VOLUME 10 2018

NOT FOR SALE

WWW.SECUREMETRIC.COM

SECUREMAG

SECUREMETRIC TECHNOLOGY GROUP

FORMULA FOR STRONG DIGITAL SECURITY

PAGE 12-13 INFOGRAPHIC

PAGE 3-6

"Two essential security components you should include in your Mobile Enterprise strategy"

PAGE 14-15

SMETRIC

10

securemetric.com

SECUREMETRIC TECHNOLOGY

TOGETHER WE ARE STRONGER

CONTENT

PRODUCT HIGHLIGHT

NEWS & EVENTS

INFOGRAPHIC

ARTICLE

AWARD

SecureMetric Technology Sdn. Bhd.
Level 5-E-6, Enterprise 4,
Technology Park Malaysia
Lebuhraya Sg. Besi - Puchong,
Bukit Jalil, 57000 Kuala Lumpur,
Malaysia.
Phone: +603-8996 8225
Fax: +603-8996 7225

638/SEC09C 01817/SEC02A

SecureMetric Technology Sdn Bhd

SecureMetric is a digital security specialist with core expertise in Software Licensing Protection, 2-Factor Authentication, Advanced Identity & Access Management and more to help companies solve their information and transactional security needs.

Over the past decade, the SecureMetric brand name has been steadily growing and gaining respect in their respective domain of expertise just as their team have been growing. From 10 staff members in 2007, SecureMetric has expanded across Asia in countries such as Singapore, Indonesia, Vietnam and the Philippines to build a strong regional workforce of about 90 employees.

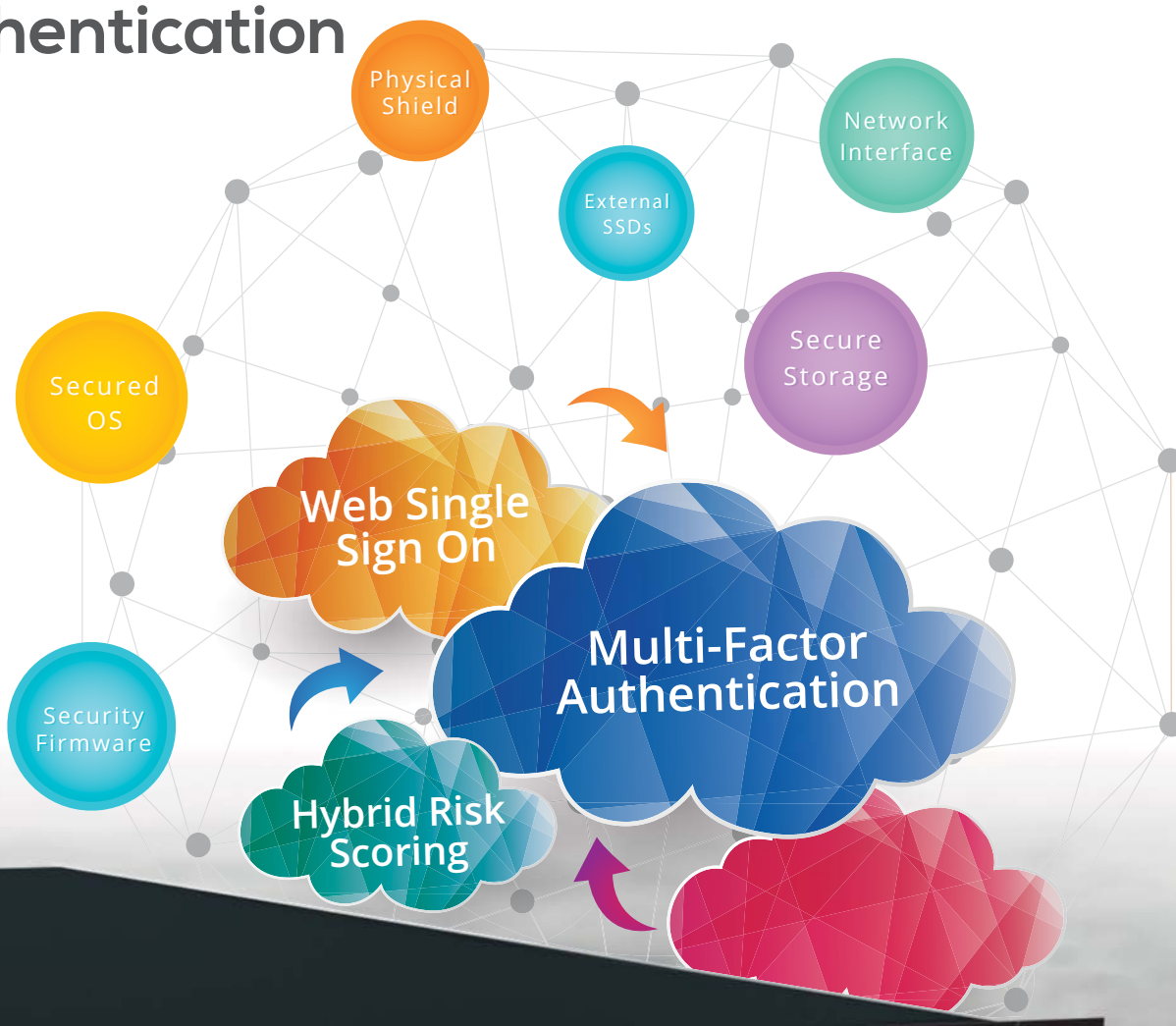
SecureMetric probably the Southeast Asia's No. 1 Software License Protection and PKI Token provider

SecureMetric is well recognized as the the regional TOP PKI System builder originated from Southeast Asia.

CENTAGATE® BOX

HARDENING AUTHENTICATION SECURITY

All-in-One Authentication Appliance



CENTAGATE® BOX

is one of the latest innovation from SecureMetric that bring forward the adoption of next generation authentication never been so easy. It is an all-in-one FIPS 140-2 Level 3 certified made in Germany hardware appliance that integrated with Common Criteria EAL 4+ certified CENTAGATE® Software. It's certainly tackle right into the high demand of migrating obsolete authentication system to a new authentication system due to either comply with new regulatory requirements or defence against new cyber threats.

KEMENTERIAN SAINS, TEKNOLOGI DAN INOVASI
Ministry of Science, Technology & Innovation

This project is successfully commercialized and funded by MOSTI TechnoFund

CENTAGATE® BOX is a complete authentication solution which offers multi-factor authentication with Hybrid Risk Scoring engine; unify various applications login credentials, maintaining only single credential to access multiple applications; and manages user's identity intelligently.

Hybrid Risk Scoring engine is a comprehensive authentication and fraud detection platform. It is designed to measure the risk associated with a user's login and post-login activities by evaluating a variety of risk indicators such as Geo-location, Operating System, Browser Type, IP Address, Device and Time. Using a risk and rules based approach, then system then requires additional identity assurance for scenarios that are high risk and violate a policy.

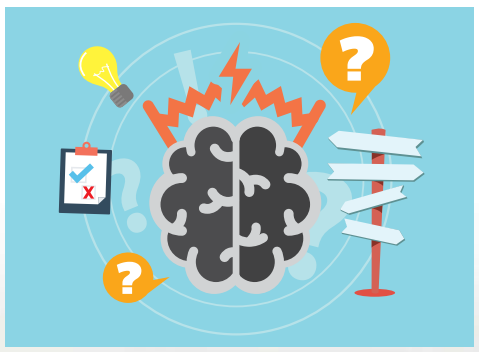
CENTAGATE® BOX provides out of the box support for SMS gateway providers such as MacroKiosk and Twilio, the system uses both SMS gateway provides APIs to invoke SMS messaging.

This solution also provides native application for Android and iOS, which can be customized to meet customer's required look and feel. In addition, CENTAGATE® mobile app comes with mobile SDK which can be integrated with the customer's existing mobile application. It can do more than just authentication but also include transaction authorization with integrated Hybrid Risk Scoring engine.

In consideration for performance and high availability of the authentication service, SecureMetric proposes two units of CENTAGATE® BOX in production environment on active-active mode and one unit of CENTAGATE® Box for Disaster Recovery (DR) site. For development and test environment, it is recommended to have separate boxes as well.

Common Challenges

Hard to Choose the RIGHT Authentication System

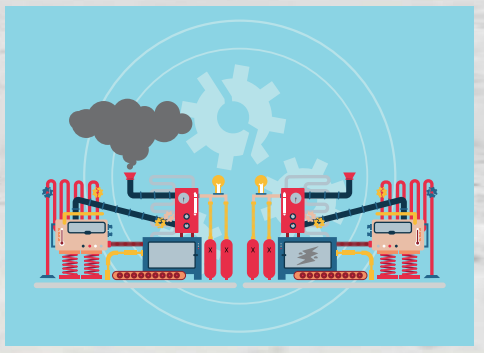


Solved with
CENTAGATE®, CC EAL 4+
Certified MFA + SSO + Risk Scoring

Hassle to Deal with Multiple Vendors

Solved with
CENTAGATE® Box, Single Vendor,
All-in-One Box

Difficult to Ensure Data / System Security Integrity



Solved with
CC EAL 4+ Certified CENTAGATE®
Core + FIPS Level 3 Certified Appliance

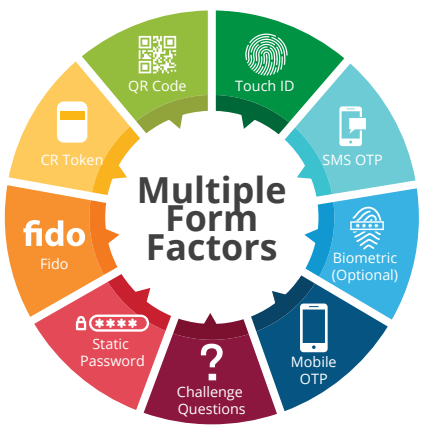
Concern about Time to Market

Solved with
Out Of The Box CENTAGATE® BOX
with Shorter time to deploy

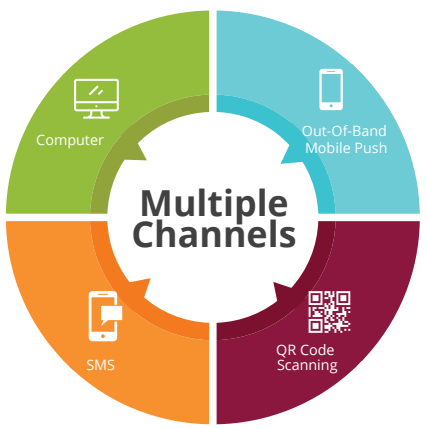
High Total Ownership Cost

Solved with
Highly competitive CENTAGATE®
BOX pricing

Key Features of **CENTAGATE® BOX**



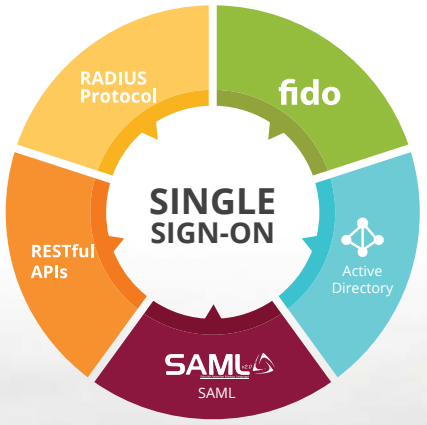
CENTAGATE® BOX has a built-in support for SMS OTP, OTP Token, Mobile OTP, CR Token, Mobile CR, QR Code, Touch ID, PKI Token, Mobile PKI, FIDO Token, challenge questions and answers, static password with policy, and list goes on. CENTAGATE® BOX offers a centralized Identity Management with highly flexible yet comprehensive authentication form factor option that will surely fit your requirement.



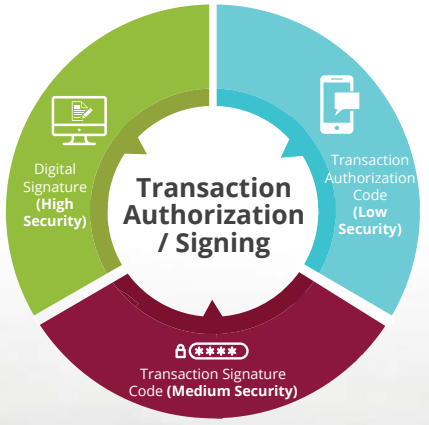
Multiple channels during authentication could effectively help to prevent real-time attacks that includes Man-In-The-Middle / Browser and real-time phishing / Pharming. CENTAGATE® BOXprovides different channels via PC, Out-Of-Band Mobile Push, QR Code Scanning and SMS. Whenever is needed, the system will authenticate a user through multiple channels to increase the security strength.

CENTAGATE® BOX provides native mobile application compatible with iOS and Android devices which has built-in with strong cryptographic mechanisms that can be used as a reliable security token. CENTAGATE®'s Mobile SDK will be provided to facilitate client mobile application integration.

CENTAGATE® BOX Hybrid Risk Scoring engine is a patented comprehensive authentication fraud detection platform that is designed to measure the risk and rules associated with a user's login together with its post-login activities by evaluating variety of risk indicators such as Operating System, Browser, IP Address Location, Time and Transaction Behavior (only for customised project). Whenever the system detects any scenarios that are high risk, it will trigger additional steps of authentication through different channels. This method can effectively detect suspicious transactions, even before it could happen.



CENTAGATE® BOX supports various different integration interfaces such as WebSSO using SAML 2.0, Web Service APIs through RESTful APIs, Radius Protocol, FIDO U2F standard and Active Directory. Generally CENTAGATE® BOX support on any JAVA, PHP, ASP, ASP.Net or any other web applications that can call Web Services methods. It can also be integrated to any compliant devices, such as Firewall, networking devices, and other closed source applications which provides Radius protocol compatibility or SSO via SAML2.0 integration. CENTAGATE® BOX help organization to achieve the objective of "All-in-One Authentication Platform".



CENTAGATE® BOX supports 3 different security level methods to authorise an transaction,

• Transaction Authorization Code (low security)

Request a SMS-OTP code to be keyed in to as to authorize a transaction.

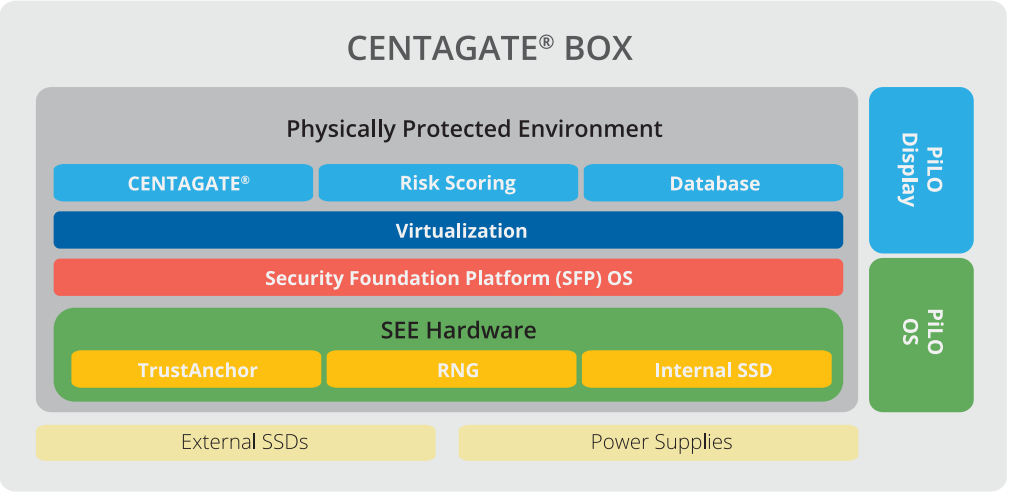
• Transaction Signature Code (medium security)

An OTP signature to authorize a transaction that will be generated after an input data provided by the client application.

• Digital Signature (high security)

User will sign the transaction digitally using PKI (either hardware token or token) where a PKCS#7 digital signature format will then be validated by CENTAGATE® BOX.

Concept of **CENTAGATE® BOX**



Inside CENTAGATE® BOX

CENTAGATE® BOX is a FIPS 140-2 Level 3 compliant secure hardware appliance that is integrated with Common Criteria EAL4+ Certified CENTAGATE® software.

TrustAnchor (TA)

1) TrustAnchor (TA) is an independent hardware-based security built into ARM based System on Chip (SoC) to provide secure end points and a device root of trust.
2) TrustAnchor (TA) validates the boot images before change will apply to the mainboard and control the status of the server mainboard.
3) TrustAnchor (TA) commonly used to run as Secure Boot to assure integrity of started system.

Physical Shield

1) The entire server hardware is submerged into epoxy, creating a physical shield.
2) There is enough processing power to deliver high performance operations.
3) There are enough connectivity to deliver server grade applications and there is replaceable storage and power supply.

RNG (Random Number Generators)

1) Random Numbers are a cryptographic primitive and cornerstone to most cryptographic systems.
2) Entropy and good random numbers are critical for crypto operations.
3) RNG is the non-deterministic random number generator that complies to NIST SP-800 compliant hardware.
4) In order to have the good random numbers, RNG will use hardware entropy as source feeding OS(Linux) entropy pool.
5) Based on microcontroller with a multiple analog voltage sensors, which is better source of entropy with better performance.

Controlled interfaces

1) No low level access to hardware and software
2) Onle Ethernet or serial line communication is available

Zeroization capabilites

1) Completely erases all configuration information on the device, including all plain-text passwords, secrets, and private keys for SSH, local encryption, local authentication

Out-of-band Management

1) PiLo is server management technology which provides out-of-band management facilities.
2) PiLo perform activities on a server from a remote location. PiLO has a separate network connection to which one can connect via HTTPS.
3) With PiLo, activities such as reset the server or power-up the server can be done remotely, even if the server is shut down.
4) PiLo display with Multi Touch User Interface to administer security functionalities.

SECUREMETRIC JOINED

Technology Conference for IT Systems

Ho Chi Minh, Vietnam – Technology conference's objective is to enhance the security, safety and lower risk reduction in electronic payment and card payment. The Governor of the State Bank of Vietnam requires units and payment service suppliers to actively inform, propagate and disseminate the regulations of the State to prevent the methods and tricks of high-tech criminals as well as to study all application of international standards to the payment system. Last July 20th 2017 the Information Technology Department of the State Bank of Ho Chi Minh City organized a technology conference about deployment of security solutions for IT systems and invited SecureMetric as one of the two organizations with the most effective security methods to speak and introduce to the banks and credit institutions in Ho Chi Minh city.

At the workshop, information of the modes operation, tricks of high-tech crime, types of risks and frauds in payment operations were discussed and attendees were interested in the solution that were presented. Being trusted by the Information Technology Department of the State Bank of Ho Chi Minh city,

SecureMetric presented their solution that helps to prevent the risk and asset security for customers and payment service providers. After the demo and presentation on how the CENTAGATE® BOX works, guests showed interest by asking inquiries.

The Information Technology Department of the State Bank of Ho Chi Minh City was pleased with the success of the workshop.

SECUREMETRIC'S

Breakthrough Reinvention

The world is advancing minute by minute so is technology and a lot of changes has been brought by continuous technology development-it has simplified people's lives, for instance, modern technology improved healthcare, education and communication. Investing in technology especially in business can bring vast of advantages no matter what industry and how big or small the business is, it can increase profits, business processes can be modernize and it can open up new opportunities.

Since technology never stops evolving, Southeast Asia's leading regional players in the field of digital security, SecureMetric, is constant in learning new possible ways to enhance their solution to provide its client the most effective and reliable digital security solution. SecureMetric's R&D team continues in innovating, reinventing and developing new and exciting solutions that keep pace with technological advances.

This year, SecureMetric launched its newest innovation, CCENTAGATE® BOX, an all-in-one appliance based solution that includes everything you need to set up your enterprise authentication. It has a single Made Germany 2U appliance and hardware architecture that is designed based on rigid security requirements (FIPS 140-2 Level 3) similar to Hardware Security Module with the proprietary security firmware as the base using CENTAGATE® software. It is a centralized Multi-Factor Authentication management that features multiple integration interface that makes it the perfect choice as "All-in-One Authentication Platform" It has a controlled well defined interface, touch screen front panel, protected OEM software stacks, high security level which will not access the hardware and software easily, with signed and encrypted software packages and secure reset cycle deleting all secrets (zeroization).

CENTAGATE® BOX, was officially launched at the respective SecureMetric branches in Vietnam and Philippines. Last July 20 2017, SecureMetric Vietnam joined a workshop organized by State Bank Vietnam's IT department, held at their office in Ho Chi Minh City. The workshop aim to introduce and share experiences of deploying authentication and security solution for IT system. Attended by IT Managers and Staff of commercial banks' in HCMC, SecureMetric was privileged to be one of the vendor who presented Centagate Box. Six days after the launch in HCMC, Securemetric Philippine team arranged an affair to introduce CENTAGATE® BOX, to its clients. Clients from diverse industries such as government agencies, banks, software integrators were invited to witness the latest Multi-Factor Authentication solution. Aside from CENTAGATE® BOX, presentation, there was also a panel discussion facilitated by SecureMetric Chief Executive Officer, Mr. Edward Law to discussed "Hints and Trends of financial service industry towards cyber security investment in view with increasing threats from ransomware and central bank's new policies on electronic banking authentication security". Experts from bank and government led by Bank of the Philippine Island's Assistant Vice President for Systems Quality Assurance Management, Mr. Jonathan Paz and from Philippine National Police, Anti-Cyber Crime Group Supt. Jay Guillermo from Anti- Cyber Group gave their ideas and shared relevant information regarding the issues towards cyber security. Both CENTAGATE® BOX, introduction was headed by Mr. Edward Law.

SecureMetric always make sure that all solution that they offered is affordable, easy to implement and fits all their client needs.

CEO Talk 2017 @

Management and Science University of Malaysia

Kuala Lumpur, Malaysia - Mr. Edward Law, Chief Executive Officer of SecureMetric Group had given a talk to the group of post graduate students of Management and Science University last 15th April 2017. This session was attended by around 80 Master and PHD students from various faculties. Mr. Edward shared his insights and experiences along with his entrepreneur journey focus on the topic "From Small to Big : Transforming Innovation Solution". This is part of SecureMetric's ongoing CSR initiatives to connect to the higher education institutions to offer volunteer basis industrial mentoring and coaching programme.

SECUREMETRIC @

Policy Forum KL

Kuala Lumpur, Malaysia - Policy forum "Cybersecurity: Safeguarding the Future for Innovative Financial Inclusion" was held last 1 & 2 of August 2017 in Kuala Lumpur, Malaysia. Over 130 financial policy makers and regulators from 40 countries attend the forum, co-hosted with Bank Negara Malaysia, this is the first time Alliance for Financial Inclusion (AFI) is focusing on the linkages between cybersecurity and financial inclusion in a peer-learning forum.

The policy forum provides an overview of global cybersecurity risks, typologies of cyber events and behaviors, profiles of cyber attackers and victims, particularly within sectors relevant to financial inclusion and in the context of developing countries. The forum was developed in recognition of the linkages between cybersecurity and financial inclusion based on strong AFI member demand. Cybersecurity was highlighted in a recent AFI member survey as one of the three top areas within the realm of new financial technologies where members would like to learn more.

SECUREMETRIC @

GovWare 2017

Singapore - Singapore held last 19-21 of September, the GovWare event is the region's most established premier showcase for cybersecurity at its 26th chapter. GovWare is the cornerstone event for the Singapore International Cyber Week (SICW).

The event features the latest trends in technology, organisational implementation and user perspective, GovWare attracts practitioners to network, discuss and collaborate about cybersecurity.

Speakers were government officials, thought leaders, visionaries, technology experts and industry professionals and with over 100 exhibitors and sponsors, these event was the leading platform for practical, focused and unbiased knowledge on cybersecurity.

This event was sponsored by MDEC and it was a good collaboration between IT security firms that is spearheading cybersecurity agendas in their respective countries.

SECUREMETRIC PARTICIPATED

RSA Conference 2017

San Francisco, USA – SecureMetric participated at RSA Conference 2017 together with PrimeKey, a standout infosec event that attracted more than 43,000 attendees. These event was held last 13th to 17th February 2017 at Moscone Center, San Francisco, USA.

SecureMetric is pleased to learn and exchange valuable insights with regards to the current trends and future direction in the space of Infosec. During the event, SecureMetric showcased their upcoming solution, CENTAGATE® box and received positive feedback from several international visitors.

Security is always hard, and not about open or closed source

Tomas Gustavsson
Chief Technology Officer and co-founder at PrimeKey Solutions AB

One of the largest data breaches lately, of the credit bureau Equifax, was by some sources blamed on the open source web framework Struts. Whatever security issue the attackers used to breach Equifax, putting focus on the topic of open source vs proprietary software is a flawed though. Security is always hard and many security issues exist in both proprietary and open source software, and there are plenty of examples of both proprietary and open software that have had severe security issues. There are some examples where having open source is likely to have exposed, and fixed, problems earlier, but there are also examples where flaws have hidden in open software for a long time undetected. One thing that must be emphasized is that flaws are usually discovered sooner or later, regardless of the type of software. The one thing that sticks out is that security protocols and standard are always developed openly and transparently (except in some military applications), and security protocols designed in closed fashion are usually easily broken.

Open code reveals security issues?

Two example where open source might have caught problems earlier are the recent vulnerability in a proprietary library used to generate key in common smart cards, and the now infamous Volkswagen diesel fraud.

A vulnerability in a proprietary software library has recently rendered millions of issued electronic ID cards vulnerable. The software flaw was hiding in a proprietary library since 2012, and was discovered by security researchers doing black box analysis on keys generated by the smart cards. Had the library been a commonly used open source library, it is likely that the code had undergone more rigorous analysis, although the library as is had already undergone the highest level of security certification, Common Criteria EAL5.

Open source also have it's share of long time bugs though, as the heartbleed vulnerability of the highly popular openssl library showed. This software flaw had also been hiding, in plain sight, for several years, until discovered forcing many web sites across the Internet to re-generate cryptographic keys that might have been exposed.

Data breaches due to outdated software

Both these examples are highly specialized security software bugs, while most internet breaches, like the Equifax and the now infamous DigiNotar breach is due to bad operating procedures where old version of software, containing known security flaws, are used instead of upgrading to newer versions. In many cases a collection of proprietary and open source components are assembled, and then never upgraded.

The most notorious hack of a public certificate authority, leading to the shutdown of the entire DigiNotar business, was due to outdated prorietary software systems, both the operating system and the application software. Because the software were not upgraded, it was possible for attackers to exploit weaknesses in these proprietary systems with disastrous consequences.

The latest Equifax breach is claimed to have used weaknesses in an open source framework that Equifax used to develop their own system with. Also in this case the open source software was not updated, although there were fixed versions available.

These examples shows that when it comes to security, there are no silver bullets. Research shows that there are weaknesses found in proprietary as well as open source components, and they are both exploited by attackers to breach systems. Security is a very complex area of IT, with limited expertise world-wide, and neither expensive security audits and certifications, nor full openness and peer review is a guarantee for security.

This of course also means that since there are no security benefits of not being open, there is no reason to not be open.

Stay updated

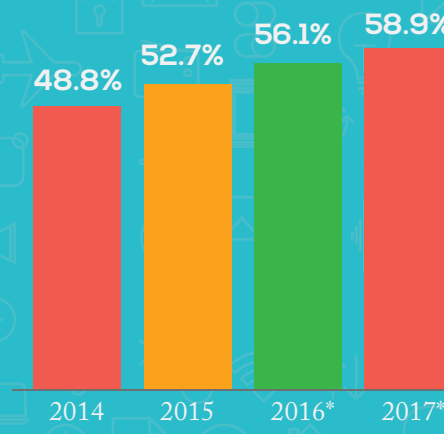
So what can one do? The best way is to be prepared for security issues, and staff projects properly so that systems can be upgraded when security issues are discovered. Keeping system upgraded is the best insurance you can get to stay as protected as possible. Specifically security issues are usually announced, so if you have staff assigned to security, they have the possibility to be notified and find out about most security issues affecting open source components in due time.

Mobile SECURITY

Do you think it's safe to access sensitive data on your mobile phone? Perhaps you should think again. With malicious programs designed to target mobile phones, it's becoming increasingly dangerous to use your phone without any necessary precautions.

Mobile phone intern penetration worldwi

from 2014 to 2019



The Dangers of Mobile Apps

Users expect mobile apps to be vetted and trustworthy, but there are more than **500** third-party apps containing malicious apps.

The History of Risks and Threats

2004 First case of mobile malware found

2009 First iPhone worm found in 100 jailbroken devices

2010 Mobile malware increased by 250% year over year & first bank-phishing mobile app identified

2011 Botnet malware hits Android devices through OS vulnerabilities

2012 Zeus malware is designed to steal mobile transaction authentication numbers (mTANS) / Trojan app in iPhone strealing user address book found in App Store

2013 Android OS vulnerability exploited certificate validation disguising itself as a legitimate application

2014 Android ransomware infects 300,000 devices and stole millions of money / unflod baby panda malware stole Apple ID and password / Adthief malware infects 75,000 jailbroken iPhones

2015 Yanbian Gang hacking group from South Korea lured victims with fake banking apps via sms to steal financial data

2016 DroidJack allows hacker to have full smartphone control via a Pokemon Go game

PHISHI

A fake version of a real site gathe log-in and other private infor

MAN-IN-THE-MIDDLE ATTACKS

Any mobile device that connects to a **Wi-Fi network** is open to this type of attack. The **attacker becomes a "middle man"** in a communication stream and logs all information relayed between the communicating parties

Wi-Fi SNOOPING

Can occur when you access a **public network** at any hot spot. An attacker can easily **"watch"** your online activities and a**ccess your private information.**

EXPLOITING

Some malware will exploit mobile platform vulnerabilities to gain control of the device

WORM

A program that replicates itself, spreading throughout a network

Sources:
https://news.sophos.com/en-us/2015/05/19/check-out-this-infographic-showing-the-history-of-mobile-threats-2004-2015/
https://www.trendmicro.com/vinfo/us/security/news/mobile-safety/revisiting-ios-security-as-apple-cracks-down-on-antimalware-apps
https://www.checkmarx.com/2016/07/18/malicious-mobile-apps-pokemon-go-brief-history-infographic/
https://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/
http://www.visualistan.com/2014/08/mobile-security-infestation-infographic.html
http://www.trendmicro.se/infographics/unwrapping-mobile-security/index.html
https://www.allot.com

net user ide

61.2%

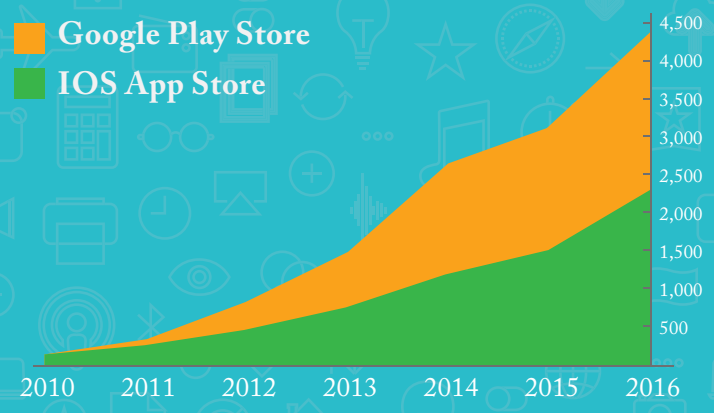
63.4%

2018*

2019*

Global App Volume, By Store

in thousand , 2016



Fake And Infected Apps in Official Stores

Consumer View

Awareness

68% of mobile users **know** about malware and

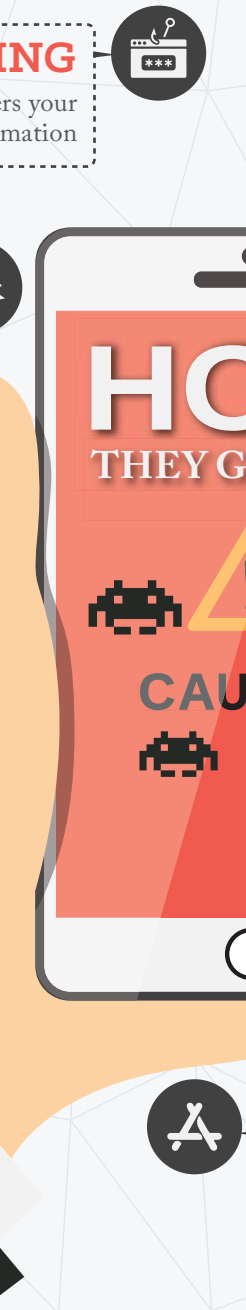
1 in 7 fell **victim** in the past 12 months

Protection

but **89%** have **not** purchased protection for their mobile devices

Opportunity

61% would like to **buy** mobile security services from their service provider



SPYWARE

Silently collects information from users and sends it to eavesdroppers

DIRECT ATTACK

Comes from **files or viruses** sent right to your cell phone.

SMS text messages can contain viruses

Viruses can send requests for **Bluetooth connections** in order to spread.

TROJAN

A program (or app) that seems to be legit, but is really malicious

APP STORES

Copies of legit apps are infected with malicious code and placed in official app stores

THIRD-PARTY ONLINE APPLICATION REPOSITORIES

Unofficial websites where users can freely download applications. They are a general threat since there is no control on what applications are made available

PROTECT YOUR MOBILE DEVICE

53% of users say that they are unaware of security software for smartphone

24% of mobile users bank from a phone, yet most don't have security measures in place.

DO

- Make sure the OS and software are up to date at all times
- Make sure to check the feedback from other users before installing the program from an app store
- Turn off Bluetooth and other connections when not in use
- Download apps from reputable sites and closely review app permission requests
- Use a strong complex password
- Use a personal firewall
- Install a mobile security app

DON'T

- Download apps from third-party application repositories
- Access banking or shopping sites over a public Wi-Fi connection
- Jailbreak your phone
- Leave your Wi-Fi ad-hoc mode
- Leave your mobile device unattended in public places

Two essential security components you should include in your Mobile Enterprise strategy

Tom Lysemose Hansen is on a mission to protect mobile applications from bad actors. Mr. Hansen is CTO of Promon, inventor of the cybersecurity product Promon SHIELD™. "Mobile Enterprise Security is an increasingly important topic, Mr. Hansen said in a recent interview. "Mobile technology has become mainstream, and security technologies are rapidly catching up. Enterprises now need to define their mobile security strategies for the next five years," he emphasized.

Promon's goal is to reduce the risk of data leakage by protecting the apps on mobile devices like smartphones and tablets. Promon SHIELD™ both monitors the operating system and protects software applications on desktop machines, mobiles and IoT devices. The company believes, though, the mid to long-term trend in security for organizations is toward safeguarding against vulnerabilities in the mobile space.

Mr. Hansen sees enterprises continuing to focus on securely enabling the mobile devices their workforces use. Indeed, organizations are looking for more-sophisticated and less-invasive solutions to address a long list of security requirements. "Technologies such as; Application Shielding and Mobile Threat Detection, will be central to this effort," he said. "They will continue to enjoy adoption."

Mobile threats can no longer be ignored.

Gartner has found that 53% of organizations surveyed already had mobile applications in their enterprises, while 40% were planning to deploy them in the future.

Mobile applications pose additional levels of risk since much of the business intelligence, and sometimes intellectual property, resides in the application that is downloaded on the employees mobile device. Further, the enterprises cannot be assured that mobile handset providers will roll out software patches frequently enough to address operating sytems vulnerabilities.

Another concern arises out of a growing trend of hackers to create fake app versions. Hackers can obtain a public copy of a mobile app, reverse engineer it, place malicious code into the app, and redeploy it to the market. Unsuspecting victims then download and use the app, leaving their credentials and personal information exposed to the hackers, including sensitive corporate data such as financials, credit card accounts, patient records, intellectual property, and customer information.

Mr. Hansen explains, "A decade ago, mobile malware was considered a new and unlikely threat. Today, mobile apps are coming under increasing attack – and no enterprise is immune. Malicious actors continue to pump out new and more deceptive malware, and more than 1.5 million new strains of mobile malware have been detected in the first quarter of the year alone."

Mr. Hansen also belives that taking an proactive role in shoring up your mobile enterprise security before an attack strikes, by implementing Application Shielding software and best practices to mobile app development, you can enjoy the treats of mobile security without succumbing to the tricks of digital threats.

How to get ahead of the mobile threats?

As enterprises push ahead with mobile-first strategies – and employee smartphones and tablets increasingly become business tools – the importance of mobile threat detection is growing.

The idea behind Mobile Threat Detection software is for the software to sit in the background and monitor the application and the operating system to identify anomalous behavior. By monitoring the operating system your apps run within, you can determine what is normal and what is abnormal behavior, and what might lead to a malicious attack.

For example, if you have x amount of mobile devices on iOS 11.1 and most of them have very similar types of firmware, but one of them diverges significantly from whats normal, chances are there is a modified library; that modification is abnormal – and it might be done for malicious purposes.

A recent survey also showed that 75% of the surveyed enterprises had an average of 35 jailbroken or rooted devices, a state that leaves devices completely vulnerable to attacks, since the process strips away all built-in security provided by iOS and Android. With application monitoring and detection capabilites in place, your enterprise is in a better position to determine and to set a risk level score for each device the enterprise application runs on.

The financial value and frequency of malicous attacks on mobile devices exceeded that for PCs in 2017 and mobile devices are essentially the new 'backdoor' for cyber-criminals. To proactively combat advanced and presistent mobile threats, Promon believes enterprises should implement in-depth protection and detection that monitors and controls the execution of the application, including the interactions with operating system components, to protect from attacks and data exfiltration. Mr. Hansen explains, " Promon SHIELD™ solution does exactly this and it also provides essential security such as; Obfuscation, Anti-tampering and Integrity Checking, as well as White-box Cryptography and many other security features.

Promon SHIELD™ actively defends applications and more

Runtime Application Self-Protection (RASP) is a security technology that is built or linked into an application or application runtime environment. When the RASP software sees that malware is changing the permissions attached to an application, RASP will modify the activity of the application to ensure the attack is not satisfactory.

Whitebox cryptography dissolves keys into the programming code and obscures algorithms, even at runtime. The technique keeps keys safe even when an attacker has complete access to the device on which the cryptographic functions are executing.

Privilege Escalation detection alerts app custodians whether malware has compromised a device's operating system at the root level. This form of systems subversion is called Jailbreaking or Rooting.

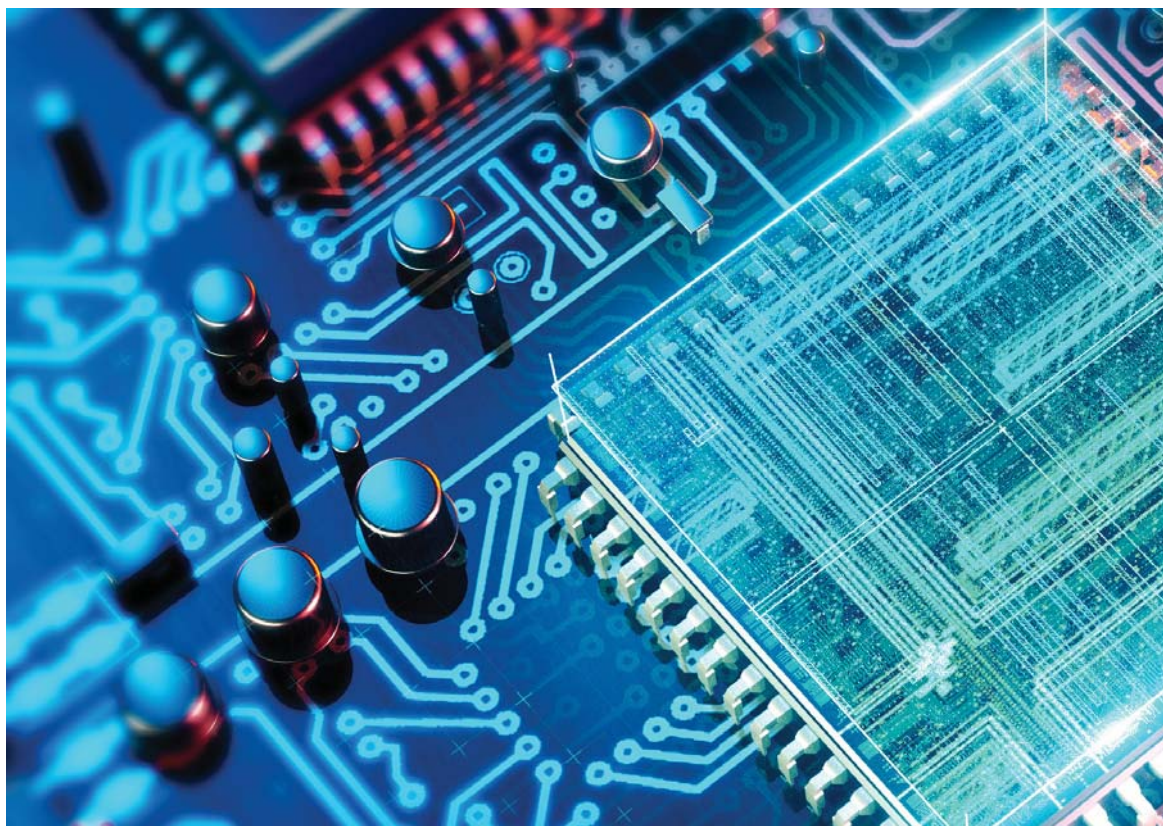
Additionally, **Integrity Checks** can detect whether malware has altered an application. Integrity checks use validations like checksums to ensure apps are secure. They also audit the inventory of libraries and calls included in the software.

Device Binding securely links an authorized user to his device(s). It is crucial for the prevention of cloning or repurposing of cryptographic keys.

Anti-debugging / Emulation detection can identify ongoing attacks to a device. It also protects against the use of debug tools that reverse-engineer applications.

The threat of quantum computing and the emergence of post-quantum PKI

Tomas Gustavsson
Chief Technology Officer and co-founder at PrimeKey Solutions AB



A hot topic in the cryptographic community during the last few years is the discussion on when we can expect quantum computers to be useful. The reason why this is so interesting for cryptographers is that with powerful quantum computers the public-key crypto systems we use today for digital signatures and key exchange are easily breakable. While symmetric key encryption still stands, symmetric encryption keys are typically exchanged using public-key cryptography, meaning that security as we know it on the Internet will start falling apart.

Quantum computers exists today but are so limited that they can not do any real processing and no-body knows for sure when they will be able to break todays algorithms. Estimates range from within 5 years to never.

Post-quantum cryptography to the rescue

With the looming threat about emerging quantum computers, the cryptographic community doesn't sit and wait. Lots of research is done on constructing crypto systems that we can use today, but that will still be secure when quantum computers have arrived. This is called post-quantum cryptography (as opposed to quantum cryptography which is cryptography performed by quantum computers).

Standardization institutes have started looking at standardizing post-quantum algorithms. NIST has started the process by calling for post-quantum algorithm proposals to be standardized, ending in December 2017.

Post-quantum PKI

PKI today relies on the popular, and currently very secure, algorithms RSA and ECDSA. Both these algorithms are thought to be easily breakable by quantum computers, once they are powerful enough. There are already a number of suggested algorithms that are believed to be secure against quantum computers and we have been looking into some of them to find post-quantum digital signature algorithms that might be suitable for use in Public Key Infrastructures today.

What post-quantum digital signature algorithms available today are suitable for digital signing in Public Key Infrastructures? The algorithms looked at so far are hash-based XMSS and SPHINCS, multivariate-based Rainbow and lattice-based BLISS-B. What could be recommended for use today were SPHINCS and possibly BLISS-B.

Changed usage pattern?

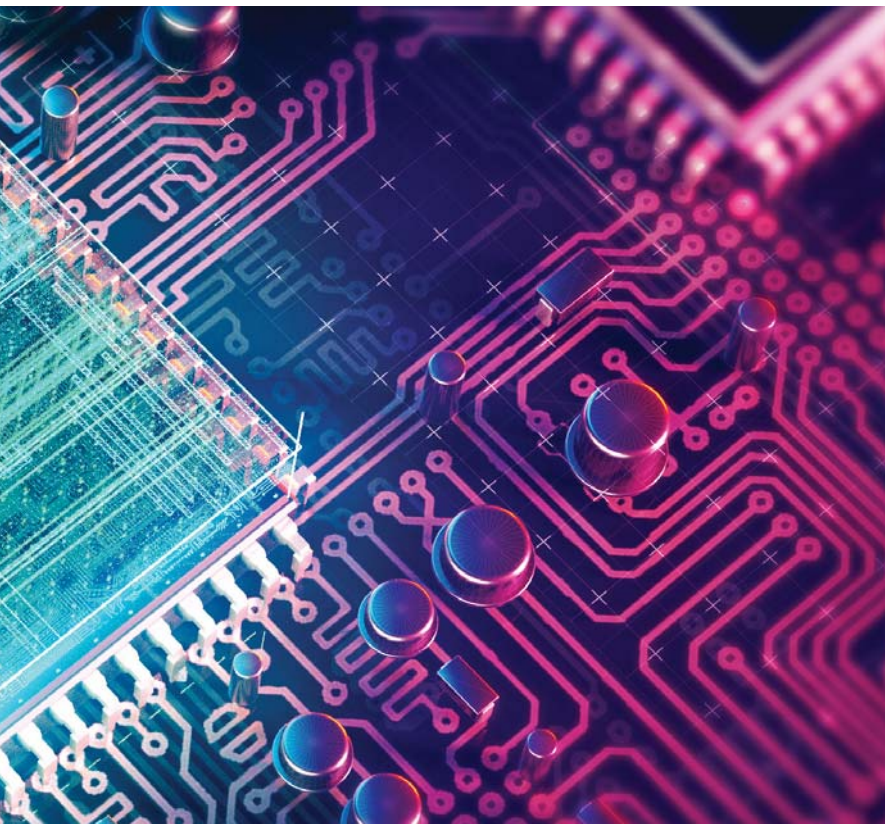
One important thing, at least with todays post-quantum algorithms, is that they are not as general purpose as todays algorithms. This means that usage patterns may need to change into using some algorithms for high security applications,

or long term cryptography, where the algorithms are secure but very slow, and other algorithms for short term security where the algorithms are fast. This is in contrast to today where algorithms are both fast and secure, making them easier to standardize and use.

What is holding us back?

There are a few obstacles to start using post quantum algorithms today.

- Uncertain security levels – the suggested algorithms have not had time to undergo enough research, so we can not yet be confident that they are secure.
- Lack of standardization – without standardization interoperable use in standard applications is impossible, and only specialized custom applications can use the new algorithms.



- Inefficient operations – some of the suggested post quantum algorithms are very inefficient compared to todays algorithms.

Be prepared

For normal users the only thing that we can do currently is to monitor the research going on to know when it is time to start asking questions to vendors, and upgrade our systems. For software and hardware vendors it is important to monitor the landscape and to start preparing applications for a level of cryptographic agility that allows to change to new algorithms once they are standardized and ready to be used.

References

Mikael Sjöberg, Post-quantum algorithms for digital signing in Public Key Infrastructures, Master thesis as KTH and PrimeKey.

SECUREMETRIC JOINED

ISOG Summit 2017: Keep your Information Society Secure

Manila, Philippines - Last July 4-5, 2017, Information Security Officers Group (ISOG) Summit has once again organized an event which highlighted the importance of the role played by the Information Security Professionals in the Information society, held at SMX Aura, Bonifacio Global City, Taguig. ISOG is among the organization formed for the organization in the Philippine IT community.

These two-day event is dedicated on how InfoSec and IT will remain secure against present and future threats. Most delegates who were present during the event were CEOs, CISOs, CIOs, CTOs, Vice-Presidents, Directors, and Heads specializing in Information Security, Cybersecurity, Data Privacy, Data Security, Information Protection, Security Architecture, Risk/Compliance from various industries who would like to have a safe and simpler cyber environment. During the conference, top executives from local and international business shared their insights about the challenges, new trends in technology and how would benefit the industries.

SecureMetric participated in this significant event as an Exhibitor to showcase its products and solution that would help its client to defend them in any digital threats and risks. SecureMetric Philippine team were able to exchange ideas and their perspective in today's digital world.

SECUREMETRIC JOINED

Seamless Philippines 2017: Future of Payments, E-Commerce & Retail

Manila, Philippines – Entrepreneurs, innovators across payment, e-commerce and retail sectors brought together last Sept 26-27, 2017 at SMX Convention Center, Pasay City, for the Philippine's leading event and conference organized by Terrapin, a global events company for over 30 years. Seamless Philippines is Asia's largest and longest running conference focused on a large scale exhibition that is committed to showcasing products, ideas, and innovation to allow new business opportunities and valuable connection.

These two-day event aim to help Filipino business chain to deal with their clients seamlessly especially for the front end e-commerce, retail and business value chain. The conference structure is intended to give extreme flexibility that tackles the entire omni-channel platforms. There are dedicated tracks for payments, retails and e-commerce. During these tracks speakers delved deeper topics such as major challenges facing the banking and payments industries, latest innovation and strategies in both in payments and logistics.

Key speakers from top companies including senior leaders, innovators, and entrepreneurs kindles new ideas and motivates delegates to be creative in handling their business as this year is the most exciting and challenging year for e-commerce, retail, logistics and payments industries. Delegates were privileged to be joined onstage by Guest of Honor, Mr. ChuChi Fonaciere, Deputy Governor from Bangko Sentral ng Pilipinas. He shared his insights on the central bank's response and regulatory framework for promoting innovation. Opening address were delivered by Finlab's mentor Mr. Malikkan Kotadia and Intrepid Ventures Singapore & Hongkong's Co-Founder-Partner, Mr. Zach Peister.

Aside from the conference inside the plenary hall, there were also an on-floor seminars and talks for the visitors within the exhibition. With his intensive experience in digital security, SecureMetric's Regional Sales Manager, Mr. Joshua Chin shared his knowledge, understanding and insightful presentation in protecting business through digital security. SecureMetric Technology was also visible in the event as an exhibitor to unveil its products and solution that are suitable to the developing Philippine market together with over 100 sponsors and exhibitors.

SecureMetric's latest innovation help its clients from the possible cyber-attack which is chronic especially to the business industries whether it's big, medium and small enterprise. As the Southeast Asia's leading regional players in the field of digital security, SecureMetric is committed to providing its client the best and secured products and solutions for their business. SecureMetric has expanded strong local footprints with branches in Indonesia, Singapore, Vietnam and Philippines with core focus in Software Licensing Protection, Two-Factor Authentication, Advanced Identity and Access Management, Public Key Infrastructure and Cryptography.

SECUREMETRIC JOINED

Chamber of Thrift Banks Convention: Maximizing Opportunities in Countryside Development

Manila, Philippines

Last March 14, 2017, Chamber of Thrift Banks once again organized a convention, which focuses on their efforts in helping to enhance further growth for Small and Medium enterprises. The convention was held at Dusit Thani Manila, attended by over two hundred guests from banking and other industries. The event started with ribbon cutting ceremony led by Bangko Sentral ng Pilipinas, Deputy Governor, Mr. Nestor Espenilla Jr., Chamber of Thrift Banks' President, Mr. Gregorio Anonas III and Chamber of Thrift Banks', and Convention Chairman Trustee, Mr. Cecilio San Pedro.

The keynote address was delivered by Hon. Amando Tetangco Jr. Mr. Tetangco is the third and incumbent Governor of the Bangko Sentral ng Pilipinas. He opened his remarks by noting the importance of the theme of the convention. He mentioned that the BSP's major objective is the promotion of economic growth to reach the peripheries through the inclusive financial system. "The timeless and relevance of these efforts have increased as the economy is being primed and thrift banks are positioned to service micro, small and medium enterprises (MSEs) that will benefit from increased development in rural areas", he added.

There were seventeen speakers who discussed various topics including Cyber Security, Philippine Development Plan, Banking Technology for Thrift Banks, Housing, Credit Bureau and MSME's. All delegates who were present during the convention had a chance to express their ideas and asked queries about the topics discussed since there was a panel discussion right after the presentation.

As South East Asia's regional player in the field of digital security, SecureMetric Technology participated in the event as an exhibitor. SecureMetric shared their knowledge and expertise in the world of digital security. They spread awareness on how they can help enterprise in protecting them from cyber-attacks.

SecureMetric offers Software Licensing Protection, Two-Factor Authentication, Advanced Identity and Access Management, Public Key Infrastructure and Cryptography. SecureMetric has expanded a strong local establishment in Indonesia, Singapore, Vietnam and here in the Philippines.

SECUREMETRIC

Won 3 Awards from The Star Outstanding Business Awards (SOBA) 2016

Kuala Lumpur, Malaysia - January 17 2017 marked a meaningful day for SecureMetric, as they received three (3) prestigious awards from The Star Outstanding Business Awards ceremony night.

It was SecureMetric's 2nd year on participating in this annual event. This awarding ceremony is recognized by Malaysian companies that have a significant impact on the growth of the nation and economy.

SecureMetric bagged Platinum Award for the Best Marketing Category, Gold Award for Best Innovation and Silver Award for Best Global Market.

SOBA 2016 awards were presented by guest-of-honour Transport Minister and MCA President, Datuk Seri Liow Tiong Lai, Star Media Group Bhd, Chairman Datuk Fu Ah Kiow and Star Media Group Bhd, Group Managing Director and Chief Executive Officer Datuk Seri Wong Chun Wai.

This day marked a great milestone for SecureMetric and these award meant so much for them since they are stepping into their 10th year anniversary this 2017. SecureMetric hope for another 10 great year to come for SecureMetric.

SECUREMETRIC JOINED

Cyber Security Malaysia Awards, Conference & Exhibition (CSM-ACE 2017)

Kuala Lumpur, Malaysia – SecureMetric Technology participated in the CSM-ACE 2017 last October 10-12 at The Royale Chulan Kuala Lumpur. The CSM-ACE 2017 gathers cyber security industry experts and community to exchange ideas on security management, policy and technology. It is an annual industry gathering organized by CyberSecurity Malaysia, the national cyber security specialist centre under the purview of the Ministry of Science, Technology and Innovation (MOSTI)

This event serves as a platform to increase brand recognition and visibility among Malaysian enterprises and government agencies. SecureMetric Technology was able to market its product and solutions and being acknowledged during the event.

SecureMetric CEO, Mr Edward Law introducing products & solutions to Minister & Deputy Minister of Science, Technology and Innovation (MOSTI), Datuk Seri Panglima Wilfred Madius Tangau & Datuk Wira Dr. Abu Bakar Mohamad Dia.

There were about 200 delegates from various background that had attended the 3 days event. 68 quality leads were generated and 4 were identified to have immediate potential for Centagate Box and other authentication solutions.

The event was a great platform to discover the latest multifactor authentication trends from various sectors and to gather feedback from relevant players in the industry.

SECUREMETRIC

Awarded for Cyber Security Project of the year

Kuala Lumpur, Malaysia – SecureMetric Technology was honored to be part of the significant event held last October 12, 2017 at Royal Chulan, Kuala Lumpur, Malaysia officiated by YB Datuk Seri Panglima Wilfred Madius Tangau, Minister of Science, Technology and Innovation (MOSTI). The Cyber Security Malaysia Awards were created to honor individuals and organizations who contributed to Malaysia's cyber security or information security. The awards were consulted in recognition of their innovativeness, commitment, industry / product / service leadership, and sound business strategies. The Cyber Security Malaysia Awards are intended not only to recognize the efforts of information security professionals, homegrown SMEs and global organizations, but also to encourage innovation and spark strategic alliances within the local security and ICT industry.

Awards were given in six categories: Cyber Security Professional of the year, Cyber Security Company of the year, Cyber Security Outreach Provider of the year, Cyber Security Project of the year, CyberSAFE Professional of the year, Cyber Security Innovation of the year. Nominees for each category were accurately examined by Deloitte and final list were decided by notable panel of judges.

SecureMetric Technology Sdn Bhd has shown exemplary performance in 2017 both local and global and this year they are awarded for the Project of the Year category, the award was assessed based on the criteria which are design and Security Framework, Security Initiatives, Technology & Innovation and Project Deliverables. SecureMetric continues improving their solution to cater their clients digital security needs.

Coming Together. Keeping Together. Working Together as a TEAM.

"If everyone is moving forward together, then success takes care of itself"- Henry Ford

Every group of people working together toward a common goal can create a determined attitude and every successful organization has an enthusiastic approach in working together with other people as a team. In other words, an organization succeeds when team work is great, as defined in business dictionary, Teamwork means that people will try to cooperate, using their individual skills and providing constructive feedback, despite any personal conflict between individuals.

Teamwork is effective in all organization and if you want to have a successful business you have to build a strong team with a good team player to make business work and grow. SecureMetric's top management are also a believer of the power of teamwork, with branches across Asia, they decided to invite all SecureMetric team players for a two-day team building to bond and to establish good relationship.

With the help of SecureMetric (HQ) operations team together with company trip leaders. These two-day team building was a success. Held at A'Famosa Resort in Malacca, Malaysia last October 7-8, 2017, Teamlogue facilitated the activities for SecureMetric.

It was an indeed a fun filled experience with a lot of activities that builds trust, mitigates conflicts, encourages team members to communicate and increases team collaboration. Each team members showed effort, strength, and sincerely collaborating as a team that has a positive impact. This team building aim is for the SecureMetric team players to value teamwork and to understand that the company success is tied on how well the team members work collaboratively to achieve overall goals.