at the time, in the wake of the revelations about blanket NSA surveillance by whistleblower Edward Snowden, many American firms had looked to set up European operations to provide cloud services in order to satisfy the privacy demands of likely European customers.

The issue of privacy was highlighted by **a case** between Microsoft and the US Department of Justice - Microsoft refusied to hand over emails stored on one of its servers in Ireland.

The case ended when a new law, the CLOUD, signed into law by President Donald Trump on 23 March, **made the case moot**. The Act changed US law so that law-enforcement warrants would henceforth apply to data stored anywhere by US-based tech firms.

This meant that the one feature sought by foreign companies — not to have their data at the beck and call of the American Government — would no longer be available if they chose to use the cloud services of a US firm.

When Microsoft announced the deal with Deutsche Telekom, it was organised in such a way that Microsoft itself would have no access to the data unless permitted to do so by the data trustee. That trustee was Deutsche Telekom subsidiary T-Systems.

File sync and share company Nextcloud **said** a major reason why Microsoft had lost money on this service was due to poor security. Quoting Handelsblatt, Nextcloud said the Telekom cloud solution was "over-priced, under-performing and unpopular with customers."

Plus, Handelsblatt said, "extra security turned out to be a real hindrance to doing business. Companies who wanted to establish secure information links to Asian subsidiaries or overseas databases were hit with delays and crashes. Servers went down regularly, system updates were often impossible."

Nextcloud has a dog in this fight as it provided cloud services to the German Government.

Comment has been sought from Microsoft.

Sam Varghese