Sarbanes Oxley Compliance Professionals Association (SOXCPA)
1200 G Street NW Suite 800 Washington, DC 20005-6705 USA
Tel: 202-449-9750 Web: www.sarbanes-oxley-association.com

Sarbanes Oxley News, November 2017

Dear Member,

Today we will start with the presentation of Jerome H Powell, Member of the Board of Governors of the Federal Reserve System, at the 41st Annual Central Banking Seminar, sponsored by the Federal Reserve Bank of New York, New York City.

Financial innovation - a world in transition

We live in a world defined by the rapid pace of technological change.

Four of the five largest U.S. companies by market capitalization are classified as "technology companies," where the term describes the products that these companies sell and how they operate.

Thanks to decades of investment in information technology, especially in electronic communication networks, consumers now expect services to be available instantly at their fingertips.

This statement is true for almost every industry and every aspect of daily life, including financial transactions.

This evening, I will consider how technology is changing the delivery of retail banking and payments services. I will discuss the roles of banks,

fintech companies, and other stakeholders in moving the United States forward to a better payment system.

I will also review the Federal Reserve's collaboration with these payment system stakeholders in pursuing that goal.

I will argue that, for policymakers as well as the private sector, the challenge is to embrace technology as a means of improving convenience and speed in the delivery of financial services, while also assuring the security and privacy necessary to sustain the public's trust.

As always, the views I express here are my own.

Retail Banking Innovation

As with so many sectors of the economy, technology is transforming the retail banking sector. The banking industry has traditionally been characterized by physical branches, privileged access to financial data, and distinct expertise in analyzing such data.

But in today's world companies need not be bound by physical infrastructure and related overhead expenses. For example, companies can take advantage of an explosion in available data, and leverage advances in computing power, via cloud computing, analytical tools, and off-the-shelf machine learning tools, to make sense of those data.

The banking industry is adjusting to this world, and facing significant challenges to traditional banking business models.

For example, today financial technology can support access to credit through innovative approaches to gathering and analyzing data. Historically, a customer seeking a loan has provided financial statements to a bank or other traditional lending institution.

More recently, the use of a fintech platform may allow a lender to quickly monitor and analyze more up-to-date data from a broader range of sources, including those outside of the traditional lending process, to verify an applicant's identity and make inferences about the applicant's overall financial health.

For example, a business loan applicant could submit information such as shipping data or customer reviews as additional input to more traditional data sources.

With this additional information, the bank would have a more complete picture of an applicant's day-to-day activity and overall financial capacity, and potentially a greater ability to provide credit to customers, including some who might have been otherwise denied a loan based on traditional data.

Fintech firms are also finding ways to use banks' data, in some cases without entering into an explicit partnership with the bank.

With customers' permission, fintech firms have increasingly turned to data aggregators to "screen scrape" information from financial accounts.
In such cases, data aggregators collect and store online banking logins and passwords provided by the bank's customers and use them to log directly into the customer's banking account.

This information can be used to provide consumers with convenient real-time snapshots of their financial information across multiple banks and accounts.

These examples highlight that there is a balance that needs to be achieved in this innovative environment.

On the one hand, new technologies have enabled banks and other firms to find different ways of meeting consumers' demand for speed and convenience. On the other hand, these same technologies raise new considerations about data security and safety, as well as consumer privacy and protection.

Policymakers and the financial industry must assure that enhanced convenience and speed in financial services do not undermine the safety, security, and reliability of those services.

Retail Payments Innovation

Technology is also shaping changes in retail payments. As with retail banking, retail payments will need to evolve to meet consumer expectations of constant connectivity and instant access while assuring security and privacy.

It is not news that consumers' lives, including the way they pay, are now intertwined with mobile phone usage. While the overall amount of time we spend on our phones continues to grow, the duration of individual phone sessions is actually shrinking.

In late 2015, Google estimated that the average mobile session lasts only 70 seconds, and may be repeated dozens of times per day.

As a result, payment innovators have had to create new ways to move money that are not only fast and mobile-focused, but also sufficiently "frictionless" that consumers can now fit commerce into these brief interludes.

This development has ushered in a world of multiple smartphone apps that allow for "instant" payments. We can use a payments app to move funds instantly to anyone who has that app.

Some banks have similarly collaborated to build faster payments applications that leverage their deposit account systems. And we are already moving to a world in which we need not open a special app or go to our bank's website in order to send money.

Many people here will have taken an Uber or Lyft, and then paid your driver without relaunching the app, much less reaching for your wallet. Similarly, payment providers can now leverage the application programming interfaces (APIs)-essentially the protocols-of smartphone messaging services to integrate their payment tools directly into messaging applications: Nowadays, consumers can simply "attach" money while messaging a friend.

Innovation in retail payments can also offer tangible benefits to consumers beyond convenience. Improvements in security, such as our ability to authenticate consumers and detect fraudulent transactions, are also possible through innovation.

For instance, mobile payments introduce a wide array of ways to authenticate a consumer's identity, including two-factor authentication codes sent via text message to the phone; biometrics, like a fingerprint or face scan; device identification information; IP address; and geolocation data. Similarly, increased access to transaction data and cloud computing resources means that we have smarter, faster computational processes-like enhanced neural networks-to detect payments that do not match a consumer's spending patterns and help prevent fraudulent transactions.

Both security and convenience are crucial elements for successful payments innovation.

Consumers will not store their funds in a system that is not secure and will not want to transfer funds out of an otherwise secure system if the process is cumbersome.

The Role of Banks in Payments Innovation

The examples I have highlighted so far illustrate payments innovations from fintech firms and banks alike.

I want to spend a moment highlighting the special role of banks in the payments process, and how banks are needed in order to create innovations that can be used broadly across the economy.

The traditional role of banks in the payments process has been to hold deposits and enable their transfer from one individual or business to another. A depositor might withdraw cash from the bank's ATM to pay a friend or write a check to make a payment.

Over time, we have moved from ATMs and paper checks toward electronic payments and online payments through banking platforms-payment methods for which banks are still perceived as essential.

More recently, consumer-facing technology has become front and center. At times, the payments process is so seamlessly integrated that one can forget that there is even a bank in the process, as with the Uber and Lyft example.

But despite this shift in focus, payments innovation is still fundamentally about how, when, and where an individual's deposits can be held, transferred, and packaged with other information.

And banks are still important players in making that happen. Even where this reality is obscured by several layers of technology, there is almost always a bank involved in consumer transactions.

Given their importance in holding and transferring funds, banks continue to have a key role to play in the design and safety of more efficient retail payment systems. Without bank participation, it would be difficult to change how funds are transferred in a way that brings pervasive benefits to consumers.

For example, if the aim is to capture the speed and continuous nature of today's commerce in the payment system as a whole-as has become a focus

for many countries, including the United States-it would be difficult to do so without banks allowing the transfer of their deposits on a 24x7 real-time basis.

Of course, individual payment systems are already doing this for consumers within their own network. But achieving these benefits on a broad scale would be challenging without the banking system's participation, because of the large role banks have in holding and transferring funds.

All this is to say that we are at a critical juncture in the payment system's evolution, where technology is rapidly changing many facets of the payments process. Fintech firms and banks are seizing these technological changes in their own ways. But a collective and collaborative effort by all payment stakeholders will also be important as the United States works to achieve a payment system that has broad reach and can seamlessly integrate with other systems to transfer funds in a reliable, secure, and convenient manner.

When we pay with cash or write a check, we don't spend a lot of time worrying about who our recipient banks with; that universality seems an appropriate standard for new payment options as well.

Strategies for Improving the U.S. Payment System

At the Federal Reserve, we believe it is important to embrace opportunities provided by technological change to improve the convenience and safety of the U.S. payment system.

About five years ago, we launched our payment system improvement initiative, which committed the Federal Reserve to working with the full range of payments system stakeholders to achieve a faster, more secure payment system. We saw that technology was transforming the nature of commerce and end-user expectations for payment services.

We saw some players coming to market with innovative product offerings, but it was a fragmented approach. Meanwhile, other countries were advancing on initiatives to improve the speed and safety of their payment systems, creating a gap between the U.S. payment system and those abroad.

While the Federal Reserve does not have plenary authority over payment systems, as is the case in some other countries, we have often played an important role as a leader and catalyst for change.

It was in this role that we issued a call to action asking stakeholders to come together in pursuit of a better payment system for the future-focusing on speed, security, efficiency, international payments, and collaboration.

I believe a collaborative approach ensures that change is designed by those whose commitment and expertise are needed to improve the payment system.

Stakeholders - including banks, fintech companies, consumer groups, regulators, and others - answered our call to action, signing up for two task forces convened by the Federal Reserve.

More than 300 stakeholders joined the Faster Payments Task Force, and around 200 joined the Secure Payments Task Force. Let me first touch upon the Faster Payments Task Force, which has recently completed its work.

The Faster Payments Task Force's mission was to identify and assess alternative approaches for implementing a safe, ubiquitous, faster payments system in the United States.

The task force began its work by developing a set of effectiveness criteria laying out desirable attributes for faster payment solutions covering the broad categories of ubiquity, efficiency, safety and security, speed, legal framework, and governance.

While the task force was focused on improving speed and convenience, it also underscored the importance of safety and security by establishing 11 criteria of a total of 36 focused on those objectives.

The task force encouraged its members to submit proposals for faster payment solutions that would meet the criteria that its members had agreed upon. A diverse range of task force members rose to the challenge by submitting 16 proposals to be vetted against its criteria.

These proposals represent a broad universe of creative and innovative ways to deliver faster payments by embracing technology. They range in structure from solutions that use a centralized clearing and settlement mechanism to others that focus on distributed networks. Some are based

on traditional assets held in transaction accounts, and others depend on new asset forms like digital currencies.

The role of the task force process was not to recommend or implement a faster payment solution, but rather to offer a range of ideas to move the United States further along the path to a better payment system. We believe that the task force has successfully carried out this role.

We are very grateful to the members of the Faster Payment Task Force for all of their work and for the collaborative spirit they brought to the job. But there is more to be done to advance our collective vision of a ubiquitous, real-time, secure future payment system.

Last month, the Federal Reserve reaffirmed its commitment to that vision in the paper, "Federal Reserve Next Steps in the Payments Improvement Journey," which outlines refreshed strategies and tactics that we, in collaboration with the payment industry, will employ to make further progress.

I will mention just a few.

One of the recommendations from the Faster Payments Task Force work was to establish an industry governance framework for collaboration and decision-making on faster payments.

To move forward in creating this framework, the task force established the Governance Framework Formation Team to develop, publish, and solicit public comment on a proposal for a governance framework.

This work group will carry out many of the task force recommendations and the Federal Reserve, at the request of the task force, is chairing and facilitating this effort.

In addition, the Federal Reserve is considering providing settlement services-a traditional core function of a central bank-to address the future needs of a ubiquitous real-time retail payments environment.

We plan to actively engage with the industry and other stakeholders to further understand gaps and requirements for real-time retail payments settlement and assess alternative models that will support needs over the long term.

We also plan to explore and assess the need, if any, for other related Federal Reserve services or capabilities. In carrying out this assessment, we will be guided by current and potential market developments and challenges, as well as our long-established criteria for offering new products and services.

These criteria include the need to fully recover costs over the long term; the expectation that the new service will yield clear public benefit; and the expectation that other providers alone cannot be expected to provide the service with a reasonable effectiveness, scope, and equity.

The Federal Reserve will also continue to support the ongoing work of the Secure Payments Task Force.

This task force has been working to educate stakeholders on payment security practices, risks, and actions that could enhance payment security.

These are challenging topics, because they require stakeholders to be open and forthcoming about potential vulnerabilities if there is to be substantial progress.

The Federal Reserve will also pursue two new efforts focused on security. Early in 2018, we plan to launch a study analyzing payment security vulnerabilities. This study is similar to other research efforts that the Federal Reserve has pursued to build foundational and collective understanding of the U.S. payment system.

We also plan to build upon the contributions of the Secure Payments Task Force to establish work groups focused on approaches for reducing the cost and prevalence of specific payment security vulnerabilities. In a world of ever-escalating threats to the integrity of our payment system, this collective action is needed to sustain public confidence.

These were just a few of our new initiatives. The package of next steps the Federal Reserve outlined in its recent paper confirm that we remain steadfast in our commitment to work with industry and other stakeholders to achieve a better payment system through both leadership and action.

Summary

Rapidly changing technology is providing a historic opportunity to transform our daily lives, including the way we pay.

Fintech firms and banks are embracing this change, as they strive to address consumer demands for more timely and convenient payments.

A range of innovative products that seamlessly integrate with other services is now available at our fingertips.

It is essential, however, that this innovation not come at the cost of a safe and secure payment system that retains the confidence of its end users.

The examples I have drawn upon today highlight that fintech firms and banks must each play a role in assuring that enhancements to convenience and speed do not undermine safety and security.

More broadly, the Faster and Secure Payments Task Forces demonstrate the importance of broad and diverse stakeholder input, which are essential if the United States is to implement safe, ubiquitous real-time retail payments.

Working together, we can achieve a safe and fast payments system that meets the evolving needs of consumers and our dynamic economy.

The Importance of Diversity and Inclusion to Fulfilling our Mission

PCAOB
Public Company Accounting Oversight Board

Welcome to the launch of the PCAOB Diversity and Inclusion program. This program means a lot to us – to our continued growth and success as an organization, to our mission to serve the public good, and to our involvement with different cultures around the building and around the world.

As we mark the PCAOB's 15 year anniversary next year, I'm reminded that everything good about the PCAOB comes from you, and our shared effort to do well and take pride in our work.

Our people make us who we are. Our Diversity & Inclusion program has an important role to play in reminding us of that, and how important it is to honor, respect and support all of our people.

A focus on D&I is vital to enrich our ability to attract, retain, and develop an exceptional workforce; and to encourage each other to draw upon our unique experiences, skills and knowledge in ways that enhance the PCAOB's ability to fulfill its mission.

I want to emphasize the importance of inclusive leadership at the PCAOB.

It means sharing information, breaking down silos, encouraging collaboration, and opening yourself up to trying new things. And it always means continually working to build more trust and more mutual reliance on each other.

It means encouraging and respecting diverse points of view. Creating a climate that supports honest, open dialogue can only enhance our ability to communicate, work in teams and problem solve effectively.

Robust discussion, even spirited argument, do not crowd out that respect and support we are talking about. Rather, vigorous debate confirms mutual respect and allows for creativity and increased engagement.
Under the capable leadership of our D&I champions, Shaneen Trotman and Jacqueline Blount, we begin a new chapter in the PCAOB's growth and

development as an effective, creative, and innovative organization for the public good.

But the responsibility for creating and maintaining a diverse workforce and an inclusive workplace is all of ours. Board members and directors need to set the tone. But each one of us needs to do our part.

Cyber-enabled intimidation of NATO personnel in Baltics

National Cyber Security Centre
a part of GCHQ

According to open source reporting, advanced surveillance techniques (possibly including drone monitoring and/or IMSI grabbing) are being used to pull data from personal smartphones of NATO personnel despite warnings not to use them following previous incidents.

There are accounts of personnel then being approached in public by individuals who convey details pulled from smartphones – in one example details about the personnel's family.

This is not the first time NATO personnel operating in Europe have reported call interference or unusual behaviour by their mobile phones.

Mobile devices operating over the public telephone system are susceptible to exploitation including interception of communications or tracking of the user.

The capability to mount operations against personal electronic devices, including the use of rogue cell towers is within technical and financial reach of well-resourced threat actors.

However, the more recent reporting is different as exploitation of devices has been *followed up by personal approaches.*

It is almost certain that personal mobile devices will increasingly become targets for a wide range of threat actors due to the amounts of personal information they hold, which is useful for espionage, targeting and criminal purposes.

Personal mobiles are susceptible to a range of compromise vectors and have widely varying levels of cyber hygiene.

This threat could expand beyond NATO personnel to businesses operating in the region or individuals traversing these areas on business or personal trips.

The Internet of Things: when your washing machine and blood pressure monitor become a target for cyberattacks

Europol-ENISA conference tackles security challenges of IoT

With at least 20 billion devices expected to be connected to the internet by 2020, the Internet of Things (IoT) is here to stay.

While it has many undeniable positive effects, the threats and risks related to the IoT are manifold and they evolve rapidly.

For this reason, ENISA and Europol joined forces to tackle these security challenges by organising a dedicated two-day conference on 18 and 19 October 2017, which was attended by more than 250 participants from the private sector, security community, law enforcement, the European Computer Security Incident Response Teams (CSIRT) community and academia.

The Internet of Things is a wide and diverse ecosystem where interconnected devices and services collect, exchange and process data in order to adapt dynamically to a context.

In simpler words, it makes our cameras, televisions, washing machines and heating systems 'smart' and creates new opportunities for the way we work, interact and communicate, and how devices react and adapt to us.

It is important to understand how these connected devices need to be secured and to develop and implement adequate security measures to protect the Internet of Things from cyber threats.

Beyond technical measures, the adoption of IoT has raised many new legal, policy and regulatory challenges, broad and complex in scope. In order to address these challenges, cooperation across different sectors and among different stakeholders is essential.

The risk of criminals 'weaponising' insecure IoT devices was already identified in the 2014 and 2015 editions of Europol's Internet Organised Crime Threat Assessments and in ENISA's 2016 Threat Landscape Report.

It became a reality at the end of 2016 with several DDoS attacks of unprecedented scale originating from the Mirai botnet.

It must be assumed that cybercriminals will develop new variants and enlarge the variety of IoT devices affected by this type of malware.

This joint Europol-ENISA conference, the first one on the topic, provided the opportunity for all the relevant stakeholders to come together, discuss the challenges faced and identify possible solutions, building on existing initiatives and frameworks. A specific focus was on the role of law enforcement in responding to the criminal abuse of the IoT.

The two-day meeting was testimony to the willingness of all the relevant international actors to ensure that the many benefits of the IoT can be fully realised by jointly addressing the security challenges and combating the criminal abuse of such devices, ultimately making cyberspace a safer place for all.

To read more:
https://www.enisa.europa.eu/news/enisa-news/the-internet-of-things-when-your-washing-machine-and-blood-pressure-monitor-become-a-target-for-cyberattacks

How Bright is the Moon, Really?

The "inconstant moon," as Shakespeare called it in Romeo and Juliet, is more reliable than his pair of star-crossed lovers might have thought. Now researchers at the National Institute of Standards and Technology (NIST) plan to make the Moon even more reliable with a new project to measure its brightness.

Scientists put the Moon to work daily as a calibration source for space-based cameras that use the brightness and colors of sunlight reflecting off our planet to track weather patterns, trends in crop health, the locations of harmful algal blooms in oceans and much more.

The information sent from Earth-facing imagers allows researchers to predict famines and floods and can help communities plan emergency response and disaster relief.

To make sure that one satellite camera's "green" isn't another's "yellow," each camera is calibrated—in space—against a common source. The Moon makes a convenient target because, unlike Earth, it has no atmosphere and its surface changes very little.

The trouble is that, for all the songs written about the light of the silvery Moon, it's still not understood exactly how bright the Moon's reflected light is, at all times and from all angles.

Today's best measurements allow researchers to calculate the Moon's brightness with uncertainties of a few percent—not quite good enough for the most sensitive measurement needs, says NIST's Stephen Maxwell.

To make up for these shortcomings, scientists have developed complicated workarounds. For example, they must periodically check the accuracy of their satellite images by making the same measurements multiple ways—from space, from the air and from the ground—simultaneously.

Or, if they want to compare images taken at different times by different satellites, they have to ensure that there is some overlap during their time

in space so that the imagers have the chance to measure the same part of the planet at roughly the same time.

But what happens if a research team can't get a new camera into space before an old one is retired? "You get what's called a data gap, and you lose the ability to stitch together measurements from different satellites to determine long-term trends," Maxwell says.

Really knowing how bright the Moon is—with uncertainties of much less than 1 percent—would reduce the need for these logistically challenging solutions and ultimately save money.

So NIST is setting out to take new measurements of the Moon's brightness. Researchers hope they will be the best measurements to date.

"Brightness" here means, specifically, the amount of sunlight reflecting off the surface of the Moon. Its apparent magnitude is about 400,000 times smaller than the Sun's, but the Moon's exact brightness depends on its angle with respect to the Sun and Earth. And those angles follow a complex pattern that repeats roughly every 20 years.

To capture moonlight in their new experiment, researchers will use a small telescope as what Maxwell calls a "light bucket," designed to collect everything from ultraviolet radiation (about 350 nanometers, billionths of a meter) through the visible spectrum and into the short-wave infrared (2.5 micrometers, millionths of a meter).

The 150-mm (6-inch) telescope's single lens is made of a compound called calcium fluoride, which—unlike more common glass—can focus the moonlight from this wide range of wavelengths into a detector.

But that telescope will need to be calibrated before each measurement. So about 15 to 30 meters (50-100 feet) away, the research team will set up a broadband light source—that is, one with a wide distribution of wavelengths—with a reliable output.

To validate the broadband source, the scientists will also use a second lamp that emits only a narrow band of wavelengths at a time and can be tuned to different bands as needed. Nightly tests with these calibrated sources will tie the team's Moon findings to the International System of Units (SI).

Fortunately, the NIST study won't need to collect data for 20 years, Maxwell says; three to five years will be enough time to gather more than 95 percent of the angles they will need.

To get as much unadulterated moonlight as possible, the experiment is scheduled to start taking measurements in 2018 at the Mauna Loa Observatory in Hawaii. Sitting at about 3,300 meters (11,000 feet), on one of the world's largest volcanoes, the planned site is above much of the distorting influence of Earth's atmosphere.

Though the experiment will take years to complete, Maxwell thinks even preliminary data will be useful to the community "almost immediately," as a check against the current system.

Earth-facing imagers that could benefit from NIST's new dataset include the Landsat (link is external) series, GOES-16 (link is external), the soon-to-be launched JPSS-1 (link is external) and dozens of commercial satellites.

Vulnerability of Wi-Fi WPA2 networks

A serious vulnerability affecting the Wi-Fi Protected Access II – WPA2 protocol has been discovered. A potential attack would work against most Wi-Fi network setups e.g. the original WPA, WPA2, and even against networks that only use the Advanced Encryption Standard (AES) technique.

Every time a vulnerability affects the security of a network or a cryptographic protocol, a wide range of devices or services are potentially put at risk.

This vulnerability enables an attacker to modify the protocol's handshake, which can essentially lead to intercepting the internet traffic of a Wi-Fi network. Also, depending on the network configuration, the attacker could inject and/or manipulate data without owning or breaking its password security.

The affected devices such as smart devices, Internet of Things (IoT), routers etc. might never receive a patch addressing the issue.

A potential attacker who is in the physical proximity of a protected Wi-Fi network and carries out this attack performs a 'man-in-the-middle' attack. The attacker can essentially intercept or decrypt internet traffic without owning any passwords or cryptographic keys. Therefore, changing the Wi-Fi password would not be of help.

The EU Cybersecurity Agency ENISA has collected and analysed information on this situation and has issued a cybersecurity info note at: https://www.enisa.europa.eu/publications/info-notes/an-overview-of-the-wi-fi-wpa2-vulnerability

This provides a comprehensive overview of the event and key recommendations on how to proceed in case people and organizations are affected.

Despite the fact that this vulnerability is present in the Wi-Fi standard and thus affects a very large number of devices, Wi-Fi users should not panic.

This issue can be resolved through software and firmware updates.

While waiting for manufacturers to prepare and push patches for their devices, you should either apply the available security measures or to use the 4G mobile internet connection deliver by your carrier instead of a Wi-Fi connection.

For each of your Wi-Fi enabled devices, check with the manufacturer or vendor and apply patches as soon as they become available.

Also, apply security measures on different layers. For example, use only HTTPS websites and trusted Virtual Private Network (VPN) providers.

If you're an organization, you should separate your wireless network from the enterprise, wired networks.

All EU Member States regulatory authorities are aware of the seriousness of the situation. They have issued warnings, alerts or other relevant information that include also recommendations for end users.

An overview of the Wi-Fi WPA2 vulnerability

What happened?

A security researcher discovered and disclosed a serious vulnerability affecting the Wi-Fi Protected Access II – WPA2 protocol, which is used by all modern, protected Wi-Fi enabled devices.

The vulnerability enables an attacker to modify the protocol's handshake, which can essentially lead to intercepting the internet traffic of a Wi-Fi network -and depending on the network configuration, it is also possible to inject and/or manipulate data, without owning or breaking its password security.

The vulnerability is serious, has a very big attack surface but it also has its limitations: it cannot be performed remotely.

It can be performed only when the attacker has physical proximity to the victim. There are already ways that people can protect themselves from the attack while waiting for security patches to be released for their devices.

The severity of the issue should not be underestimated, albeit people should not panic as well.

The biggest issue raised by this vulnerability -given its scale - is the fact that a vast majority of affected devices, e.g. smart devices, IoT, routers etc., might never receive a patch addressing the issue.

This note provides an overview of the vulnerability, and some basic recommendations that can be followed whilst patches are rolled out by the various manufacturers/vendors.

Overview of the vulnerability and attack

The identified weakness is in the Wi-Fi standard itself, and not in individual products or implementations.
Hence, according to the researcher, any correct implementation of WPA2 is likely affected (list of affected vendors).

The attack against the vulnerability is dubbed KRACK (Key Reinstallation Attack) and enables an attacker to attack the 4-way handshake of the WPA2 protocol, i.e. the initiation of the WPA2 connection.

This handshake takes place every time a client wants to join a WPA2 Wi-Fi protected network in order to confirm that the client and access point hold the correct credentials, i.e. Wi-Fi password, before the client joins the network.

During the same 4-way handshake a fresh encryption key, which is used for encrypting subsequent traffic is established.

By manipulating this 4-way handshake an attacker can trick a victim into reinstalling an already-in-use encryption key, while a key should only be installed and used once.

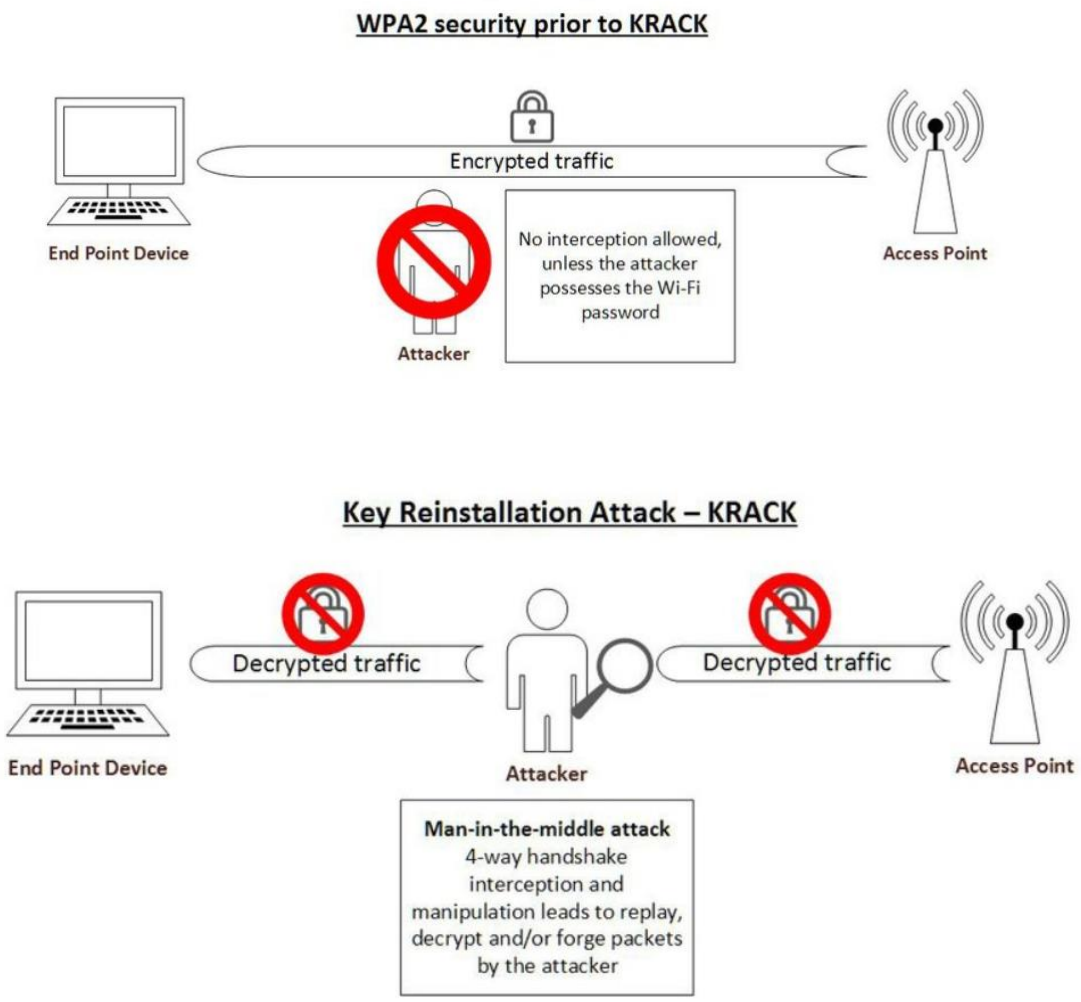
Reinstalling an encryption key, forces two counters (known as “nonces”) used by the encryption protocol to reset and this enables an attack against the protocol e.g. replay, decrypt and/or forge packets.

A potential attacker who is in the physical proximity of a protected Wi-Fi network and carries out this attack, performs a man-in-the-middle attack.

The attacker can essentially intercept/decrypt internet traffic without owning the credentials of the protected Wi-Fi network (therefore changing the Wi-Fi password won’t help).

This attack can further be combined with downgrade attacks against SSL/TLS websites (that have not applied security measures against downgrade attacks) in order to turn an HTTPS[1] connection to HTTP and steal more sensitive information.

The Key Reinstallation Attack is illustrated in the simplified figure below:



The attack works against personal and enterprise Wi-Fi networks, against the original WPA, WPA2, and even against networks that only use AES, i.e. pretty much most Wi-Fi network setups.

For the technical interested audience, the researcher who discovered the vulnerability noted that the same key reinstallation technique can also be used to attack the group key, PeerKey, TDLS, and fast BSS transition handshakes as well.

The researcher describes the vulnerability in the paper called “Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2”, which is a highly technical paper for those interested in the details of the attack.

To read it: https://papers.mathyvanhoef.com/ccs2017.pdf

Additionally, the researcher provided a video with a proof-of-concept attack against an Android smartphone.

Lines to take

- Despite the fact that vulnerability is present in the Wi-Fi standard and thus affects a very large number of devices, do not panic!

- The WPA2 vulnerability is severe and provides a big attack surface but it can only be exploited within the physical proximity of the target Wi-Fi network and not remotely through the Internet, which reduces its impact.

- WPA2 is only one of the available layers of security impacted. Keep in mind that properly configured websites, e.g. usually banks, e-mail providers, social media etc. that use TLS (HTTPS) are still protected from such an attack.

- There is no evidence that the vulnerability has been exploited in the wild and it is uncertain of how easily this vulnerability can be exploited.

- WPA2 is still a more secure solution compared to WEP -the previous Wi-Fi protocol. Hence, switching to an older -trivially exploitable- protocol, is highly discouraged. It is better to continue using WPA2 when using Wi-Fi.

- Avoiding WPA2 protected Wi-Fi networks all together is highly unrealistic. Thus, in such cases people should be pragmatic, apply available security measures or use 4G mobile internet connections, while waiting for manufacturers to prepare and push patches for their devices.

- The issue can be resolved with software/firmware updates. Check with the manufacturer/vendor for each of your Wi-Fi enabled devices and apply patches as soon as they become available. Manufacturer readiness on such issues should be a weighting factor for purchasing technological devices. Home users who obtain their routers from their broadband providers should contact their provider and check whether there is a patch available for their equipment and ask for installation instructions.

- Whenever possible use a 4G mobile internet connection instead of a Wi-Fi connection.

- While waiting for patches, you may treat all Wi-Fi networks like public, open and insecure networks. Therefore, apply security measures on different layers. This is an essential rule in security and quite effective in this case as well.

  Namely:

  a. Use only HTTPS websites. Refrain from using simple HTTP websites and sharing personal information through them. Consider using a browser extension like HTTPS Everywhere, which forces any site that supports HTTPS connections to encrypt your communications with that website by default

  b. Use a trusted Virtual Private Network – VPN provider. VPNs establish an encrypted tunnel between an endpoint and the trusted provider, protecting internet traffic routed through untrusted networks. This means that by using a VPN, an attacker that carries out KRACK cannot intercept the user's traffic. Keep in mind that choosing a trusted VPN provider is crucial when using a commercial VPN solution.

- Organisations should separate their wireless networks from their enterprise, wired networks.

Relevant ENISA actions

In the last years ENISA has invested a lot of resources in the Telecom area. Since 2011 a considerable number of guidelines/studies have been produced and more than 700 incidents have been collected and analysed. All those were made possible through the support of the Art. 13a Expert Group, a dedicated security group made of national authorities across EU.

In the case of the WPA2 vulnerability, an ad-hoc cooperation initiative started within the group, and the results can be summarised at this point as follows:

- All Member States regulatory authorities are aware of the seriousness of the situation; they have issued warnings, alerts or other relevant information that include also recommendations for end users;

- A dialog has been established between authorities and telecommunication providers (ISP) at national level in order to identify specific risks within each context (e.g. main types of routers used in

each country, if patches have been released etc.) and actions taken by providers.

Closing Remarks

Every time a vulnerability affects the security of a network or a cryptographic protocol a wide range of devices or services are potentially put at risk. In such cases it is useful not to panic and carefully assess the theoretical and practical risk of the vulnerability.

Having said that, it is advised to also take into account the available security measures, in order to determine the vulnerability's potential impact.

One of the main issues and challenges raised by this vulnerability is the state of readiness of manufacturers to respond to such incidents, prepare, push patches to their products in a timely manner, and not leave their products vulnerable.

As internet connected devices are becoming ubiquitous, it is essential to work on keeping this ecosystem protected since we have already experienced security incidents that aim to undermine the state of cyber security.

Bad Rabbit ransomware

National Cyber Security Centre
a part of GCHQ

This week, 'Bad Rabbit' ransomware infections have been reported in countries including Russia, Ukraine, Bulgaria, Turkey, Germany and Japan.

The NCSC has not received any reports that the UK has been affected by this latest malware attack. The majority of infections have been in Russia, where media organisations were worst affected. Russia's Interfax News Agency suffered outages to several of its services, including its news portal. Ukrainian victims included the Ministry of Infrastructure, Odessa airport and Kiev metro.

Bad Rabbit asks victims to pay 0.05 Bitcoin (currently worth approximately £210) to restore their files.

A small number of transactions are reported to have been made, although these are unconfirmed, and it is currently unknown whether paying the ransom leads to decryption of files.

The infection vector is believed to be via certain compromised media websites in the affected regions, which asks the user to execute a fake Adobe Flash Player update.

Researchers including FireEye and Crowdstrike have identified several links between Bad Rabbit and the NotPetya ransomware, including the use of similar Javascript code to redirect victims.

While claims have been made that Bad Rabbit made use of the EternalBlue exploit leveraged by WannaCry and NotPetya, these have been widely refuted; subsequent claims have been made that the EternalRomance exploit was leveraged.

It is currently unclear who is responsible for this ransomware. NCSC technical analysis is ongoing to provide more clarity on technical indicators. There are no reported UK victims to date.

Nevertheless, it should be noted that UK organisations would be vulnerable were they to visit any of the infected websites. In the case of NotPetya for instance, a number of UK organisations were infected.

The NCSC has provided some mitigation advice in its public statement, highlighting the importance of patching, using proper antivirus services and having effective backup procedures. To read the advice: https://www.ncsc.gov.uk/news/statement-bad-rabbit-malware-incident

In addition to this, Bad Rabbit makes use of a set of hard-coded username/password combinations in order to attempt to spread to SMB shares on the local network.

Organisations should ensure that these username/password combinations do not exist anywhere on their network, and in general that they follow good password practices (as per NCSC password guidance at https://www.ncsc.gov.uk/guidance/password-collection).

Clear Talk for First Responders

NIST modeling tool to help advance cellular emergency communications

For first responders, such as firefighters, police officers and emergency medical technicians, a successful outcome to a mission—and perhaps the difference between life and death for them and those they are helping—depends on their communications system.

Recognizing this critical need, first responders and emergency management officials have been calling for high-speed, LTE (Long-Term Evolution) cellular devices with three public safety "mission-critical voice" capabilities: "push-to-talk" for an immediate connection, "one-to-many" allowing an individual to broadcast to a large group, and "direct mode" that maintains a walkie-talkie connection when a wireless network is down, blocked or otherwise unavailable.

To make this technology work effectively and ensure consistent product quality, the experts have already started developing standards.

There's just one catch: a device that employs all of these desired features doesn't yet exist. And without a working device to scientifically evaluate in different emergency situations, it hasn't been easy to design the standards that will optimize its performance.

So, to keep mission-critical voice communications development and standardization moving forward, the National Institute of Standards and Technology (NIST) is putting a new computer modeling tool on the job.

The NIST tool uses ns-3 (https://www.nsnam.org/https://www.nsnam.org/), an open-source network simulation software, giving researchers the ability to virtually recreate any emergency scenario and draw upon a variety of environmental, structural, technological and human behavioral factors that could impact the performance of future LTE cellular devices.

Models produced by the NIST tool address performance issues such as voice traffic: who's talking, blocked or waiting in line to speak at any moment, and how well is the overall conversation flowing; location: how do first responder movements—such as into and out of buildings, behind trees

or next to metal walls—affect transmissions; networking: how easily can additional first responder units join the communications network established by the team initially on the scene; and the use of protocol emergency buttons: how effective are these functions that give first responders the ability to break through ongoing communications to request immediate assistance for victims or themselves.

A graphical user interface (GUI) can be used with the NIST tool so that results from the models can be viewed as animations.

Videos with demonstration scenarios showing first responders and the LTE communications protocol in operation during different types of emergencies are available from NIST.

"We hope that the new modeling tool will be widely used by researchers who want to experiment with different ways to optimize the three key mission-critical voice capabilities, by manufacturers who want to 'field test' device designs without having to build multiple versions, and by emergency management officials who want to educate first responders under their command about the advantages of LTE communications in hazardous situations," said Richard Rouil (link sends e-mail), a computer engineer in NIST's Communications Technology Laboratory (CTL) who helped create the tool.

"Most importantly, the tool makes it possible to develop, test and refine standards for the next generation of emergency response communications devices concurrently with, rather than after their development."

According to Rouil, a collaborative effort with the University of Washington will work toward integrating the NIST module directly into the ns-3 software to enable expansion of the tool's modeling capabilities.

Funding for this project comes from a NIST grant awarded in June 2017 to the University of Washington as part of the Public Safety Innovation Accelerator Program, a technology advancement effort for public safety communications that also is funding the development of the LTE modeling tool.

The Innovation Accelerator Program, managed by NIST CTL's Public Safety Communications Research (PSCR) Division, provides research, development, testing and evaluation of broadband communications technologies to foster nationwide interoperability among first responders.

The NIST LTE Device-to-Device Communication Model for ns-3 is available for downloading (link is external) as is the free ns-3 software (link is external).

A recent NIST paper provides information on the implementation and validation of the model – you may visit: https://www.nist.gov/publications/implementation-and-validation-lte-d2d-model-ns-3

A tribute to Stanley Fischer

A tribute to Mr Stanley Fischer, Vice Chair of the Board of Governors of the Federal Reserve System, by Mr Erkki Liikanen, Governor of the Bank of Finland.

Stanley Fischer is leaving the Fed today. Not very many people excel during their careers as both academics and practitioners at the very highest level. Stanley Fischer is an outstanding example of those rare people: A first-rank researcher and teacher, who is also one of the world's most influential policy-makers, a man who has led some of the most important policy institutions on earth.

Stan Fischer's experience and achievements are such that they defy all attempts to summarize them. Larry Summers was right to write that Stan's departure is the end of an era.

On a personal level, I appreciate our many encounters and our continuing friendship. It is actually remarkable how many contacts Stan has had with my home country, Finland, and Finnish economists.

I will mention just four of them.

The first goes back to the 1970's. Stan had just published the famous macroeconomics textbook he wrote together with Rudi Dornbusch. Soon after that, Stan spent twice two weeks in Finland, together with Dornbusch, teaching the graduate course organized by the Yrjö Jahnsson Foundation.

These courses were invaluable for the growth of the economics profession in Finland, and dominated graduate education in the country for a decade. As the lead instructors of the 1979 course, Stan and Rudi Dornbusch made a durable contribution to the development of the burgeoning economics profession in Finland.

The second is linked to his role as a thesis advisor. As we know, Stan is famous for having been the thesis advisor or teacher of many of the giants of the economic profession. Ben Bernanke, Larry Summers, Olivier Blanchard and others come to mind.

For us Finns but for others, too, the late Pentti Kouri is a particularly evocative name: a brilliant Finnish economist who during his short academic career made a big impression in the field of international monetary economics. Pentti Kouri hailed from Lapland.

His career as a researcher was like the Lapland summer: bright, but did not last long. Stanley Fischer was Pentti's thesis supervisor at the MIT.

Stan told me about Pentti: "He came almost every day after 4 o'clock to talk. Pentti had an incredibly wide scope of interest. So it was very interesting. But finally in April, I told to him that it is nice to talk but not much has happened with your thesis. Only two months later he came back with a very good thesis."

That happened in about 1974. The story describes well Stan's general approach to leadership: he is one of the friendliest and warmest people, but also firm when needed.

Third, he also made great recruitments. At the MIT, Stan was the one who recruited Bengt Holmstrom, the recent Nobel laureate and a University of Helsinki alumnus, from Yale to the faculty of his department.

Bengt has told me that the presence of Stan at the department was an important attraction for him, so he was actually quite disappointed when Stan was soon asked move to the IMF.

Stan's move to the IMF in 1994 occurred on the eve of very momentous events. Together with managing director Michel Camdessus, they navigated the Fund, and the global economy, through the turbulence of the 1990's, which included the Asian and Russian crises, for example. They also witnessed the formation of the euro area.

We all know that Stan, as the first deputy managing director at the IMF, was much respected and admired in the Fund, by the staff and by the executive directors.
Stan is one of the fathers of New Keynesian economics, which is now the dominant and evolving approach in leading economics departments and policy institutions.

His choice of approach has been motivated by the desire to combine theoretical rigor with applicability to real-world problems of real-world people.

When I was appointed Governor of the Bank of Finland, before starting my term I naturally asked for some briefings about what was going on in the world of central banks.

Our head of research told me, before you read anything else, start with this. And he gave me a copy of Stan's essay written for the Bank of England tercentenary conference of 1994, titled "Modern central banking".

Indeed, it is all there: price stability, independence, accountability and transparency. That gave me a good start, for which I am grateful.

Finally, I come to the fourth connection between Stan and Finland. As Governor of the Bank of Finland, I have had the privilege of meeting Stan often and in different places: in the U.S., at the BIS meetings, in Israel, and elsewhere.

We were particularly honoured when Stan, then Governor of the Bank of Israel, took the time to participate in the Bank of Finland's 200th anniversary conference in Helsinki in 2011.

In the remarks he gave in that conference, Stan asked whether a more developed financial system is associated with higher growth rates. He expressed some skepticism on the issue.

In his early research, Stan had found a negative correlation between financial liberalization and economic growth. For example, Japan growing much faster than the U.S. and the U.K. Stan's question, does tighter financial regulation necessarily come with a cost in terms of growth, is just as timely now as then.

I visited the Bank of Israel twice while Stanley was the Governor there. During my first visit, Stan organized a seminar where I gave a talk about the ECB and the Eurosystem.

I told the audience that it was my first visit to Israel, but I had had a particular opportunity to learn about the country and the culture. During my high school years, I had been an exchange student in Yeshivah of Flatbush in Brooklyn, New York.

Then a tall man in the audience stood up and asked: "Do you remember me, I was the captain of the basketball team?" Of course: he was Ed Offenbach, now a senior economist at the Bank of Israel.

Stanley Fischer has left a deep impact on me and others by his intellectual and moral integrity. We feel having been in a particularly privileged position to have worked with him.

My wife Assi and I have also enjoyed our many encounters with Rhoda and Stanley Fischer during our many years in the central banking community. They stay in our memory.

Thank you.

Li-Fi technology offers benefits in mobility, speed, cost, security

Light fidelity, or Li-Fi, is a ground-breaking light-based communication technology which makes use of light waves instead of radio technology to deliver data.

Li-Fi is a bidirectional, high-speed, and fully networked wireless communication technology similar to Wi-Fi, but capable of 10 times faster transmission rates from point to point.

"Li-Fi technology has the potential of being faster than any radio based technology existing at present," said Dr. Bill Butler, project lead for the DISA Li-Fi University Affiliated Research Center (UARC) Project. "With Wi-Fi, all devices are fighting for the same 800 megabits per second (Mbps) of bandwidth. With Li-Fi, the entire visible and non-visible light spectrum is available for use - laying the groundwork for 10 gigabits per second (Gbps) transmission rates within the next calendar year."

Li-Fi can provide the military with high speed, non-detectable communications that cannot be identified through current direction-finding technology. The high-speed, multi-frequency communication capability inherent in Li-Fi can free up bandwidths used in critical legacy applications that haven't converted to newer technology.

With Li-Fi, inter-soldier, inter-vehicle, and inter-ship line-of-sight communications can render mobile units ubiquitous relays of information and orders without any verbal communication, while remaining totally invisible in the battlespace.

Li-Fi will be especially valuable in commercial applications, such as communication between cars and other vehicles requiring integrated high-speed motion detection; in hospitals, where radio waves interfere with delicate instrumentation; in airplane environments, where radio frequencies (RF) can interfere with navigation equipment; and in construction, where heavy explosives are currently detonated through radio signals.

How it works

According to Dr. Butler, "light is already used for data transmission in fiber-optic cables and for point-to-point links, but Li-Fi is a special and novel combination of technologies that allow it to be universally adopted for mobile ultra-high speed internet communications using normal light frequencies across the 440 to 770 terahertz (THz) spectrum. However, Li-Fi can also be used in the non-visible frequencies, such as infrared, X-ray, and ultra-violet frequencies between 300 gigahertz (GHz) to 400 THz - presenting endless possibilities for manufacturing new and complex communication equipment."

Li-Fi uses a photo-detector to receive light signals and a signal processing element to convert the data into 'streaming binary digital' content.

An LED lightbulb is a semi-conductor light source, meaning that the constant current of electricity supplied to an LED lightbulb can be dipped and dimmed, up and down at extremely high speeds, without being visible to the human eye.

For example, data is fed into an LED light bulb (with signal processing technology), it then sends data (embedded in its beam) at rapid speeds to the photo-detector (photodiode). The tiny changes in the rapid dimming of LED bulbs is then converted by the 'receiver' into electrical signal.

The signal is then converted back into a binary data stream that we would recognize as web, video, and audio applications running on internet enabled devices.

Benefits

"Li-Fi offers benefits in mobility, speed, cost, and, most importantly, security," said Dr. Butler.

Currently available Li-Fi commercial products run on visible light, and because light cannot penetrate through solid walls, signals can't be intercepted while being transmitted - unlike traditional radio frequencies. This is a critical advantage when it comes to protecting classified and sensitive DOD missions.

"In battlefields, Li-Fi can be used for vehicle-to-vehicle communications through the use of headlights and taillights without system interference, and the data is secure because information is only transmitted to those in

the line of direct sight. It can also replace the complex cabling required in forward-deployed command centers by combining the network access points in the overhead lighting. This reduces power consumption and simplifies command center setups," said Dr. Butler. "Additionally, there is greater bandwidth availability in light waves than radio waves, and the transmission of data using LEDs is highly energy efficient."

On the Horizon

DISA is in the early stages of exploring Li-Fi technology and the applicable uses for DOD. The technology was demonstrated in a classified work environment and initial pilots confirmed Li-Fi provided secure networked communication within an enclosed space.

"Right now, we are working to procure equipment and configure a demonstration of Li-Fi within a secure, multipoint networked environment," said Dr. Butler. "We will continue to work with our academia partnerships to explore and prototype the next-generation DODIN and move the DOD towards a wireless non-RF complimentary environment."

In the future, Li-Fi may be offered as an enterprise service for secure environments, and may also serve as a solution for other communication requirements.

Data for laptops, smart phones, and tablets is transmitted through the light in a room using diodes pulsing at extremely high speeds undetectable to the human eye. Security is established through direct light transmission, therefore if you are not in the amplified light network you can't access the data or other networked appliances.

Note

DISA, a Combat Support Agency, provides, operates, and assures command and control, information sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to joint warfighters, national level leaders, and other mission and coalition partners across the full spectrum of operations.

Disclaimer

The Association tries to enhance public access to information about risk and compliance management.

Our goal is to keep this information timely and accurate. If errors are brought to our attention, we will try to correct them.

This information:

- is of a general nature only and is not intended to address the specific circumstances of any particular individual or entity;

- should not be relied on in the particular context of enforcement or similar regulatory action;

- is not necessarily comprehensive, complete, or up to date;

- is sometimes linked to external sites over which the Association has no control and for which the Association assumes no responsibility;

- is not professional or legal advice (if you need specific advice, you should always consult a suitably qualified professional);

- is in no way constitutive of an interpretative document;

- does not prejudge the position that the relevant authorities might decide to take on the same matters if developments, including Court rulings, were to lead it to revise some of the views expressed here;

- does not prejudge the interpretation that the Courts might place on the matters at issue.

Please note that it cannot be guaranteed that these information and documents exactly reproduce officially adopted texts.

It is our goal to minimize disruption caused by technical errors. However some data or information may have been created or structured in files or formats that are not error-free and we cannot guarantee that our service will not be interrupted or otherwise affected by such problems.

The Association accepts no responsibility with regard to such problems incurred as a result of using this site or any linked external sites.

Sarbanes Oxley Compliance Professionals Association (SOXCPA)

1. Membership - Become a standard, premium or lifetime member.

You may visit:
www.sarbanes-oxley-association.com/How_to_become_member.htm

2. Monthly Updates - Subscribe to receive (at no cost) Sarbanes-Oxley related alerts, opportunities, updates and our monthly newsletter:

http://forms.aweber.com/form/30/1922348130.htm

3. Training and Certification - Become a Certified Sarbanes Oxley Expert (CSOE).

You must follow the steps described at:
www.sarbanes-oxley-association.com/Distance_Learning_and_Certification.htm

For instructor-led training, you may contact us. We can tailor all programs to your needs.

4. Authorized Certified Trainer, Certified Sarbanes Oxley Expert Trainer Program (SOXCPA-ACT / CSOET) - Become an ACT. This is an additional advantage on your resume, serving as a third-party endorsement to your knowledge and experience.

Certificates are important when being considered for a promotion or other career opportunities. You give the necessary assurance that you have the knowledge and skills to accept more responsibility.
To learn more:
www.sarbanes-oxley-association.com/SOXCPA_Authorized_Certified_Trainer.html