VOLUME 7 2015

Not for Sale

WWW.SECUREMETRIC.COM

SECUREMAG

SECUREMETRIC TECHNOLOGY GROUP

FORMULA FOR STRONG DIGITAL SECURITY

PAGE 10&11

Special Supplements

ASEANFIC
ASEAN Financial Institution Conference

PAGE 6-16

National eID & ePassport Budapest 2014

PAGE 19

Virilicious: The World Of Computer Viruses

This Is Not That Sinister.
You Can Beat Them, With Our Help

BY Krishna Rajagopal | PAGE 6

SecureMetric Wins Best of Security at MSC APICTA Award 2014

CONTINUES ON PAGE 20

PKI in a BOX Launches in South East Asia

KUALA LUMPUR: PKI in a Box launching in CSM-ACE IPOH by YAB DATO SERI DIRAJA DR. Zambry Abdul Kadir

MOU signing during ASEANFIC Manila

MOU signing during ASEANFIC Hanoi

MOU signing during ASEANFIC Jakarta

SecureMetric Technology Editorial Team

Address: SecureMetric Technology
2-2, Incubator 2,
Technology Park Malaysia, Bukit Jalil,
57000 Kuala Lumpur, Malaysia.
Tel: +603 8996 8225
Fax: +603 8996 7225

ASEAN

Philippines' National Science and Technology Week – Welcome to PKI Country

PHILIPPINES: The Department of Science and Technology (DOST) opens the National Science and Technology Week (NSTW) last July 24, 2014. Focusing on government technology, health, education and government e-services and will all come together for one week at the SMX Convention Center, Mall of Asia Complex, With the theme, "Philippines: A Science Nation Meeting Global Challenges," NSTW ran for one week and was definitely filled with remarkable interactive exhibits and technology demos, engineering innovations and audio-visual presentations, and other relevant materials and activities showcasing local expertise and capabilities in science and technology both for professionals and students.

SecureMetric Joins Philippines' National Science and Technology Week.

Cooperation and synergy were at play during the opening ceremonies last July 24 was followed by concurrent forums, on emerging technologies, and on the Philippine National Public Key Infrastructure PNPKI, ASEAN integration in 2015, among others. For the Philippine National PKI, Mr. Denis Villorente, gave an update of the government's e-services and role of the PKI in securing the country's ICT Infrastructure.

The iGovPhil Project and SecureMetric have partnered during the 5-day NSTW event to educate the masses what PKI is. On-hand were the proponents for PKI of iGovPhil Project and SecureMetric Technology Inc, to do a demo in issuing digital certificates on the GovMail of the Philippines and using PKI to preserve their data integrity through PKI encryption.

The digital certificates are part of the Public Key Infrastructure (PKI) designed to make online government transactions and communications safe and secure. The PKI uses public and private keys for encrypting and decrypting data, and digital certificates for authentication of information. Users will be able to access PKI-secured applications and digitally "sign" authenticated files and documents through the certificates.

10th Government electronic ID forum

PHNOM PENH: SecureMetric and Primekey joined 10th Government Discussion Forum on Electronic Identity in Phnom Penh.

Being a PKI Expert in the South East Asia region, SecureMetric participated the 10th Government Discussion Forum on Electronic Identity together with Primekey Solution AB, as the Silver Sponsor of the event.

10th Government Discussion Forum on Electronic Identity was organized by Asia Pacific Smart Card Association (APSCA), and hosted by the Ministry of Interior of the Royal Government of Cambodia. This 2 day forum was held on 11th – 12th December at Sofitel Phnom Penh Phokeethra, Cambodia with the title of "Government eID Evolution: From 1st Generation to 2nd Generation. The forum is for government agencies that issue national electronic identity cards, manage population registers, work with citizens' electronic identities and facilitate the delivery of eGovernment services and benefits to citizens.

The 10th Government Discussion Forum on Electronic Identity was formally opened by H.E. Lt. General Sophana Meach, Advisor (Secretary of State) to Deputy Prime Minister and Minister of Interior, after delivering his opening speech for the forum, and followed by a short tour to the exhibitors and sponsors of the event.

This forum is a targeted high quality delegate from government agencies, professionals and experts in the electronic identity field around Asia and Europe. A Gala dinner was held on the 1st Night of the conference, where the sponsors and delegates are able to meet up while having networking session with local government officers.

10th Government electronic ID forum – Danny listening to delegate's feedback on SecureMetric solutions.

Mr. Konstantin Papaxanthis, CEO & President PrimeKey Group of Companies made his exciting presentation about eID Silkroad on the 2nd day of the conference. At the end of the forum, the Chairman, Asia Pacific Smart Card Association, did a final conclusion and review with takeaways from the 2013 forum.

SecureMetric Technology at RSA Conference Asia Pacific & Japan 2014

SecureMetric Technology at RSA Conference Asia Pacific & Japan 2014 – Danny introducing AEP Keyper DNSSEC HSM to RSA Conference delegate.

SINGAPORE: SecureMetric Technology exhibited at the RSA Conference in Singapore this year. This event was held from 22nd till 23rd July at Marina Bay Sands.

The conference hosted a series of IT security-related workshops and conference tracks attracting industry professionals from all over the globe especially Asia region. RSA plays a key role in keeping security professionals from around the world connected and up to speed with the latest updates in the IT security field. Japanese and Mandarin sessions were offered for the first time.

RSA Conference Asia Pacific & Japan started with the Opening Keynote speech by RSA Executive Chairman Art Coviello, highlighting the security implications of today's digitally interdependent world. Mr Coviello emphasized that society's digital interdependence now requires more effective security measures and greater cooperation.

SecureMetric Technology showcased our newly launched product partnering with Primkey Solutions, Sweden: PKI in a Box. PKI in a Box is an innovative PKI appliance built by experienced PKI experts with the objectives to simplify PKI implementations with complete features.

PKI in a Box received high interest from the visitors at the events with its innovative ideas on implementing the right and safest way of authentication security with ease.

It was great to have our visitor visiting our booth while sharing and discussing security issues and concerns at this event. Thank you again to our visitors and hope to see you again next year.

MALAYSIA

Chief Minister of Perak Darul Ridzuan Launches PKI In A Box

SecureMetric's Chief Business Development officer, Mr. Lim Chin Wan explaining how the PKI In A Box works.

It was a busy day at the Cybersecurity Malaysia Awards, Conference and Exhibition event in Ipoh, Perak.

IPOH: Chief Minister of the Great State of Perak Darul Ridzuan, YAB DATO' SERI DIRAJA DR. Zambry Abdul Kadir, today visited SecureMetric's booth at the Cybersecurity Malaysia Awards, Conference and Exhibition (CSM-ACE) and launched SecureMetric's latest innovation, the PKI In A Box. This officially puts SecureMetric as the PKI solution leader in the ASEAN region.

The CSM-ACE event started with a walkabout by the Chief Minister. When he reached SecureMetric's exhibition booth, he was intrigued by the display of PKI In A Box. SecureMetric's Chief Business Development Officer, Chin Wan, explained that the PKI In A Box is a joint development between SecureMetric from Malaysia, PrimeKey from Sweden and Utimaco from Germany. The Chief Minister was duly impressed that the development of PKI In A Box was conceptualised and made into a product for market in less than 2 years.

In a typical PKI implementation, the setup for a Certificate Authority (CA) is very complex. A mid-size CA would usually requires an implementation of more than 20 servers, 6 HSMs and multiple PKI device management system. With PKI In A Box, SecureMetric, together with its partners have shrunk down the implementation size to only one 2U server. This has made the cost of implementation to come down by more than 500%. In addition to lowering the cost, the implementation time for PKI In A Box compared to a typical CA implementation is reduced from months to weeks.

One of PKI In A Box's key success factor is its ease of use. The user-friendly user interface, coupled with its wizard style setup process, SecureMetric's customer can now set up the PKI In A Box in less than one week. This has helped make PKI more acceptable in this region. SecureMetric understands that one of the main barriers to PKI usage in ASEAN is the ease of use. This has always been our goal, to make PKI more acceptable in ASEAN. With PKI In A Box, SecureMetric has achieved the goal of making PKI a more acceptable solution.

PKI In A Box also won the Best of Security product in the APICTA 2014 Awards. Asia Pacific ICT Alliance (APICTA) Awards, under the patronage of the Prime Minister of Malaysia, provides a platform to stimulate creativity, innovation and excellence in ICT in Malaysia, benchmark Malaysian ICT products and solutions, and to recognise outstanding achievements in ICT of students, technopreneurs, SMEs and organisations with operations in Malaysia.

This annual Awards Program initiated in 1999 by the Multimedia Development Corporation, has evolved from being known as the Asia Pacific MSC IT & Telecommunications Awards (APMITTA) to MSC-Asia Pacific ICT Awards (MSC-APICTA) in 2002 when the international Awards Program, APICTA, was launched.

SecureMetric has been doing a multiple roadshow around ASEAN; namely Indonesia, Vietnam, Philippines and Myanmar, to launch PKI-In-A-Box. With the signing of the PKI In A Box plaque by the Chief Minister, PKI In A Box is officially launched in the ASEAN market.

PKI in a Box

PKI in a Box is an innovative Public Key Infrastructure (PKI) appliance built by a team of highly experienced PKI and Cryptography experts with the objective to simplify PKI implementation with complete feature set needed to operate a full-blown PKI out of the box. It includes a complete Certificate and Hardware Token Lifecycle Management System; can support unlimited number of Certificate Authorities (CAs) and/or subordinate CAs; Registration Authority (RA) either via centralized or distributed RA model; and a Validation Authority (VA) that supports both Certificate Revocation List (CRL) and Online Certificate Status Protocol; Server Signer to support XML and PDF signing with common Time-stamping functionalities (coming soon); with integrated Hardware Security Module (HSM) onboard.

What PKI IN A BOX Can do?

- SSL Certificates for Server Authentication
- Email Signing
- VPN Server Authentication
- Document Signing
- Digital Signing
- Code Signing
- End User Client Authentication for 3rd Party Applications
- Digital Time Stamping

SecureMetric & Primekey

- The Only PrimeKey's Certified Trainer and Exclusive Partner for Asia
- Joint development experience with PrimeKey's R&D
- Lower project costs by leveraging on SM cost advantage
- Dedicated local technical support
- Complement PrimeKey's offer with Token Management System, Distributed RA System, HSM, PKI devices and digital signature solutions.

ASEAN

SecureMetric Opens Representative Office in Yangon, Myanmar

MYANMAR: Yangon, 4th September 2014. Minglabar! In line with SecureMetric's vision of ONE ASEAN NETWORK, SecureMetric opens its representative office in Yangon, Myanmar. Having secured multiple projects, including 2 of the Top 5 Banks in Myanmar, SecureMetric is committed to provide its customers in Myanmar with top quality local support.

SecureMetric with the support from its local partner in Yangon, Myanma Computer Company Inc., opened its local rep office with the following contact details:

3rd Floor, Building (8), Junction Square,
Pyay Road, Kamaryut Township,
Yangon, Myanmar
Tel: 951 2304155
Fax: 951 2304155

With this new office expansion, SecureMetric is now able to serve its customer better with shorter response time. SecureMetric is focusing it effort to promote the following products in Myanmar:

Public Key Infrastructure (PKI) including digital signature, authentication and encryption
One Time Password (OTP)
Hardware Security Module (HSM)
Security Posture Assessment (SPA)
Digital Security Services (Training, Forensic Investigation)

Finally, SecureMetric would like to thank our customers and partners in Myanmar for their strong support. We hope to be able to serve you better with our local support team and that we can grow together in the Myanmar market.

SoftCon.PH 2014 – Hotel Intercontinental, Makati, Philippines

PHILIPPINES: PSIA or the Philippine Software Industry Association organized SoftCon.PH 2014 brings together the country's top executives and decision makers in a one day, action packed event that tackles the issues we face in the software and IT industry today. Learn about the timelines and the AEC rules of engagement and how we can take advantage of the opportunities the ASEAN integration will bring; find out the impact on global and regional sourcing of technology and support services and how this will impact in the Philippines and wider ASEAN; tackle issues in the kind of talent we employ - a remote and mobile workforce, free lancers/consultants, geographically dispersed project teams; and discover how companies of all sizes can use "Lean Innovation" as a proven framework for developing new products and services.

Held at the Hotel Intercontinental, in Makati City Philippines, situated at the top commercial business districts in the Philippines, the hotel itself gave the ambience of synergy for the conference to be successful.

Starting the morning of the conference is ICTO Executive Director Monchito Ibrahim gave a speech on The Technology of the Roadmap of the Philippines wherein he introduced the platforms for e-government services for the next 5 years. He gave a short history on the security platforms being undertaken by Philippine government which he gave special mention to SecureMetric Technology Inc. who implemented the country's CA for securing their platforms for e-government services.

Other forums were held discussion focused for the Philippines on Competing with the ASEAN Community, where in what will impact the Filipinos and Philippine Businesses. Also, this became an avenue in learning how to thrive and take advantage of the coming opportunities for software providers.

Topics discussed during the day were IT Entrepreneurship – Creating Value for the Greater Good, panelists showcased some of the start-up IT companies and their apps in which has generated value for the economy and society. This also benefits the larger IT eco-system and had suggestions from SME's on how large companies can help in the achievement of the greater good in the IT Industry.

Participants got also involved in the fun game of scanning the QR Code and answer questions and got around to all exhibitors during the event. Before the closing, they were giving prizes for their efforts such as phones and tablets.

Final announcement was also made that there will be another tour of the SoftCon.Ph event to be held on September 2015.

SecureMetric at SoftCon.PH 2014 – Hotel Intercontinental, Makati, Philippines.

SecureMetric product showcase during the SoftCon.PH 2014.

SecureMetric Technology at SoftCon.PH 2014 – Hotel Intercontinental, Makati, Philippines
Bryan introducing SecureMetric products to Conference delegate.

MALAYSIA

SecureMetric ST3 ACE Received Common Criteria EAL2 Certification

29th December 2013

KUALA LUMPUR: Globally Trusted Security Certification Further Reflects SecureMetric's Commitment to Government and Enterprise Customers.

As a South East Asia leading digital security provider, SecureMetric is proud to announce that the company's ST3Ace Security Token firmware has received certification for Common Criteria Evaluation Assurance Level 2 awarded from Cyber Security Malaysia. As a digital security pioneer and innovator in Malaysia, SecureMetric leads the industry with globally trusted certifications and products that consistently meet the stringent requirements and standards set by international professionals and organizations.

The Common Criteria certification process provides a third-party evaluation service for determining the trustworthiness of information technology security products, which is fundamentally important to the company's enterprise and government customers. Extensive testing activities involve a broad and formally repeatable process, confirming that the security product functions as claimed by the manufacturer. Security weaknesses and potential vulnerabilities are specifically examined during the evaluation.

"Common Criteria certification is critical to the success of our large enterprise and government customers, and it's our big step to move forward internationally." said Edward Law, CEO of SecureMetric. "This latest EAL 2 certification validates our technology innovation and continued drive to lead the industry and produce and develop higher and better security products."

The Common Criteria for IT Security Evaluations was developed by the national security organizations of the United States, Canada, the United Kingdom, France, Germany and The Netherlands. It offers a broad range of evaluation criteria for many types of commercial and nationally sensitive government-use IT security products.

SecureMetric USB Based Products Are Not Affected By BadUSB Vulnerability

14th October 2014

On the 7th of August 2014 at the Black Hat 2014, German security firm Security Research (SR) Labs revealed one of the first USB vulnerabilities known as BadUSB where this malware is designed to attack the device itself instead of the data on the device.

This means that this malware is capable of reprogramming the entire USB where this infected device now can be malicious in many ways:

> 1. A device can emulate a keyboard and issue commands on behalf of the logged-in user, for example to exfiltrate files or install malware. Such malware, in turn, can infect the controller chips of other USB devices connected to the computer.
> 2. The device can also spoof a network card and change the computer's DNS setting to redirect traffic.
> 3. A modified thumb drive or external hard disk can – when it detects that the computer is starting up – boot a small virus, which infects the computer's operating system prior to boot.
>
> Taken from SR Labs official blog

Why are we not affected?

SecureMetric has always been following the best practice of updating firmware.

This means that not only firmware updating of our tokens and dongles are done in a controlled manner, our firmware update process is also protected with encryption key that eliminates access from any unauthorized person.

Any tampering of information during the firmware update process will be detected during our cryptographic operations.

Therefore, we are confident to announce that our PKI Token and Dongle products are not affected by this attack.

Security Advisory Regarding Heartbleed OpenSSL Vulnerability

14th April 2014

Certainly many of you likely read about the Heartbleed vulnerability that has affected much of the Internet. On Monday April 7th, security researchers reported the so-called Heartbleed bug in OpenSSL, which is a cryptographic library implementing the SSL/TLS security protocol.

What is the Heartbleed bug?

The Heartbleed Bug is vulnerability in the OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS is widely used to protect communication via websites, e-mail, instant messaging, etc.

The Heartbleed bug allows an adversary on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content, which in turn allows attackers to eavesdrop on communications and impersonate servers.

What versions of the OpenSSL are affected?

Status of different versions:

- OpenSSL 1.0.1 through 1.0.1f (inclusive) are vulnerable
- OpenSSL 1.0.1g is NOT vulnerable
- OpenSSL 1.0.0 branch is NOT vulnerable
- OpenSSL 0.9.8 branch is NOT vulnerable

Does it affect SecureMetric PKI products?

SecureMetric PKI products SecureCA and TMS-RA are not affected by this vulnerability, and does not use or link with OpenSSL. In the case of if you deployed an Apache server as front end to SecureCA and TMS-RA, you should look into this vulnerability closer. By the nature of the vulnerability makes an attack difficult to detect, therefore you can take a cautious approach as following.

- Verify OpenSSL version on apache server
- Update OpenSSL on all HTTPS endpoints and restart all services (If it is affected version)
- Re-issue all SSL certificates using new signing keys

ASEANFIC
ASEAN Financial Institution Conference

Special Supplements

PKI in a Box

Introduced at

ASEANFIC
ASEAN Financial Institution Conference
Hanoi 2014

HANOI: With the support of MSC Malaysia again this year, SecureMetric Technology organized the ASEANFIC 8th edition at Hanoi on 18th June 2014 at Pullman Hotel, Hanoi. Participants from all over the Financial Institutions gathered to take part on the conference. The event was an accomplishment, with more than 120 delegates gathered to exchange knowledge, collaborate, network and enjoy.

With a pleasant opening speech from the Chairman of ASEANFIC, Mr. Lim Chin Wan, the event was welcomed with smiles on everyone's faces. PKI Appliance PKI in a Box have its official launched with the signing of the Memorandum of Understanding (MoU) between SecureMetric Technology's CEO, Edward Law and Primkey Solution AB's CEO, Mr. Tomas Gustavsson.

The 8th edition of ASEANFIC has its first panel discussion of PKI Usage in Banks. Mr. Lim Chin Wan moderated this panel, with CEO of SecureMetric, Mr. Edward Law, CEO of Primekey Solution AB, Mr Tomas Gustavsson, and International Sales Manager of UTIMACO, Mr. Joerg Horn. This panel discussion attracts the attention from the delegates. Good questions were asked by the delegates to understand the usage and importance of PKI security that can help the banks and financial institution to excel and improve on their security system.

The success of this edition is not going to be possible without the help of our partners namely Epic Malaysia for Mobile Branchless Banking, PrimeKey Solutions AB for Public Key Infrastructure (PKI), Aetins for Insurance System, Cyber Security for Common Criteria Awareness in the Banking Industry and UTIMACO for hardware security module.

A simple cocktail session was organized to conclude the conference to celebrate another success of the edition. Everyone was enjoyed with the foods and beers arranged and served. A big smile and joy was marked on everyone's face at the end of the cocktail party with lucky draw prizes given out to the winners.

ASEANFIC
ASEAN Financial Institution Conference
Yangon 2014

6th Edition ASEANFIC Yangon 2014 Kicks Off The 2014 Road Show

MYANMAR: The 6th Edition ASEANFIC was held in Yangon, Myanmar on the 5th March 2014. The organising committee and our local host, Myanmar Computer Company Ltd. (MCC) welcomed delegates from banks, insurance company and government agencies with some excellent coffee and tea served in Parkroyal Hotel Yangon.

The event started with a welcoming speech by MCC's Director, Brian Aung Soe Lin. We then started the conference with a keynote topic presented by Chief Inspector Major Jay Guillermo from the Phillipines National Police Anti-Cybercrime Unit. Major Jay spoke about the cybercrime situation in the Philippines as well as how the Philippines National Police cooperates with Interpol and police forces from around the world to tackle the growing cybercrime scene. Present to listen to the talk was the Myanmar Police Force from the Anti-Money Laundering Unit.

Presentation topics were focused on Banking IT Security as well as in the Internet Banking deployment. ASEANFIC partners from across Southeast Asia namely, Malaysia, Indonesia, Philippines, and Singapore attended the event. The most popular topic were on how cybercrime affects the confidence of bank users especially in Mobile Banking and Internet Banking.

Another interesting topic which got a lot of questions from the floor was the use of cheque. ASEANFIC partner, InsiteMY who presented the topic, "The Rold of Cheque Payment in the Modern World" went on to explain how cheques were a unique payment instrument which offers features that no other modern payment instrument can offer. A new subject was also introduce this year. The insurance industry in Myanmar is booming so ASEANFIC partner Aetins spoke about how adapting technology for the insurance industry can help encourage more people to purchase insurance which in the end is a WIN-WIN situation.

The event ended with a cocktail session where delegates and partners were given a chance to network and get to know each other more. The cocktail session is when the lucky draw session was done. This year, ASEANFIC added more lucky draw prizes. All the delegates enjoyed the conference and went home happy.

ASEANFIC
ASEAN Financial Institution Conference
Jakarta 2014

9th Edition ASEANFIC Jakarta 2014

INDONESIA: ASEANFIC organized its 9th edition in Jakarta Indonesia again on Wednesday, 19th Auguest 2014. ASEANFIC came back to Jakarta with co-host PT Dymar Jaya choosing the prestige Mulia Hotel as our venue of the event.

ASEANFIC Jakarta successfully accommodated 120 guess and delegates from Banks Insurance companies, and other financial institution. The event started with a warm welcome speech from the Chairman of ASEANFIC, Mr. Lim Chin Wan, followed by an opening remark from Ms. Yuliani Kusnadi, Managing Director of Dymar Jaya.

In conjunction with ASEANFIC Jakarta, SecureMetric launched PKI in a Box together along with Mr. Edward Law CEO of SecureMetric and Mr. Bjorn Jansen, signing a memorandum of understanding for the launching of this product in Indonesia.

Mr. Ami Azrul Abdullah, General Manager of Scan Associates Berhad Malaysia presented the first keynote about the Needs of PKI for Banks Transactions. The presentation is informative and captured the eyes of all delegates on the needs of PKI. Mr. Lim Chin Wan and Mr. Bjorn Jansen also presented on the topic regarding PKI on showing how banks and other financial institutions can benefit on using PKI.

ASEANFIC Jakarta is rather different this year with a panel discussion with the 3 PKI expert on the stage, Mr. Bjorn Jansen, Sales Manager from Primekey, Mr. Ami Azrul Abdullah, General Manager of Scan Associates Berhad Malaysia, and Mr. Edward Law, CEO of SecureMetric. Mr. Lim Chin Wan moderated the panel discussion and received lots of feedback and questions from the floor. It was interactive and good discussion.

Mr. Ravindra Mohan from Aetins, Mr. Kenny Lee from Epic Malaysia, Dr. Solahuddin from Cyber Security Malaysia, Mr. Satish S. S., from Tess International, and Pak Hazairin from PT Praisindo Technologi presented their interesting topics to the floor. Together with keynote speaker Chief Inspector Major Jay D Guillermo, Chief, Intelligence and Investigation, Anti Cybercrime Operations and Training Division Philippines have done a great job on capturing the attention of the guests on their interesting presentations.

ASEANFIC Jakarta 2014 ended with a cocktail with lucky draw. Everyone was in joy especially the ones who got the iPads and iPhones as their lucky draw prices. Most of them stayed mingling and talking with the partners on possible or potential projects. Again ASEANFIC Jakarta achieves another successful event this year.

Special Supplements

ASEANFIC ASEAN Financial Institution Conference

MANILA: SecureMetric Technology with the support of MSC Malaysia organized the 7th ASEANFIC on April 29, 2014 at the Makati Shangri-La Hotel. Participants from all over the Financial Institutions in the Philippines gathered to take part on the conference. The event was an accomplishment, with more than 130 delegates gathered to exchange knowledge, collaborate, network and enjoy.

ASEANFIC's intention is to establish a highly effective knowledge sharing and industrial focus business networking event across the region. One of the most important attribute about ASEANFIC is high level of industry expert speakers from Europe and South East Asia bringing in their A-Level presentations.

With a delightful opening speech from SecureMetric Technology's Chief Business Development Officer, Mr. Lim Chin Wan, the event started with a big smile on everybody's face. To follow the opening act, a key ceremony transpired, it is now time to introduce the PKI Appliance in the Philippines. PKI Appliance was launched in the Philippines with the Memorandum of Understanding (MoU) between SecureMetric Technology's CEO, Edward Law and Primkey Solution AB's Vice President for Sales, Björn Jensen. The signing was witnessed by PNP's (Philippine National Police) Chief Inspector Jay Guillermo of the Anti-Cyber Crime Group and by MSC Malaysia's Head of Business Development, Mr. Rajen Dorairaj.

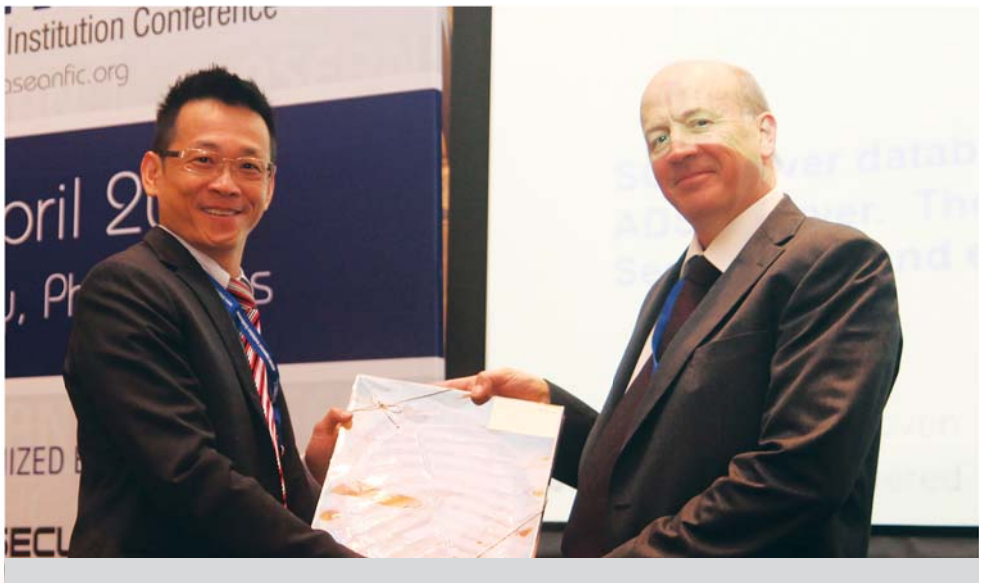
The signing followed an interview with Edward Law, Björn Jensen together with (Department of Science and Technology) DOST – (Advanced Science and Technology Institute) ASTI's Knowledge Management Division Chief, Rene Mendoza by the Local Media. Reporter's interest and enthusiasm were shown by the two hours session that surprised even the media themselves. The media interest was highlighted by article published by PNA (Philippine News Agency), PhilippineStar and more.

The PKI Appliance Launch was perfect inauguration to fire up the delegates inquisitive minds. From then on, the Bankers were all focused on listening, acquiring new knowledge and being interactive with each topic presented. Questions and inquiries were overflowing, especially during coffee break and lunch time wherein partners across the region were full of activity answering queries from guests in the banking industry. With everybody busy networking and collaborating, lunch time was even extended as we've seen that every person around are still having fun eating and getting to know each other.

The top 3 topics that a caught our audience attention was "Compliance – The Art of Living" by Mr Satish of Tess International, "Mobile Money in Social Development" by Dr. Supriya Singh of RMIT University and lastly "What the Hack? Inside A Hackers Mind" by Mr. Rajagopal, he was the last to present but definitely not the least as everyone was all amazed and stunned after he did an actual hacking demonstration.

The success of this edition is not going to be possible without the help of our partners namely Epic Malaysia for Mobile Branchless Banking, PrimeKey Solutions AB for Public Key Infrastructure (PKI), Ascertia Pte. Ltd for Digital Signature, Tess International for AML System, PT Aprisma for Corporate Internet, and Mobile Banking, Cyber Security for Common Criteria Awareness in the Banking Industry and Akati for the Penetration Testing.

To conclude the conference, an after event cocktail session was held at the Sage Tapas Bar to celebrate another successful edition of ASEANFIC. Together with the partners and delegates across the banking industry, everyone relished the relaxing ambiance of the cocktail hall. Everybody's attentions were all captured when Mr. Edward Law started to draw the prizes that were given away. The event started and ended with an interest, a big smile and joy on everybody's face. ASEANFIC Manila Edition received a positive response that delegates were looking forward to 2015 edition.



Rod Crook from Ascertia UK receiving ASEANFIC souvenir after his exhilarating talk on digital signature.

Delegates paying close attention at the ASEANFIC 2014 Manila.

Professor Supriya from RMIT Australia wrapping up her talk about Mobile Money and the Philippines market.

Anti-Money Laundering is one of the hottest topic in ASEANFIC 2014 Manila.

ASEANFIC
ASEAN Financial Institution Conference

Special Supplements

ASEANFIC
ASEAN Financial Institution Conference
Manila 2014

Manila, Philippines
Makati Shangri La Hotel
29th April 2014

1 Branchless banking expert, Mr. Viraj Mudalige from EPIC Malaysia receiving event souvenir from SecureMetric's CEO.

2 Bankers at the ASEANFIC 2014 Manila are listening to the presentation from Mr. Rod Crook that relates about document signing.

3 Erin from Aprisma explaining to delegates about Internet Banking and the Philippines Banking Market.

ASEANFIC
ASEAN Financial Institution Conference
Hanoi 2014

Hanoi, Vietnam
Pullman Hanoi Hotel
18th June 2014

4 Insurance industry expert, Mr. Ravindra Mohan from Aetins talked about the future of the Insurance industry in Vietnam.

5 One of the winners of the Samsung Note 3 smart phone. Congratulations!

6 Press conference at ASEANFIC 2014 Hanoi. Both SecureMetric CEO, Mr. Edward Law and PrimeKey CEO, Mr. Tomas Gustavsson answered questions from the press.

7 SecureMetric's Chin Wan giving a talk about Internet Banking security.

8 Mr. Viraj Mudalige from EPIC Malaysia explains about the advantage of Branchless Banking.

9 Mr. Joerg Horn from Utimaco Germany discussed the importance of HSM in the banking industry.

Special Supplements

ASEANFIC ASEAN Financial Institution Conference

ASEANFIC ASEAN Financial Institution Conference Yangon 2014

Yangon, Myanmar
ParkRoyal Yangon
5th March 2014

1 The 6th Edition ASEANFIC was held in Yangon, Myanmar on the 5th March 2014. The organising committee and our local host, Myanmar Computer Company Ltd. (MCC).

2 Mr. Brian Aung Soe Lin, CEO of MCC ICT Services welcoming all the bankers to the 6th edition of ASEANFIC.

3 Mr. Navin Vasdave from Cyber Intelligence receiving souvenir from MCC.

4 Bankers arriving at the ASEANFIC 2014 Yangon event.

5 Pak Hafiz from Bank Jatim Indonesia introducing MCC Chairman to Dr. Solahuddin Bin Shamsuddin, CTO of Cybersecurity Malaysia.

6 InsiteMY COO, Mr. Robin Hoo getting to know the bankers from Yangon.

ASEANFIC ASEAN Financial Institution Conference Jakarta 2014

Jakarta, Indonesia
Mulia Hotel Jakarta
19th August 2014

7 Bankers from around Jakarta getting ready for ASEANFIC 2014 Jakarta to start.

8 TESS International's VP, Mr. Satish S.S talks about Anti-Money Laundering.

9 SecureMetric CEO, Mr. Edward Law having a discussion with delegate from Intikom Indonesia.

10 Cybersecurity Malaysia CTO, Dr. Solahuddin Bin Shamsuddin, explaining about Common Criteria Certification, MyCC.

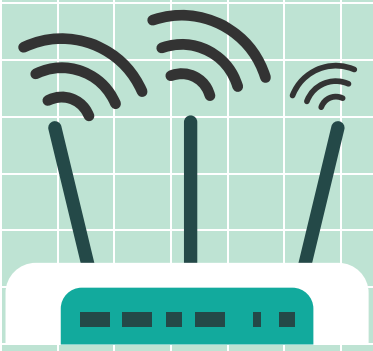
11 Local host, Dymar Jaya and delegate bankers having talk & networking during the coffee break session.

12 Highly engaging Panel discussion on the usage of PKI in the banking industry.

The Dangers of FREE WIFI

FREE WIFI network "HOTSPOTS" are easy to access and easy to hack!

Wi Fi HOTSPOT

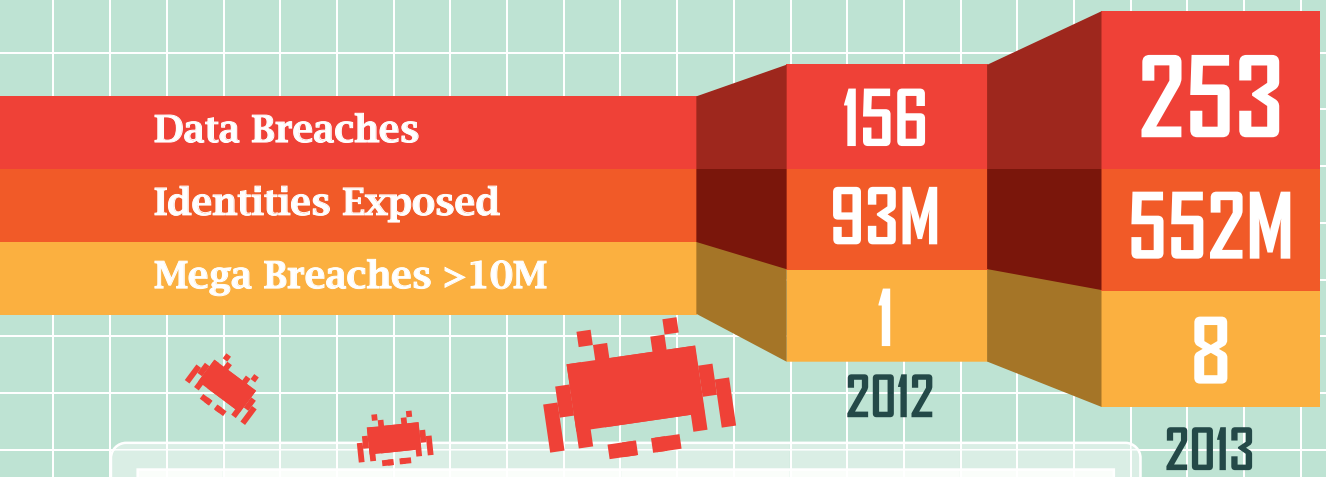


64% of those who use an unsecured wireless networks say they have little to no concern about using them

BUT UNSECURED WIFI HOTSPOTS IS ONE OF THE LEADING SOURCES OF IDENTITY THEFT!

2013 Year of the Mega Breach

the total number of breaches in 2013 was **62%** greater than in 2012



EACH OF THE EIGHT TOP DATA BREACHES IN 2013 RESULTED IN THE LOSS OF TENS OF MILLIONS OF DATA RECORDS

Widespread Corporate IT Threats

- **Malware Attacks** 61%
- **Vulnerabilities** 40%
- **Accidental Data Leaks** 35%
- **Phishing Attacks** 35%
- **Network Intrusion** 23%
- **Targeted Attacks** 8%

Today. 35% of online users around the world do not feel safe from cyber crime attacks while online.

compared to 4% in 2010. Are you among this group?

Malware for Every Device

PC

200 000 New Malware Samples Daily***

The most dangerous threats:

- Banking Trojans
- Ransomware
- Rootkits

MAC

700 000+ Macs Were Infected With Flashback Malware**

The most dangerous threats:

- Phishing Sites
- Fake AVs
- Spyware

Phone Tablet

99% Of All Mobile Malware Is For Android***

The most dangerous threats:

- SMS-senders
- Mobile Banking Trojans
- Malicious Apps on Google Play

Ways to Minimize Your Risks

1 Choose Strong, Unique Password

Using numbers, symbols and mixed-case letters increase the difficulty or cracking your password

2 Enable 2-Step Verification on Password

The user enrolls in 2-step verification and selects the method for receiving their verification code on their device via text, phone call or app

3 Always Update Your Operating System

Most desktop security incidents are centered around flaws in the operating system. As these flaws are discovered, vendors release patches to cover these security holes

4 Avoid Suspicious Emails and Offers

Use email software with built-in spam filtering . Spam is any kind of email that you don't want and that you didn't sign up to receive.

5 Regularly Scan for Viruses

Run a complete virus and malware scan on your entire computer

**By"Devices,"we are refferring to larger portable electronics, not charges or accessories. data displayed is from a Naked Security Survery" How do you compare to Steve Wozniak?" conducted in January 2013 of 2,226 respondents*
***According to B2B International Survery, April 2013*
****According to Kaspersky Security Network*

Source:
https://nakedsecurity.sophos.com/2013/03/14/devices-wozniak-infographic/
http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf
http://media.kaspersky.com/en/Attack_and_defense.png
http://media.kaspersky.com/en/kaspersky-lab-infographics-multi-security-for-multi-devices.jpg
http://programs.online.utica.edu/infographics/cybersafe-internet-security-infographic.asp
http://www.gryffin.com/mobile-security-infestation

CYBERSAFE INFOGRAPHIC

How Many Device Do You Carry?

85%

The Smartphone is by far the most popular device carried...

65%

48%

The Average Person carries **2.9** Devices*

Most Popular Smartphone By OS

40.9% 40.5% 8.9% 3.4%

Android beats iPhone by only a whicker, outstripping Windows and the old business favorite Blackberry

Windows is the leading laptop OS carried twice as popular as MAC and six times more than Linux

22% 49% 8%

VIRILICIOUS: THE WORLD OF COMPUTER VIRUSES

by Krishna Rajagopal

I. Background

In the beginning, God made virus, and soon after man made.. computer virus. The former is a very simple cell which does not have the capacity to multiply on its own, like its more powerful counterparts. But boy, when they attach themselves to a host cell, they can use the host's power for their own benefit. Not only do they propagate throughout the host cell's body, but also attack other host bodies - and in a short time creates an epidemic. The result can be as insipid as a common cold, or as deadly as AIDS or Ebola.

The Computer Virus exhibits similar properties. Indeed, the first people who wrote these malicious code must have been inspired by the biological counterpart while christening them "Virus". Right from the very first - the CREEPER virus that created havoc on the ARPANET (a US military computer network) that spread itself through a modem, and displaying " I'M THE CREEPER: CATCH ME IF YOU CAN" when infected, to the latest PEACOMM virus that infected 1.7 million computers before it could be brought under control, the journey has been a long one for both the Evil and Samaritan.

Virilicious, the world of the computer viruses is like the dark, demonic world that the protagonist in Harry Potter's movies is time and time again thrown into! And while it has been the cause of sleepless nights and increased stress levels for thousands of MIS managers and system administrators, it has also helped mankind in a convoluted way by creating jobs in the form of an entire computer security industry: witness the army of anti-virus programmers who now lead happy lives and take home some decent pay checks, thanks to the business that comes their company's way due to the perceived threats! Interesting eh ?

II. What Motivates Them?

Viruses and all other forms of malware are the biggest threats to computer security in today's age of internet-is-everywhere and I'm-always-connected world. So what are these virus writers really made of? What motivates them to write malicious code that can decapitate and main computers, wipe off the entire Gringott's Bank treasury, and even potentially trigger off wars?

The physical appearance of any member of this tribe is far removed from the Satan-like persona pictured by the antagonist of the Harry Potter movies.
Imagine this.. you're sitting down in your favorite coffee house. Notice that guy or gal sitting at the table next to you, quietly sipping on his/her latte? For all you know, he/she must have just risen from his or her attic desk after unleashing the latest strain onto the unsuspecting world, and the latte is their way of celebration! How's that ?

But seriously Krishna, what motivates these people? Asked one of my students in my class once. There was a time when the only reason a programmer would do it was to impress peers and draw attention to self. But that was long ago. Even now, this particular motive seems to be one of the drivers. The sight of newspapers and the TV channels across continents screaming hoarse about entire systems having crippled because some new virus got loose, the millions of words written by blog writers and tech editors speculating how fast an antidote can be found - all these must give these programmers the ultimate kick.

If we were to quickly go over the behavioral characteristics of these individuals who do it for anything other than money, then a brief list that emerges is as follows:

Hobby
Curiosity
Having fun

Continues Next Page >>

Avenging the world for some wrongdoing (Hacktivism)

The virus coders of today with their eyes on the moolah are very savvy indeed. He/she may be self-driven, or may be hired by someone else with their own hidden agenda of wrecking havoc in the world, and benefiting from the havoc. From my experience as a computer forensics investigator, I have ran across many examples of such corporate espionage incidents.

And what could the agenda be? Ah, there is a wide range:

- Denying users access to a company's website (the company's competitor – corporate espionage, or a ransom-seeker might typically pay for this job),

- Using the infected computers as Zombies to send out spam mails (and thus conduct a very effective "sales" campaign). Don't be surprised if your very own computer turns up in a list on an EBay auction, put up by Zombie-creators to be sold to the highest bidder!

- Using the infected computers to steal personal data such as credit card numbers (with their three-digit cvs pins, thank you), social security information, pay-pal account information, online banking passwords, maybe even some launch codes to a number of ballistic intercontinental nuclear missiles ? The latter , of course was an example of a true incident that happened to a premier of a well-developed nation around May 2005.

The list above ,of course goes on and on.

III. Creating A Virus: The How

There was a time, in the age of innocence, when all the virus writer had to do was to add their malicious code at the beginning or at the end of the (host) program. This was done by altering the File / Disk Allocation Table such that the program call begins with the first instruction of the viral code. An additional, crafty, step would be to remember the program's original date-time stamp and retain it after the virus latches itself to the program.

These programs would typically reside in the boot sectors, or were system softwares that users typically ran. The spread to user-created commercial apps was just another hop, skip and jump.

When Microsoft's Office Suite began becoming popular, its macro feature was exploited to the hilt by amateur virus writers who used its simple programming facilities to mass-mail. A most famous macro-exploiter was MELISSA which was written by David L. Smith, who brought the email gateways of giants such as Microsoft, Intel, Lockheed Martin, and Lucent to their knees. MELISSA sent out so many mails from the address-books of millions of computers it infected, that the email highway traffic simply broke down. The author of MELISSA ended up serving twenty months in a federal prison, and was fined USD 5,000 - earning the dubious distinction of being perhaps the first person to be prosecuted for virus propagation.

Virus writing has since become sleeker and more sophisticated in this cat-and-mouse game. The most energy and time that a virus writer now spends is in getting the virus code to avoid being detected by an anti-virus program. Viruses are now written so that it tries to kill off all anti-virus software tasks running in the background, before beginning their work. And, if the virus coder was an amateur and had no idea on how to go about doing such malicious tasks, resources are of course freely available on the Internet for such purposes. Other experienced coders simply look out for bait files that the anti-virus softwares may have laid out for them, and avoid infecting them altogether. Some others (polymorphic viruses) modify their signature (take on a different camouflage) each time they infect. Some others modify their body itself (that is, under metamorphosis). Yup, you guessed it right, just like Smith in the movie The Matrix.

Thanks to the enormous manpower and geographical reach at their disposal, however, Anti-Virus (AV) companies take very little time - from a few hours to a few days - to detect any fresh outbreak and come out with an antidote /signature. Phew !

IV. Countermeasures - The Good Guy Wins In The End!

While the anti-virus heroes and heroines are out there, fighting at the frontiers so that innocent netizens can enjoy a good night's sleep, there are a few easy countermeasures that the citizenry can adopt to ensure that the enemy within can be checked and liquidated. A few of these measures are listed here:

Regularly updating the anti-virus software that you have purchased (AV Signature Update). Goes without saying. In any thief-and-police game, for the police to have an upper hand, they have to have tools that are more advanced than the thieves.

Timely update of the Operating system (Patch Management). Major OS players keep sending out patches to the operating system no sooner a threat is detected. Enabling this option in one's own computer ensures that the OS is always shielded against any latest threat.

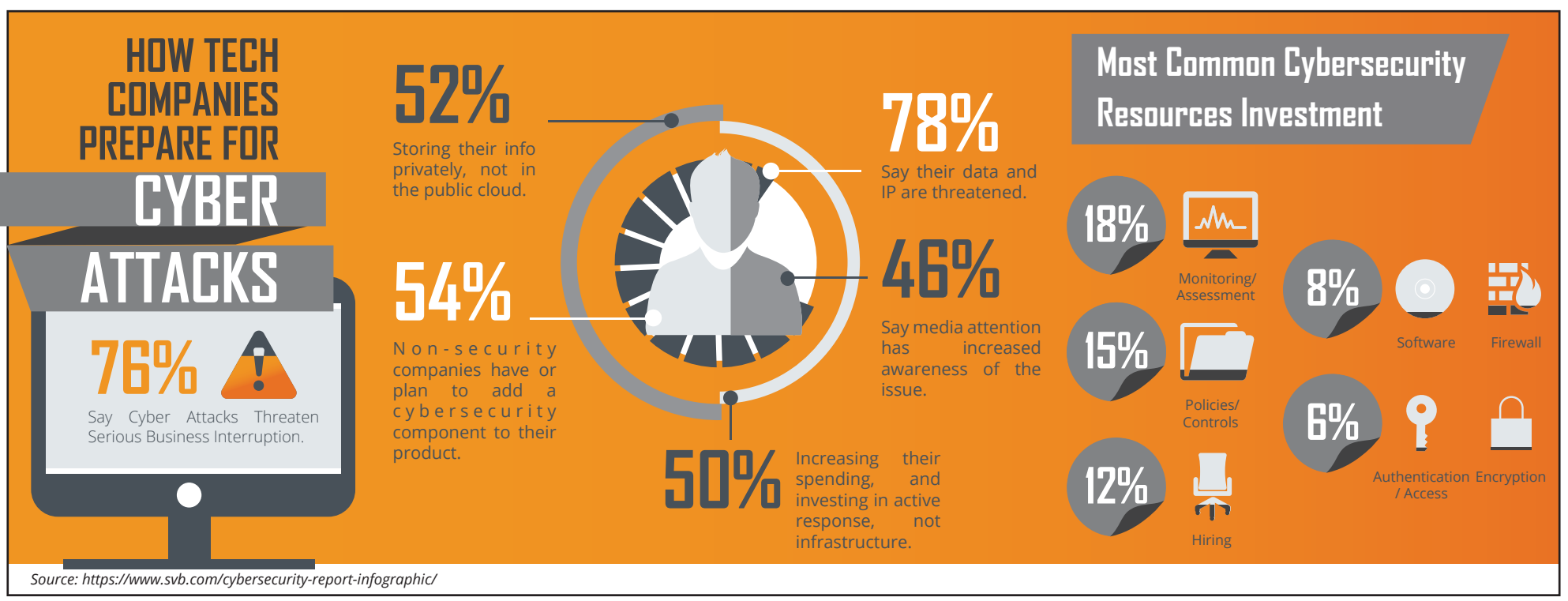
Thinking twice before opening attachments coming from strangers (Paranoia). Nowadays, email providers such as Yahoo and Google have inbuilt procedure to scan attachments on their own, and recommend whether they are safe to be opened. Still, if the attachment is coming from a stranger, it might be prudent to double-check their credentials.

Prevent unauthorized access to the system (System Hardening). The days of innocence are over. It is always better to be safe than be sorry, in these days of wolves moving around in lambs' clothing. Forgive the mixed metaphors, but the point has to be driven home real strong!

V. End Word

As this article introduces Virilicious, the world of computer viruses , I have briefly outlined the various countermeasures available. One thing to note however, is that these countermeasures are “brief” and perhaps we would have another article explaining the countermeasures alone !

Enough said, It is possible to be overwhelmed by viruses. Especially if you have already been a victim of a severe computer crash or if you have discovered that your computer was converted into a zombie that followed the instructions of some guy sipping his latte thousands of miles away. But Virilicious, the world of computer viruses, is not that sinister. You can beat them, with the help of the good guys. Yup, that’s right ! Till, next time, Adios Amigos !



Source: https://www.svb.com/cybersecurity-report-infographic/

ASEANFIC
ASEAN Financial Institution Conference

Special Supplements

Epic Malaysia Sdn. Bhd.
Solaris Mont Kiara, J-7-7, No 2 Jalan Solaris Mont Kiara
Kuala Lumpur, 50480, Wilayah Persekutuan Malaysia
www.epicmalaysia.com

Viraj Mudalige
Director / CEO of Epic Malaysia

Epic Solution Changes the Competitive Landscape of Banks in the region

The revolutionary channel innovation for banks, Epic Mobile Banking Solutions suite is now receiving tremendous attention of banking and financial institutions in the region. Speaking to our magazine, Viraj Mudalige, Director/CEO of Epic Malaysia cited several case studies to describe how this innovative solution has helped many banks in the region to reach their customers swiftly and cost effectively.

Evolving from Asia Pacific's most innovative banking solution Epic Branchless Banker can help financial institutions to extend reach by offering on-line real time banking to customers who are not required to visit banks. Banks can mobilize deposits and also recover their dues from clients in the field by issuing receipts, printed statements, pass book updates etc. This also eliminates various vulnerabilities faced by lending institutions in empowering their staff to engage in field collections as the amounts collected are immediately acknowledged. The handheld digital devices used by the field officers communicate directly with the back end systems of the banks providing tangible evidence to the customers and making the field officers immediately liable for the collections eliminating room for any misappropriations. The features we offer are amazing and quite user friendly. The solution is foolproof and strictly adheres to regulatory guidelines, prevailing electronic transaction acts and highest international standards in electronic payments and security, Mudalige added.

Epic Mobile Phone Banking and Epic EazyGo MPOS solution have been time tested by several banks and financial institutions in the region. Speaking to us Kenny Lee, Business Development Manager of Epic Malaysia Sdn Berhad said how Epic Branchless Banker transformed BSN, the state savings bank in Malaysia with 350 branches to an institution with over 4,000 online real time access points within months provides ample testimony to justify the reliability of the solution. The initial investments are quite low and can be tailor made to the needs and specific capabilities of individual financial institutions. Our ability to customize the solution with ongoing systems and procedures makes implementation fast and hassle free, he added.

With an impeccable track record of 16 years serving the banking and financial services industry in the region Epic is renowned for innovative software solutions that have changed the competitive landscape of the banking industry.

Aetins Headquarter (Malaysia)
Suites 3A02, Menara PJ, AMCORP Trade Centre,, No. 18, Jalan Persiaran Barat,
46050 Petaling Jaya, Selangor, Malaysia.
www.aetins.com

Simple, Innovative & Personalised Products & Services

Customers today are looking for easy to understand products and easily accessible channels to buy these products. Agents are looking for faster turn around times with higher customer service. Companies are looking for reduced cost with higher ROI. In order to achieve equilibrium, we need a winning strategy. The challenge for companies is to restraint cost with this augmented customer service. In order to be ahead of the game, companies need to provide customers with Simple, Innovative & Personalised products & services by bringing in the discipline of continuous monitoring & improvement of the mission critical business processes, ability to innovate and streamline business & operational models that cover the entire organisations.

In recent years, BPM (Business Process Management) & BRMS (Business Rules Management System) have become top priority for company's IT management and the process improvement has become their major focus area. Better processes lead to lower cost, higher revenues, motivated employees and ultimately happier customers. BPM has emerged as a proven technology that helps insurers meet these business objectives and gain competitive advantage. In this article, we focus on some of the key challenges faced by the Insurance companies and also the benefits delivered by BPM for insurance companies.

Insurance Business Challenges

- Being competitive in a price driven market Maintaining compliance with changing statutory, federal and international regulations
- Creating a consistent customer experience that promotes customer acquisition and retention
- Promoting "ease of use" across varied lines of business and distribution channels
- Effectively mitigating and managing regulatory reviews, fines and penalties
- Managing product development and life cycle components effectively
- Increasing growth with decreasing levels of support resources
- Increasing work automation, process efficiency and continuous improvement opportunities
- Building consistent processes that can be extended across products or lines of business
- Optimizing legacy and mainframe system environments

Benefits of BPM

- Improve profitability & lower expense ratios
- Improve customer service and agent management
- Deliver superior underwriting results
- Increase productivity
- Provides system and process flexibility and agility
- Create process transparency and integrity
- Enable continuous process improvement
- Align IT execution with business strategy

AETINS has come out with a framework (ISF bpm) that covers all lines of Insurance business, a key enabler to achieve transformational growth through Operational Excellence and Innovation. The Framework provides Empowerment to business & technical users. AETINS has gained valuable business and technological expertise by building extensive knowledge and experiences that it capitalises in delivering solutions to meet customers' needs, expectations and budget. The framework has been developed using IBM BlueworksLive, BPM & ODM

IBM BlueworksLive

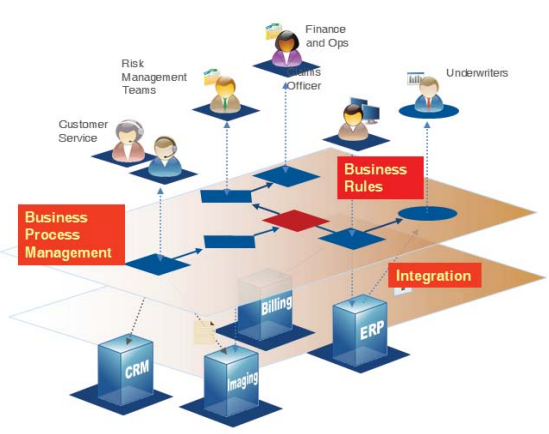
IBM BlueworksLive is a cloud-based business process modeller designed to help organizations discover and document their business processes, business decisions and policies in a collaborative manner.

IBM ODM

IBM ODM is an implementation of a Business Rule Management System. It allows the creation, management, testing and governance of business rules and events and stores them in a central repository where they can be accessed by multiple individuals and software products.

IBM BPM

IBM Business Process Manager is a powerful, comprehensive & consumable BPM platform that provides complete visibility and management of business processes. It's a simple, scalable & centralized process management system which enables the companies to design process applications that address its needs, integrate them with internal systems and manage productivity in real-time. It includes tools and run-time for process design, execution, monitoring and optimization, and is designed to make it easy for business users to engage directly in the improvement of their business processes. It scales smoothly from initial project to enterprise-wide program.



utimaco® a member of the Sophos Group

Utimaco IS GmbH
Germanusstr. 4 52080 Aachen Germany
hsm.utimaco.com/en

Utimaco Hardware Security Modules Deployed to Secure Millions of Connected Devices and Sensitive Customer, Corporate and Citizen Data

Utimaco, a worldwide leading manufacturer of hardware-based security solutions, is seeing growing enterprise and government demand for hardware security modules (HSM) to manage cryptographic keys and prevent third-party data breaches. Year-over-year growth reaches 75 percent in the U.S., four months after company expansion to North American market.

Worldwide, the industry is in the middle of a significant overhaul of old production systems and processes: Data creation and permanently connected devices are creating new opportunities, but it's also a source of concern due to hacker threats and the sheer magnitude of a potential breach. Utimaco help customers every day who are turning to a hardware root of trust to find protection.

A slew of industries apply HSM technology to secure, authenticate and enable sensitive infrastructures and data. Faced with software security breaches, and threats of backdoors, worldwide, enterprises are turning to hardware solutions to ensure the safe-keeping of encrypted data. Utimaco's scalable and customizable HSM works as the cornerstone of trust within industries such as:

- Automotive – key security to enable connected and automated driving solutions
- Big Data – enabling compliance for protection of privacy
- Conditional Access Control – keeping content safe from unauthorized access
- Connected Devices – generating and assigning cryptographic signatures to connected devices, verifying the authenticity and integrity of the permit, before executing commands
- eID – offering secure border control, electric identification and other eGovernment functionalities
- Energy Market – providing regulatory compliance and auditability to highly regulated energy market
- Manufacturing – deployed in offshore production environments to provide device identity and protect against insider threat
- Mobile Telecom – offering tamper-proof subscriber authentication
- Payment Solutions – providing secure PIN code generation, card issuing, Point of Sale and ATM management

At the core of these industries lies the need to secure sensitive consumer, corporate and citizen data, as well as advanced IP-based networks in the face of connected devices and the Internet of Things.

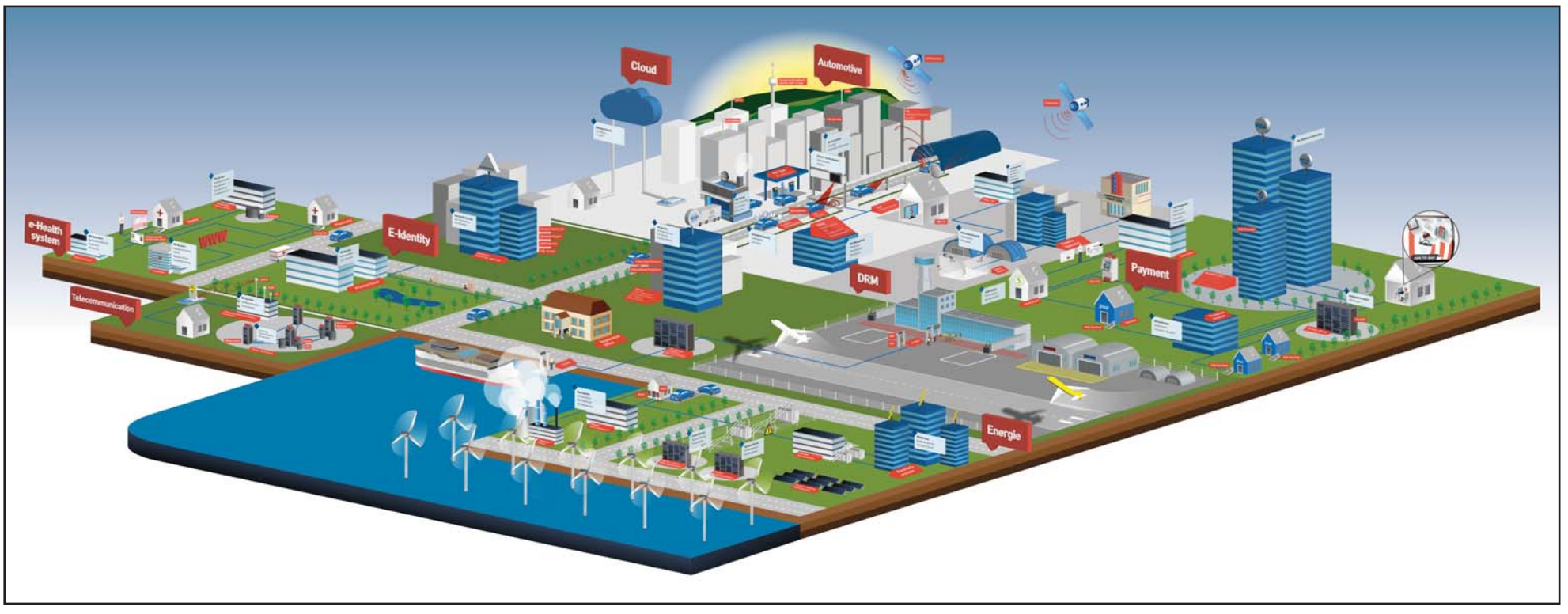
Utimaco Company Milestones:

- 100 million mobile phone users in the U.S. now authenticate against Utimaco's hardware root of trust
- 20 million smart meters communicate securely leveraging Utimaco authentication
- 5 of the top 25 semiconductor suppliers rely on Utimaco solutions as they manage the explosion of connected devices
- 2 of the top 5 telco infrastructure providers leverage Utimaco's root of trust for user authentication
- 20,000 Wi-Fi hotspots across the U.S. are ensured privacy and security with Utimaco key management
- 25,000 electric vehicles communicate securely via Utimaco to the backend

More than 50 percent of the world's Conditional Access Systems (CAS) for PayTV systems are secured via Utimaco's hardware security modules

In addition to these milestones, Utimaco has established its presence within the market of car2x communication. Top automakers from all over the world use Utimaco's FIPS-certified HSM to generate and store secure digital permits that are required for executing communication commands between the car's internal and external channels. The same goes for the financial industry; credit unions and banks alike turn to Utimaco's embedded hardware solution to generate and store cryptographic keys, securing highly sensitive payment data.

For questions on what hardware security module your organization needs, please contact SecureMetric +60389968225 or visit SecureMetric website at www.securemetric.com



APRISMA Indonesia

PT Aprisma Indonesia
Sequis Plaza 12th Floor Jalan. Jend. Sudirman Kav. 25
Jakarta, Jakarta 12920 Indonesia.
www.aprisma.co.id

Paul Wouters
SVP Regional marketing &
Business Development

From When the Sky Starts Moving Till When the Dust Settles Down.

Hardly imaginable 40 years ago , nowadays knowledge (good or bad – right or wrong) is at the fingertips of anyone willing to reach out online.

Internet banking took its first strides already in the early 1980's, by the turn of the 21st century followed by mobile banking. Actionable information thereby did shift from our imaginary safety of the keyboard on our desk to the relative insecurity of our pocket or handbag.

The result of this move is more profound than first meets the eye.

Initially perceived to be a customer retainer freebie only, the financial industry is discovering the spending potential of the impulse: cardless and cashless money at our disposal at the very moment we are tempted by a commercial offer.

The financial industry also endeavors in what used to be the big deep: making customers actually pay for a service that at first was considered a banking cost and HR saver only (the first aim of branchless banking).

The Fintech-providers also venture together with their clients in the brave new world of the 'cloud'. First from the real economy to the financial economy and now from the tangible internet to the rather unlimited cloud is not a so far fetched analogy.

The way data will be stored and transmitted will be a quantum leap that offers nearly unlimited possibilities. The way operators will bundle and charge both their hard- and software services and the way ultimate consumer behaviour will respond ... all is on the brink of a new revolution.

Aprisma is a leading internet- and mobile banking solutions provider in the Asean hemisphere and beyond. Servicing domestic, regional and international Tier 1 banks throughout Asean, we not only help our clients to manage the present (millions of bank accounts with millions of transactions every day), but also prepare them for the future with innovative and market leading financial technology.

From generic internet banking over specialized niche modules, payment hub, cloud solutions and security challenges to advanced mobile solutions for banking, insurance and telco industries ... together with our clients we not only dream about the future, but we help giving it shape. No matter how big or small the challenge is.

PT. Aprisma Indonesia is a Member of the Wirecard.com family, a German based, global leader in card and cardless payment solutions.

ascertia

Ascertia Pte. Ltd. United Kingdom
40 Occam Road, Guildford Surrey, GU2 7YG, United Kingdom.
www.ascertia.com

SECURE METRIC TECHNOLOGY
South East Asia Partner

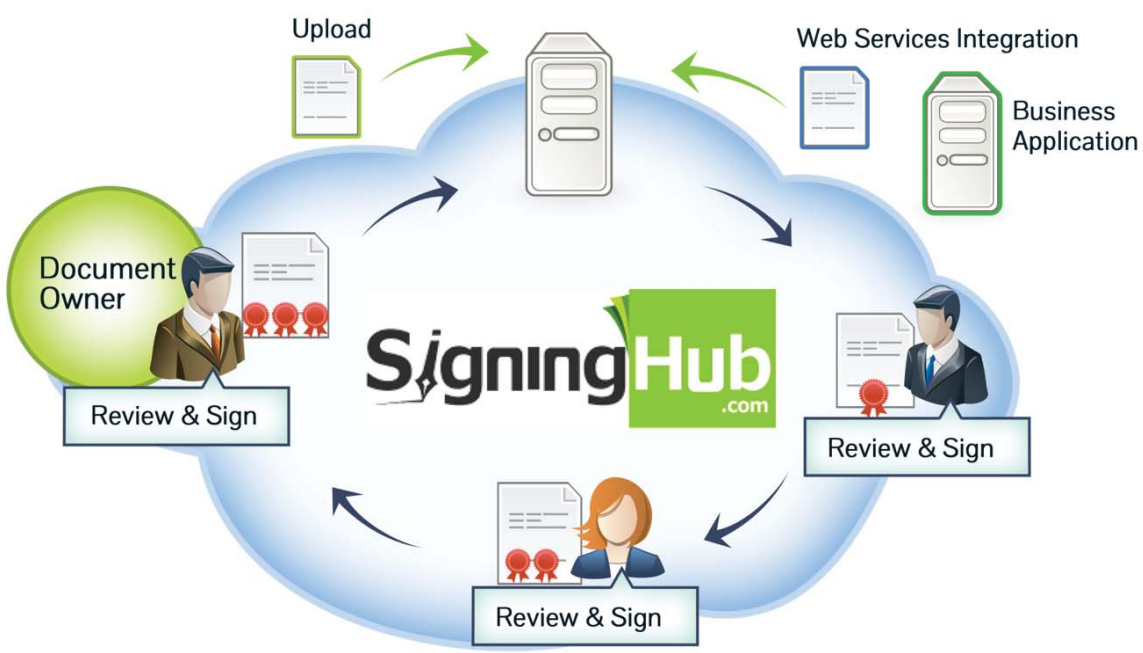
Ascertia Announces SigningHub Version 6 Availability

SigningHub v6 sets a new industry benchmark in terms of simplicity, security, branding, flexibility and interoperability!

The key to improving signing solution adoption rates is to make the process of viewing and signing documents very simple for new users. SigningHub provides an easy, fast and enjoyable experience for its users. SigningHub users can review and sign documents from any location, on any device and at any time they choose. Documents are synchronised across multiple devices so that the latest information is always shown.

SigningHub provides "the most secure way to sign" - It uses advanced standards compliant cryptographic security and hides all the complexity from its users. As a result SigningHub produces the strongest high trust signatures that are verifiable and provide legal weight evidence of signing over the long-term. Existing enterprise or national PKI services can be used. You no longer have to choose between security and ease of use - SigningHub delivers both!

Security is often retrofitted to existing business applications. SigningHub functionality can be integrated very easily using a high-level API that allow two choices: (1) Adding an intelligent View and Sign (iFrame) object within existing web-pages; or (2) Using SigningHub as an new branded web-application that delivers document workflow and digital signature approval for internal and external users. SigningHub mobile apps can be used OR SigningHub mobile APIs can be made available for companies developing their own apps.



On-premise deployment is a vital option for Government, finance and other large organisations. The SigningHub Enterprise product is cleverly packaged so that local IT staff can deploy the product in just a few hours.
SigningHub Cloud is Ascertia's multi-tenanted cloud service for those organisations wanting a cloud service. It is powered by the same SigningHub Enterprise product. SecureMetric expects to deploy a similar Malaysian hosted cloud service in 2015. Or a private cloud solution can be arranged if required.

To make it easy to deploy SigningHub provides a complete set of internal PKI services. However Ascertia recognises that there are many existing global and national PKI providers and these can also be configured so that existing keys and certificates can be used to sign documents. Existing enterprise CAs can also be used, for example signing within business banking. Adobe CDS and AATL based PKIs are also fully supported.

So for 2015 put your pen away and try sample the speed and efficiency of secure document workflow and digital signature approval provided by SigningHub!

Is Your Crypto Due a Service?

Recent revelations in the press have caused industry experts to question just how much trust can be placed in existing cryptographic standards or even in certain methods of generating key material. Companies must be prepared to respond quickly and effectively to such changes in the security landscape, else they risk reputational damage and significant costs in the event of a breach.

To understand why this preparation is challenging, we should consider how cryptography is commonly deployed within a business.

Crypto the Painful Way

Each new project will be subjected to a threat analysis and a bespoke security design created to address the risks. In many cases, cryptographic resources known as hardware security modules (HSMs) are purchased to protect cryptographic keys from exposure; the choice of HSM will be driven by a combination of cost, familiarity and security requirements. Choices of key lengths, algorithms and cryptographic modes are made by the security architect, based on company policy or their best judgement at the time. After learning the idiosyncrasies and interfaces of the chosen brand of HSM, the developers will write software to conform to the security design, hopefully in a manner that allows some degree of flexibility later, but just as likely not.

There are several problems with this traditional approach to cryptography. Foremost is a lack of agility and flexibility. Imagine what would need to happen if RSA was broken or if SHA-256 was considered too weak for further usage - an urgent and painstaking review of each project and its use of cryptography, followed by a lengthy period of development work, testing and deployment. Not only would this be very expensive, but the business would remain at risk until the changes had been made. The pressure to fix the issue quickly would result in a higher number of bugs being introduced, while the distributed nature of the cryptography would make it likely that some occurrences were not spotted.

The second issue is the cost of deployment. Buying and maintaining HSMs on a per-project basis and requiring developers to understand the peculiarities of each different type of HSM is an expensive way to operate. Bear in mind that a typical deployment will require at least four devices: two for production, one for disaster recovery and one for testing/development. Trying to re-use HSMs from other projects can prove very challenging due to the difficulties of understanding capacity and a reluctance to change systems once they have been deployed.

Finally, the effort involved in demonstrating compliance with standards is compounded when the use of cryptography is spread across a business. Demonstrating this on a per-project basis is time-consuming, even if all projects stem from a company-wide policy. If any part of the audit fails, the resolution will be a series of point-fixes on each affected system, followed by a tedious re-audit of the solution.

The time has come for companies to rethink their use of cryptography and develop new approaches that meet the demands of the 21st century.

Cryptography as a Service

Nowadays it would seem rather old-fashioned to buy new servers for each project and deploy them in their own rack. The world has moved on - servers now occupy dark datacentres and are allocated to projects with a few mouse-clicks in a virtual environment manager. Yet for some reason, few companies consider whether cryptography could operate in the same manner, despite the expense of purchasing and deploying HSMs on a per-project basis. It would be much more efficient if all the HSMs lived in a rack together and were shared between all the projects that needed them. When demand exceeded available capacity, HSMs would be purchased and added to the farm. By exploiting the standardised interfaces supported by all brands of HSM, the farm could be designed in a vendor-agnostic fashion. Imagine explaining that in a purchasing meeting! Nothing drives down costs like announcing that you don't care which vendor you use because your solution works just as well with all of them.

Now we have a farm of HSMs, it would make sense to apply some policies centrally too. If security decisions are pushed out into the individual projects, they become brittle and hard to change in a crisis. Instead, projects should express what they want to do, not how they want to do it. A centralised policy can dictate which algorithm, key length or mode of operation is currently deemed secure enough for the task. If a weakness is found in a particular algorithm, it can be removed from an approved list and projects can immediately begin using its successor. Centralised policies are easier to audit, which can dramatically reduce the cost of proving compliance with industry regulations.

By rethinking the way cryptography is deployed within a business, costs and risks can be reduced at the same time that the ability to respond to a crisis increases. Business leaders must start to consider cryptography as a strategic issue that deserves as much pre-planning as other infrastructure components. The need to adapt and the constant pressure to demonstrate compliance with standards are both excellent reasons for pursuing a service-based cryptographic deployment. To drive down both the cost and risk associated with deploying security projects, businesses must view cryptography as a strategic issue worthy of up-front investment.

SECURE METRIC TECHNOLOGY | South East Asia Partner

SecureMetric Technology Sdn. Bhd. (Reg. no. 759614-V)
2-2, Incubator 2, Technology Park Malaysia
Lebuhraya Sg. Besi - Puchong, Bukit Jalil, 57000 Kuala Lumpur, Malaysia.
Tel:+603-8996 8225
Fax:+603-8996 7225
Email: sales@securemetric.com

CRYPTOPHONE™

Immunize Your Telecommunication Against Espionage

Revelations about extensive phone interception against enterprises and governments have proven that standard telecommunication isn't safe any more and measures have to be taken.

Comprehensive protection is necessary to avoid opponents extracting sensitive information from phone calls, messages and mobile phones. The necessary measures are camouflaging of connection to protect metadata, strong end-to-end encryption to protect content of calls, messages and storage, hardened operating systems and baseband firewall protect the phone against attempts of penetration and manipulation.

Scandals of the last years have shown an unprecedented level of telecommunication interception that puts commercial success of companies and government operations at risk. The ways of interception used today reach from strategic network based interception to tactical over the air interception and penetration and manipulation of unprotected mobile phones by malicious code.

Restricting sensitive communication to confidential personal meetings is not an option, as it would result in very slow processes and high travel expenses. The only practical option is fully protected telecommunication that prevents the risk of information leakage while keeping the operational agility of the organization.

GSMK CryptoPhones provide secure mobile, fixed line and satellite communication that is comprehensively protected, trustworthy and reliable.

Protection:

By camouflaging connections GSMK CryptoPhones protect this sensitive metadata, making it practically impossible to monitor communication partners, thus preventing that opponents learn about business contacts, organization- and command structures.

Strong end-to-end encryption protects content of calls and messages, making it impossible to listen in. GSMK CryptoPhones generate fresh session keys for every call that is securely destroyed at the end of the conversation.

All GSMK CryptoPhones have hardened operating systems, which protects them against attacks over the networks. Hence the devices are protected against attempts of penetration and manipulation by malicious code.

The GSMK Baseband Firewall constantly monitors the networks for suspicious behaviour, detects attempts of active interception, warns the user and takes countermeasures.

Trustworthiness

GSMK CryptoPhones come free of pre-installed key material. Encryption keys are generated by the CryptoPhones in the hand of the user. This ensures that the encryption if fully under control of the user and not even the manufacturer has a way to listen in.

The verifiable source code gives the customer the opportunity to ascertain himself that the devices are free of backdoors and weak spots.

Reliability

To ensure reliable function under adverse network conditions GSMK has developed an extremely bandwidth efficient protocol. While standard SIP VOIP protocols require 32 Kbit/second or even more and function only in perfect 3G, 4G or WIFI networks, the GSMK IP protocol requires only 4,8 Kbit/second of bandwidth providing reliable function even in weak 2G (GPRS, Edge) and satellite connections and is not affected by measures to block IP voice communication.

GSMK CryptoPhones: 360° protection, trustworthiness and reliable function.

About GSMK CryptoPhones

- Founded in 2003 to market two years of prior research and development in voice cryptography
- First and only company to offer commercial off-the-shelf phones with strong encryption and published source code
- Privately held by its investors and employees – no bank or venture capital funding and no government shareholders guarantee the company's long-term stability and commitment to customers
- Headquartered in Berlin, Germany
- A customer base of substance in over 50 countries worldwide

SecureMetric at National eID & ePassport Conference Budapest 2014

BUDAPEST: National eID & ePassport Conference has been always the Global Forum on the drivers behind the digitalization of citizen ID documents. SecureMetric Technology is proud to join the 6th edition in BUDAPEST 2014 on 13th & 14th of October at Intercontinental Budapest as a Coffee Break & Cocktail Sponsor.

National eID & ePassport Conference 2014 Budapest is honored to have the official support from the Hungarian Banknote Printing Company, the sole producer of Hungarian Forint banknotes, and the leading security printer in Hungary specialized in production of ID documents and other products protected against counterfeiting.

200 top level government delegates together with the brightest minds in the industry, come together from all around the world to Budapest, to discuss the foundation and evolution of a global eID infrastructure, based on the digitalization of citizen ID documents.

Day One of National eID & ePassport Conference started with a warm welcome speech from the CEO of Multicert, Mr. Jorge Alcobia and Honoury Chairman Mr. Konstantin.

Mr. Edward Law, CEO of SecureMetric Technology moderated an interesting panel on the topic of “How secure is our e-Passport today? ” with Mr. Jason Clarke from Suisse International Organization of Migration and Mr. Krishna Rajagopal, CEO of AKATI Consulting Group Malaysia. The panel discussion was so interactive with lots of questions raised from the floor and it ended with putting a smile on everyone’s face in the first tiring afternoon session. The guest and delegates joined different workshop topics in different rooms for more interactive discussions.

Local host, Microsec hosted a wonderful dinner for all the delegates and sponsors on a cruise. The view was spectacular on the Danube River and everyone enjoyed the dinner and the night very much.

The conference continued with interesting topics and panel discussions on day two. Ms. Liina Areng, Head of International Relation / NATO CCD COE Ambassador at Estonian Information System Authority presented an interesting topic about eID & eServices in Estonia.

At the end of the day, the workshop panels presented their conclusion topics’ National eID & ePassport Conference 2014 ended with after event networking cocktail. It was a successful and fruitful event for SecureMetric where SecureMetric was able to meet again with European partners to discuss further corporations.

> “It is our utmost pleasure to assist in the organization of the 6th eID Conference, as co-hosts in Budapest. This great event held for the first time in Central-Europe provides excellent opportunity to all experts of the IT industry working in this region to learn about the most up-to-date trends and technologies, and to companies in and around Hungary, having strong but only local presence in the market, such as our own company, to establish important connections to key industry players and users worldwide. Bringing the conference to the capital of Hungary in 2014 is a fantastic coincidence with the 30th anniversary of Microsec this year.”
>
> says Mr. Vanczák, President of Microsec.

MALAYSIA

SecureMetric Technology Wins Best of Security at APICTA 2014

KUALA LUMPUR: SecureMetric won the MSC APICTA 2014 award for Best of Security for its PKI-In-A-Box appliance. The MSC APICTA Award highlight companies that innovates and is the leader in their field.

The judges were particularly impressed with the way that SecureMetric promotes the usage of PKI in the ASEAN region. With PKI in a Box and making the use of PKI user-friendly and acceptable to the industry.

MSC APICTA sparked innovation and awareness among a very large community of ICT companies across the south east Asia region. The feat is even more impressive as SecureMetric's employees work in business types as diverse as Two Factor Authentication, Digital Forensic Services for Software Copyright Protection. So PKI-In-A-Box provides a united platform to act on IT security issues, as well as the freedom to apply the knowledge innovatively at a local and business level regardless of which ASEAN countries SecureMetric are based.

The premise behind the MSC APICTA 2014 is to recognise innovative behaviour on IT security issues and give organizations the opportunity to share best practice with one another.

Edward Law, Group CEO and founder commented, "Although there isn't an obvious commonality between SecureMetric's very distinct and global brands, nothing else has captured the collective innovation of staff in quite the same way as a PKI in a Box. The launch pad for PKI in a Box, has for the first time enabled us to capture a truly global snapshot of SecureMetric's innovative footprint."

As part of SecureMetric's drive to promote PKI in the ASEAN region with thanks to MDeC and engagement with our global partner, PrimeKey from Sweden; SecureMetric extended the regional coverage of building a strong client base in the ASEAN region.

"Winning awards is not what our business is all about instead, it is the recognition of knowing we were having an impact goes a long way to fuel our enthusiasm and determination. A big pat on the back for everyone who got involved."