PwC Weekly Security Report

This is a weekly digest of security news and events from around the world. Excerpts from news items are presented and web links are provided for further information.

Bank hack

Tesco Bank says £2.5m was stolen from 9,000 customers in cyberattack

E-commerce hack

Hyderabad: Hackers beat e-tender plan

NIST and MFA

Understanding NIST regulations and MFA

Top stories

Ultrasound: The new hacking tool

Payment channels security systems under scrutiny over hacking fears

pwc

Tesco Bank says £2.5m was stolen from 9,000 customers in cyberattack

A total of £2.5 million was stolen from 9,000 Tesco Bank customers in a sophisticated cyberattack last weekend, the bank has confirmed.

The bank has also said that all account services have now returned to normal after all online transactions for all of its 136,000 current account holders were frozen following what the bank called "online criminal activity" spotted over the weekend.

Tesco Bank blamed the incident on a "systematic, sophisticated cyberattack" but said personal data was not compromised as a result of the fraud.

"Our first priority throughout this incident has been protecting and looking after our customers and we'd again like to apologise for the worry and inconvenience this issue has caused," said Tesco Bank CEO Benny Higgins.

The bank says it has finished refunding all current account customers who were victims of fraudulent online activity, with the cost of reimbursing 9,000 customers estimated to come to a total of £2.5 million.

Tesco Bank isn't going into details about how the cyberattack occurred, but confirmed it is continuing to work closely with the authorities and regulators in their criminal investigation of this incident.

The National Crime Agency, the Information Commissioner's Office, and the National Cyber Security Centre (NCSC) -- a newly launched arm of intelligence agency GCHQ -- are all investigating the attack.

"In the case of cyber related incidents, it can, on certain occasions, take a significant period of time to understand the incident given the technical complexities involved. So the story will emerge over time," said the NCSC.

Andrew Tyrie MP, chairman of the House of Commons Treasury Select Committee, says the Tesco Bank incident represents "just the latest in a long list of failures and breaches of banking IT systems, exposing many thousands of customers to uncertainty and disruption".

Tyrie will also be writing to Tesco Bank CEO Higgins to ask what actions are being taken to reduce the likelihood of a similar attack happening again. "We can't carry on like this," he said.

In total, Tesco Bank has seven million customers who use it for services including mortages, ISAs, and insurance. The bank launched its current account banking service in 2014.

Source:
http://www.zdnet.com/article/tesco-bank-says-2-5m-was-stolen-from-9000-customers-in-cyber-attack

Our perspective

Organisations need to step up security to avoid such attacks; various tools and technologies need to be combined to further strengthen infrastructure and network security. The weakest link in the information life cycle still continues to be the people using the system. Only by increasing awareness about new and known exploits can we ensure that the controls being implemented are effective and working efficiently. Organisations are also advised to join information security forums where the latest emerging threats are discussed and ways to remediate them are shared.

Hyderabad: Hackers beat e-tender plan

The e-tendering system is not very transparent because contractors are taking the help of hackers to hack into the corporation's account and find out who the lowest bidder is.

For instance, when a road tender is called through online system, the lowest bidder should get through as per the rule. The contractors, to check the lowest bid, peep into the system, usually a day before the tender deadline, and quote even less in their tender.

It is alleged that hackers charge Rs 15,000 for each tender hack. The E-tender Manage-ment is a software introduced by the Telangana government to help reduce the cycle time, unnecessary paper work, waiting in long queues and to maintain transparency while allocating contracts.

Mr Umesh Thota, CEO of Authbase, a cyber security company, said, "If a corporation's account is hacked, it means that the survey is very vulnerable. There are two types of surveys, security by design and security by obscurity. It depends entirely on what survey the government agency was operating under and whether they have been able to update it to the latest e-commerce security system. If not, the survey is very vulnerable. Unless the systems are secured by design concept, one will always be able to exploit the tenders."

Hackers never advertise, but work through recommendation. However, hacking government accounts is not possible in project tenders that run into crores like the Strategic Road Development Plan of GHMC, because the government agency outsources the job to a cyber security private firm. These multi-crore projects first have a pre–bid tender step, wherein the contractor's payments, performance and quality of work are evaluated. Unless the contractor qualifies the pre-bid step, he cannot submit the technical tender. The second step includes technical bid and those who qualify are eligible for the commercial bid, which decides the lowest bidder. The contractors will have to pass through these procedures to get the project.

Hacking is being done for lower cost projects. An officer of the cyber security cell said, "Hacking of tenders is possible but an alteration of prices cannot be done for contractors who have already submitted their bids due to the digital signatures. Thus most contractors submit bids in the last minute. But tenders of government agencies that have been outsourced to private firms are relatively safe since they check on the event log which records details of IDs hacking the account, documents opened, and there is also a check on internal employees."

Source:
http://www.deccanchronicle.com/nation/current-affairs/161116/hackers-beat-e-tender-plan.html

Understanding NIST regulations and MFA

The National Institute of Standards and Technology (NIST) recently updated its guidelines on two-factor authentication, including a statement that out-of-band verification methods using PSTN, SMS, or voice calls are deprecated. What does this mean, and why is it important? Most importantly, how can organizations implement multi-factor authentication (MFA) that complies with the NIST regulations?

In two-factor authentication, users are required to present something they know (such as a password) and something they have (such as a one-time-password or a card). It's best to establish the secondary authentication method through a separate communication channel; i.e., out-of-band (OOB). In order to hack an account, an attacker must compromise the password and the device/channel used for secondary authentication, which is more difficult than obtaining a single password.

The latest draft of NIST Special Publication 800-63B Digital Authentication Guideline addresses the use of the PSTN as an OOB authentication verifier:

"Due to the risk that SMS messages or voice calls may be intercepted or redirected, implementers of new systems SHOULD carefully consider alternative authenticators. If the OOB verification is to be made using the PSTN, the verifier SHALL verify that the pre-registered telephone number being used is not associated with a VoIP (or other software-based) service. It then sends the SMS or voice message to the pre-registered telephone number. Changing the pre-registered telephone number SHALL NOT be possible without two-factor authentication at the time of the change. Note: OOB authentication using the PSTN (SMS or voice) is deprecated, and is being considered for removal in future editions of this guideline."

NIST explains that SMS interoperability means that messages sent to a phone number are not necessarily sent to a mobile phone—they can be received via an SMS, Multimedia Messaging Service (MMS), or iMessage.

Understanding NIST regulations and MFA

As a result, the NIST advises federal agencies to verify that phone numbers are indeed connected to a mobile device. However, even those connected to a mobile device present a risk, since attackers are increasingly redirecting and/or intercepting SMS messages and voice calls.

While OOB authentication using the PSTN is stronger than using a single password, it is still not the best option, and the NIST says federal agencies should consider moving to a more secure alternative in the future.

Authentication alternatives to the PSTN

What are the alternatives? One option is the use of derived credentials, which leverage the cryptographic credentials associated with smart cards but eliminate the need for a physical card or to install a dedicated reader. With derived credentials, the cryptographic credential is stored securely on a mobile device in compliance with smart card regulations, meaning the mobile device has secure access to apps, websites, and services that require smart card authentication.

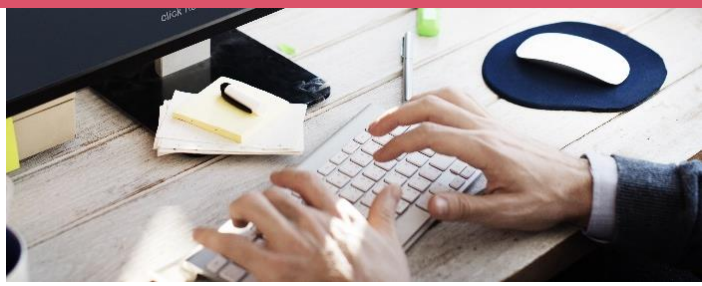
A second alternative: Leverage a trusted execution environment to securely store authentication credentials, such as private cryptographic keys and biometric data. A trusted execution environment integrated with a MFA solution can provide context-based authentication and convenience for users.

Source:
http://www.cio.com/article/3141648/security/understanding-nist-regulations-and-mfa.html

Our perspective

The NIST Cybersecurity Framework consists of standards, guidelines and practices to promote the protection of critical infrastructure. With the new guideline (800-63B), NIST tried to enhance the MFA process by introducing PSTN as an OOB authentication verifier which will add another layer of security during authentication. However, NIST has also indicated that OOB verification methods using PSTN, SMS or voice calls shall be deprecated.

Ultrasound: The new hacking tool



Ultrasound apps are still niche, but it could be an attractive technology for use in the internet of things. The apps can collect information about users without them knowing.

Sometimes it feels as if they are watching you. You idly check out some clothes online one morning, and for the rest of the week, they follow you across the internet, appearing in adverts on every website you visit.

That can be spooky enough, but what if those ads could pop out of your browser and hound you across other devices? This is the potential of ultrasound technology, says Vasilios Mavroudis at University College London – and it offers a new way in for hacking attacks and privacy invasions. He and his colleagues spelled out their concerns at this week's Black Hat cybersecurity conference in London.

So far, this kind of ultrasound technology has mainly been used as a way for companies to identify and track the people who have seen their ads, like a cross-device cookie. High frequency audio "beacons" are embedded into TV commercials or browser ads. These sounds, which are inaudible to the human ear, can be picked up by apps on any nearby device that has a microphone. But the technology has many more applications. Some shopping reward apps, such as Shopkick, already use it to let retailers push department or aisle-specific ads and promotions to customers' phones as they shop.

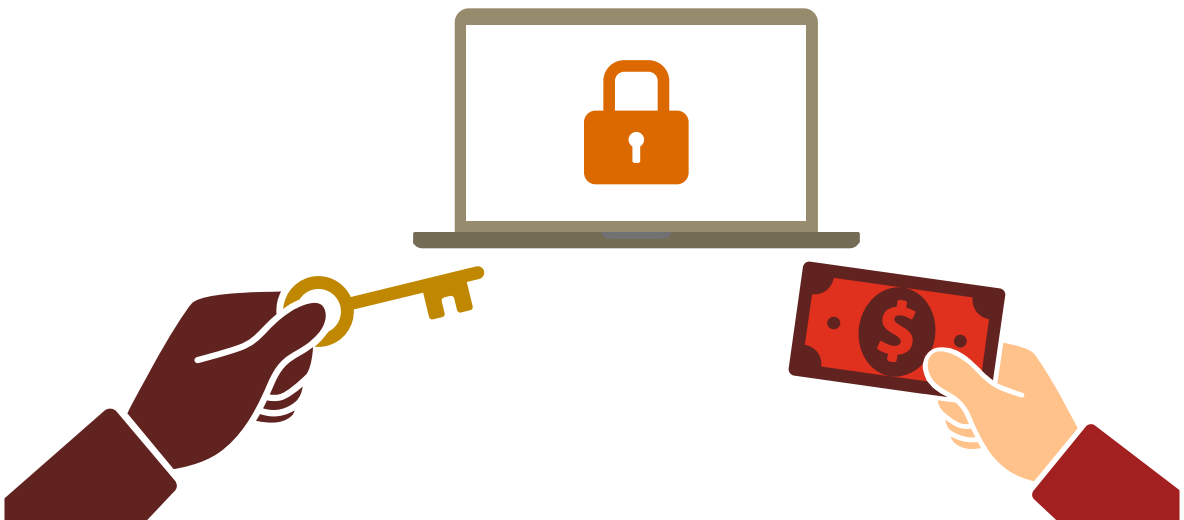
"It doesn't require any special technology," Mavroudis says. "If you're a supermarket, all you need are regular speakers."

But there is a privacy risk. In March, the US Federal Trade Commission rapped the knuckles of 12 app developers who used ultrasound for cross-device tracking – even when the apps weren't turned on. This meant that the apps could collect information about users without them knowing.

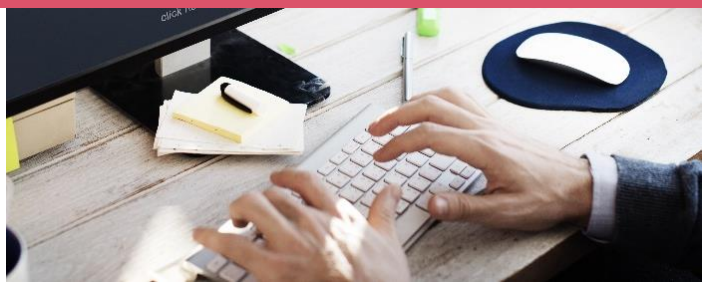
The software developer providing the ultrasound code quickly withdrew it, but Mavroudis and his colleagues identify other problems with ultrasound-based technologies.

One worry is that these programs may not just be picking up ultrasound. "Any app that wants to use ultrasound needs access to the full range of the microphone," says Mavroudis. That means it would be possible, in theory, for the app to spy on your conversation.

The ultrasonic audio beacons that these apps pick up can also be spoofed. This means that hackers could create fake beacons to send unwanted or malicious messages to your device, like malware. Mavroudis and his team realised that this would be possible when they found evidence of people trying to cheat prizes out of a shopping rewards app by playing it recordings downloaded from the internet. "That was when we realised how easy it would be to spoof these," he says.



Ultrasound: The new hacking tool



Ultrasound apps are still niche, but it could be an attractive technology for use in the internet of things, says Mu , a computer scientist at the University of Northampton, UK. Ultrasound is a good candidate for pairing devices that have a speaker and microphone. For example, Google's Chromecast app uses it to pair your mobile phone with its streaming dongle.

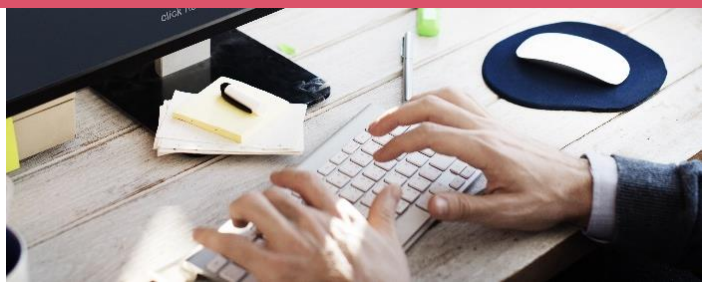
This creates a new channel for hacking attacks against these devices. Ultrasound can't carry a lot of data, says Mu. "But if you know what you're doing, just by sending a few bytes, you can hack a system and instruct it to do a lot of things. It doesn't always take a lot of data to make something bad happen."

Before ultrasound goes mainstream, Mavroudis says, we must work out how to regulate it and keep it from being hijacked for malicious purposes. "Ultrasound beacons don't have specs yet," he says. "There are no rules about how to build or connect ultrasound beacons. This is kind of a grey area where no one wants to take responsibility." He and his colleagues are agitating for standards similar to those that exist for Bluetooth. They have also developed countermeasures you can use in the meantime, including an ultrasound-filtering browser extension for Google Chrome that blocks any beacons embedded on a website from sounding. "It's going to get worse unless we fix it," says Mavroudis. SALLY ADEE/(C) 2016/ DISTRIBUTED BY TRIBUNE CONTENT AGENCY, LLC

Source:

http://mumbaimirror.indiatimes.com/others/sci-tech/Ultrasound-The-new-hacking-tool/articleshow/55382458.cms

Payment channels security systems under scrutiny over hacking fears



Mindful of the threat posed by the biggest-ever cyber security breach that hit 32 lakh debit cards recently, the Centre has decided to set up a committee to look into the overall security systems at payment channels to protect banks from future cyber attacks.

The committee would consist of representatives from Indian Computer Emergency Response Team (CERT-In), the National Payments Corporation of India (NPCI), banks and department of information technology, among others. “They have to see where security breach could happen,” an official told FE.

While the last incident occurred at the payment switches of two banks, the committee would look into whether the banking system is foolproof and suggest steps that can be taken to secure data, the official said.

A top cyber security official from the department of information technology would head the panel.

The government’s top cyber security arm, CERT-In, an arm of the department of information technology, would play a key role in this. In 2015, CERT-In handled 49,455 incidents, including website intrusion and malware propagation, malicious code, phishing, distributed denial of service attacks, website defacements and unauthorised scanning activities.

The government move is aimed at further ramping up cyber security. This is in addition to an ongoing forensic investigation by US-based Payment Card Industry Data Security Standard (PCI DSS) into the latest debit card fraud in India. PCI DSS is expected to submit its report shortly to Indian authorities. After examining the findings of the report, Indian banks would be asked to take corrective measures.

NPCI has estimated that Rs 1.3 crore had been lost by Indian customers in the debit card fraud, prompting banks to replace lakhs of debit cards or change ATM PIN.

Data across cards are believed to have been stolen from the ATM of an Indian private sector bank that is serviced by Hitachi Payment Services. Of the debit cards affected, 26.5 lakh are on Visa and Mastercard platforms, while six lakh are on RuPay. A public sector bank was also using the Hitachi Payment Services in a limited way. The corrective actions by banks could include replacing the particular payment switches that are at the centre of the security breach.

Source:

http://www.financialexpress.com/economy/payment-channels-security-systems-under-scrutiny-over-hacking-fears/445932

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 157 countries with more than 2,23,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

In India, PwC has offices in these cities: Ahmedabad, Bengaluru, Chennai, Delhi NCR, Hyderabad, Kolkata, Mumbai and Pune. For more information about PwC India's service offerings, visit www.pwc.com/in

PwC refers to the PwC International network and/or one or more of its member firms, each of which is a separate, independent and distinct legal entity. Please see www.pwc.com/structure for further details.

For any queries, please contact:

Sivarama Krishnan
sivarama.krishnan@in.pwc.com

Amol Bhat
amol.bhat@in.pwc.com

MB/November2016-8105