MEDIA RELEASE

24 June 2014
FOR IMMEDIATE RELEASE

4TH INTERNATIONAL CRYPTOLOGY AND INFORMATION SECURITY 2014 (CRYPTOLOGY2014) LAUNCH

Cryptology researches generate impact towards the improvement of cryptographic knowledge that relate to society needs, especially in the area of information security

(PUTRAJAYA, 24 JUNE 2014) - CyberSecurity Malaysia and the Malaysian Society for Cryptology Research (MSCR) in collaboration with Universiti Putra Malaysia (UPM), Universiti Sains Malaysia (USM), Multimedia University (MMU) and Universiti Institute Teknologi MARA (UiTM) today organized the 4th International Cryptology and Information Security 2014 (Cryptology2014) at the Everly Hotel, Putrajaya.

The conference is officiated by YB. Datuk Dr. Abu Bakar Mohamad Diah, the Deputy Minister of Science, Technology & Innovation.

The International Cryptology Conference is an open forum, which covers research on the theoretical foundations, applications and any related issues in cryptology, information security as well as other underlying technologies. Among the highlights of the Cryptology2014 are the keynote presentations by five top teams of cryptographic researchers.

“We are now on the brink of experiencing cryptography and its deployment in every corner of our day-to-day experiences. We apply cryptography everyday in many aspects of our lives, including ATM cards, Computer Passwords, and E-Commerce. Thus, research in this area has become so important. Without continuous research in the area, one could not know for certain the capabilities of ever-growing adversaries globally.” Said Deputy Minister of Science, Technology & Innovation, YB. Datuk Dr. Abu Bakar Mohamad Diah,

Datuk Dr. Abu Bakar also mentioned that research involves lots of efforts and time, therefore, it is a wise and prudent decision to present the findings of important researches in a suitable platform, such as the International Cryptology Conference so that the investment in research are not wasted.

Meanwhile, the President of Malaysian Society for Cryptology Research (MSCR) YBhg. Prof. Dato’ Dr. Hj. Kamel Ariffin Haji Mohd Atan explained that Cryptography,

CyberSecurity Malaysia
(726630-U)
Corporate Office:
Level 5, Sapura@Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.
T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999
www.cybersecurity.my

which means "hidden, secret"; is the practice and study of techniques for secure communication in the presence of third parties. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering.

Prof. Dato' Dr. Kamel Ariffin also informed that The Malaysian Society for Cryptology Research (MSCR), which was established in 2007 (after the success of the 1st and 2nd National Cryptography Conference in 2004 and 2006) sets its sight as being a premier research society in the field of cryptology in realizing the full potential of cryptography for Malaysia.

"Since its inception, it has been engaged by various agencies that sought after advice with relation the cryptography and cryptology in general." Prof. Dato' Dr. Kamel Ariffin added.

Dr. Amirudin Abdul Wahab, the Chief Executive Officer of CyberSecurity Malaysia praised the International Cryptology Conference (ICC), saying that "Cryptology2014 would promote research collaboration and discussion with research counterparts from the international arena. It is an important step towards enhancing and realizing research and applications of cryptology in Malaysia."

"After all, Modern Cryptology is one of the most important components of cyber security. Without Cryptology, it is impossible to implement cyber security features such as securing private data and other encryption functions." he added.

At the opening ceremony, YB. Datuk Dr. Abu Bakar Mohamad Diah also launched the Dynamic Enabler for Cryptographic Implementation with Modifiable Algorithmic Layer or d.e.c.i.m.a.l™. - a solution which is developed over a span of 4 years at the Al-Kindi Cryptography Research Laboratory, Institute for Mathematical Research, UPM. The solution caters for organizations that value all basic objectives which cryptographic solution can deliver. d.e.c.i.m.a.l™ functions among other as an enabler that secures email text as well as attachment using cryptographic properties before proceeding to be transferred either through free mail or organizational mail systems. d.e.c.i.m.a.l™ can also be utilized with other communication mediums too.

Cryptology2014 is the fourth International Cryptology Conference organized by the Malaysian Society for Cryptology Research (MSCR). The Cryptology conference series was initiated following the success of the 1st and 2nd National Cryptology Conference in 2004 and 2006 (NCC04 and NCC06) and the establishment of the Malaysian Society for Cryptology Research (MSCR) in 2007. In both occasions the Institute for Mathematical Research (INSPEM), University Putra Malaysia (UPM) spearheaded it, while CyberSecurity Malaysia supported and co-organized.

About Dynamic Enabler for Cryptographic Implementation with Modifiable Algorithmic Layer (d.e.c.i.m.a.l TM)

This solution caters for organizations that value all the basic objectives a cryptographic solution can deliver (namely confidentiality, integrity, authenticity & to disable repudiation) plus the higher values such as having 100% control over product development, having 100% control over choice of algorithm, having 100% control over generation of cryptographic keys, having 100% control over product deployment and having 100% control on the overall infrastructure. The d.e.c.i.m.a.l TM is a solution developed over a span of 4 years at the Al-Kindi Cryptography Research Laboratory, Institute for Mathematical Research, UPM. The team who are also MSCR members dedicate their research towards the enhancement of current cryptographic product concepts existing in the market.

For this specific preview – the decimal+email™ is introduced to the audience. In this practical implementation of d.e.c.i.m.a.l TM – it functions as an enabler that cryptographically secures the email text as well as the attachment before proceeding to be transferred either through free mail or organizational mail systems. The enabler functions independently from the mail provider but it synchronises in parallel with the mail provider in order to provide a seamlessly implementation for the user. Adding on to these "physical" features – the decimal+email™ also provides all of the features as mentioned in paragraph 1. To deploy the decimal+email™ organizations do not need to migrate to any new hardware specification.

Furthering the possible utilization of d.e.c.i.m.a.l TM – the sky is the limit. The potential user shall be guided and tutored in order to achieve the higher values of cryptography as well as the fundamental values. The enabler has potential to be integrated into architecture handling any data condition (either at rest or in motion). All the potential user has to execute is – engage us.

~ END ~

About Malaysian Society for Cryptology Research (MSCR)

The Malaysian Society for Cryptology Research (MSCR) is a non-profit organization consisting of academics, researchers, specialists, students and institutions interested to further research in cryptology and related fields. MSCR which was established in 2007, sets its sight as being a premier research society in the field of cryptology in realizing the full potential of cryptography for Malaysia. Since its inception, it has been actively engaged by various agencies that sought after advice with relation to cryptography and cryptology in general. For the future, MSCR looks forward to play a more integral role in educating and raising awareness among the masses on the importance of data security in a world that is being more connected than before.

Website: http://www.mscr.org.my

About CyberSecurity Malaysia

CyberSecurity Malaysia is the National cyber security specialist center under the purview of the Ministry of Science, Technology and Innovation (MOSTI) tasks to monitor the National e-Security aspects and continuously identify areas that can be detrimental to national security and public welfare; as well as provide training and technical assistance for National Cyber Crisis Management.

Corporate website: www.cybersecurity.my
Facebook: www.facebook.com/CyberSecurityMalaysia
Twitter: www.twitter.com/cybersecuritymy

For further enquiries about this document, please feel free to call 603-8992 6888, Mohd Shamil Mohd Yusoff (ext: 6978), email shamil@cybersecurity.my / Sandra Isnaji (ext: 6977), email sandra@cybersecurity.my / Zul Akmal Abdul Manan (ext: 6945), email zul.akmal@cybersecurity.my

Untuk pertanyaan lanjut mengenai dokumen ini, sila hubungi +603-8992 6888, Mohd Shamil Mohd Yusoff (ext: 6978), email shamil@cybersecurity.my / Sandra Isnaji (ext: 6977), email sandra@cybersecurity.my / Zul Akmal Abdul Manan (ext: 6945), email zul.akmal@cybersecurity.my