RSA会议的变迁和我们参会者的困惑

翟起滨
qibinzhai@ucas.ac.cn

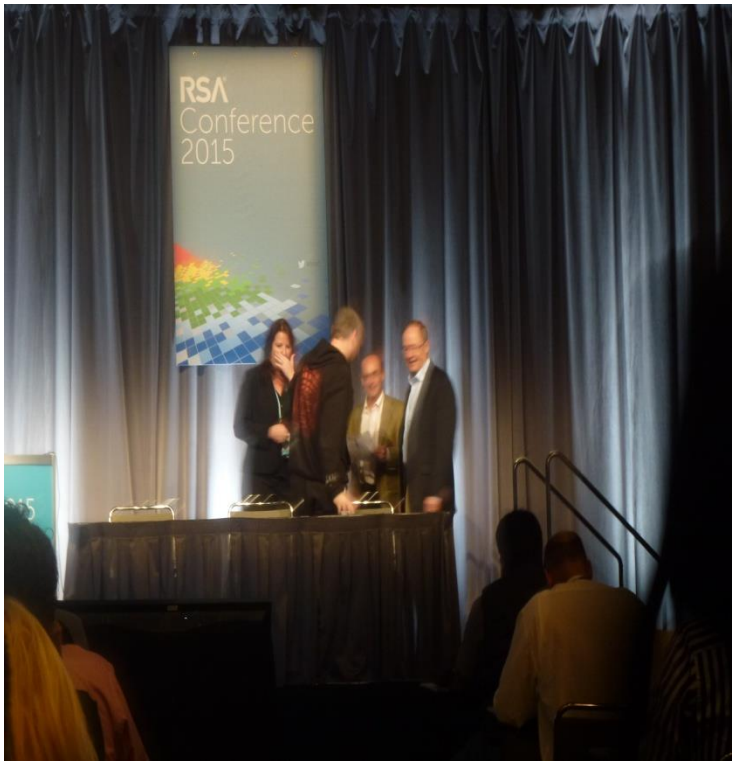
2015年6月5日北京

4月20日-24日，RSA-2015会议在美国旧金山召开。RSA大会不仅邀请全世界各地的著名安全专家出席会议探讨网络空间未来发展，也吸引全球安全厂商来参展他们的信息安全产品。RSA公司总裁Amit Yoran在本届会议上发表了题为“Escaping Security's Dark Ages”的开幕致辞。

General Alexander: Life After the NSA

3月24日,亚历山大在RSA分会场有一个小时的谈话!

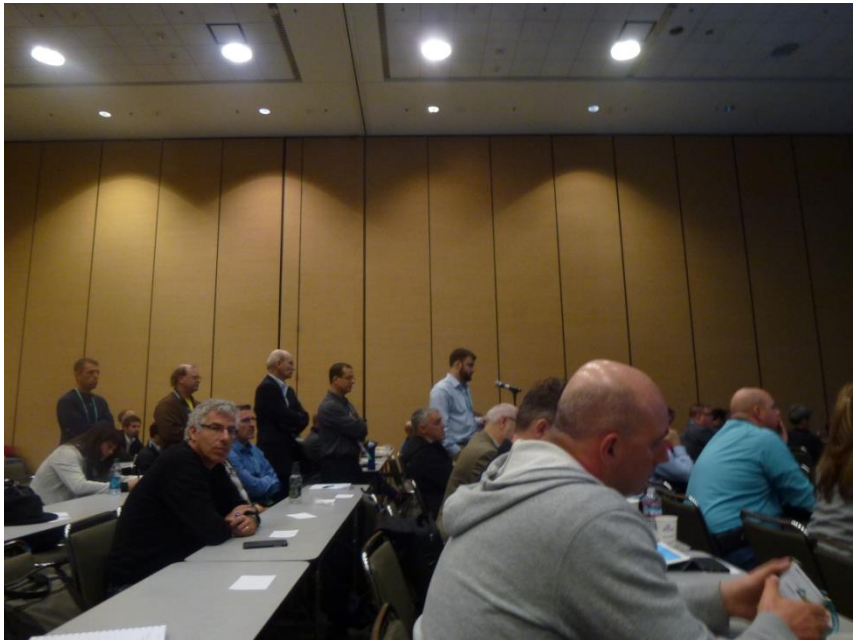
NSA前局长基斯·亚历山大(Keith Alexander)



2014年3月亚历山大从美国国家安全局(NSA)退休,很快与他人合伙创办了一家名为 IronNet Cybersecurity的私有安全公司。

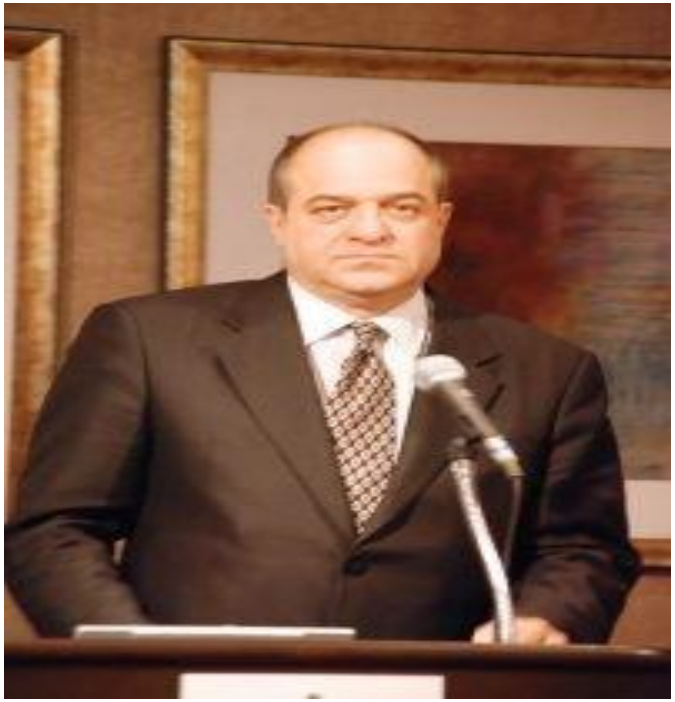
GEN (Ret) Keith Alexander is CEO of IronNet Cybersecurity, which provides strategic vision through a comprehensive cybersecurity solution to businesses. Previously, he was the first commander of US Cyber Command from 2010-2014, as well as the National Security Agency Director and Central Security Service Chief from 2005-2014. lexander's previous assignments include Deputy Chief of Staff at US Army Headquarters; Commanding General of US Army Intelligence and Security Command; Director of Intelligence at US Central Command; and Deputy Director for Requirements, Capabilities, Assessments, and Doctrine for the Joint Chiefs of Staff. He holds a B.S. from the US Military Academy, an MBA from Boston University and Master's degrees in Systems Technology, Physics, and National Security Strategy. - See more at: http://www.rsaconference.com/speakers/general-keith-alexander#sthash.FXuiXUeA.dpuf

亚历山大面对网络空间(Cyber Space)问题的谈话,诱发出一个问题-RSA会议的变迁历程!

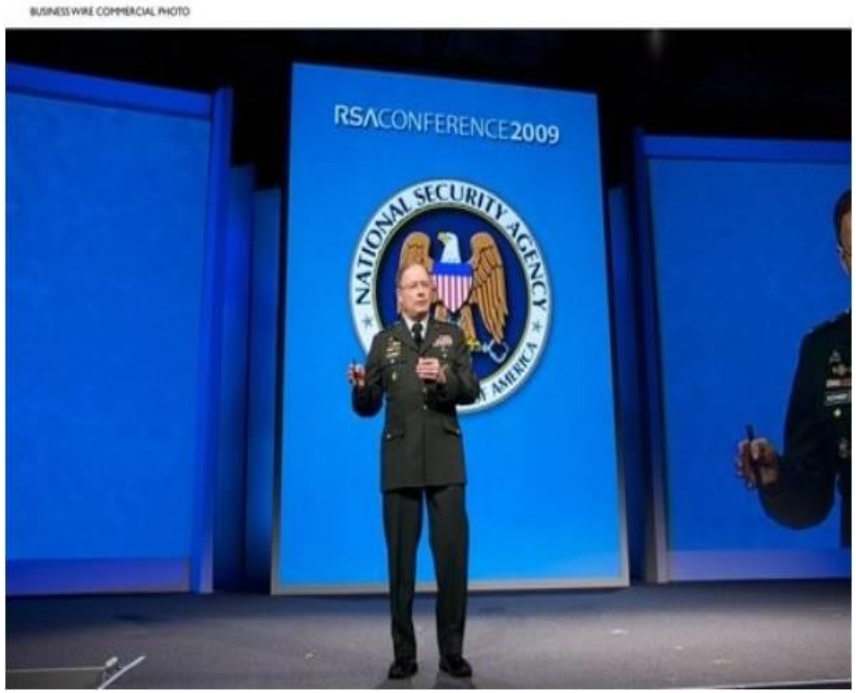


1991年11月Bidzos发起了一个论坛：“密码学，标准与公共政策”held in Hotel Sofitel in Redwood City with 50 attendees: the “Conference” starts at 9:00 a.m. and ends at 3:00 p.m.这就是首届RSA会议!当时,Bidzos希望使RSA软件成为美国及全世界的加密标准!RSA-会议是民间的年青人打造的!!

Jim Bidzos



RSA-2009 ~ RSA-2015



RSA会议最初是美国民间志士挑战政府的会议，这种挑战给美国带来了麻烦，同时也带来了光明！

U.S. government tried to mandate availability of all encryption keys via “key escrow” and/or “Clipper Chip” (1993)

信息革命是由美国民间发起的,形成现在被认知的所谓人类将进入 “The Second Machine Age!”这个结论不得了。

RSA会议的发起者Jim Bidzos主持完RSA-04 会议后，退出RSA会议主席的位置！

一个倍受尊重的贡献

In the 13th century, ch'in chiu-Shao realized that the Chinese Remainder Theorem could be used not only to count large numbers of produce or livestock,but also to conceal large numbers of troops from an enemy .This notion was refined by later thinkers and applied to modern public key cryptography.The thirteenth annual RSA Conference celebrates the mathematical and cryptographic achievements of the ancient Chinese.

RSA-04以中国剩余定理为文化背景

Jim原来打算在RSA会议上专门设立一个关于中国网络安全发展的报告厅,没有能够实现!现在RSA会议发生了重要变迁,中国报告厅的想法根本不可能了!
简介:RSA-2010China～RSA-2012China!

美国NSA局长Keith B.Alexander在RSA-09会议上做了30分钟的演讲:

“Securing Our Government Networks ”

EMC 安全事业部、RSA执行主席Arthur Coviello在RSA2014大会第一天主题演讲,中庸地说:所有国家都应该尊重和保护所有个人的隐私，希望所有国家能够确保经济活动在互联网上可以自由进行，希望所有国家放弃使用网络战武器。

今年2月,他宣布退休了！ 新上任的Amit Yoran 对中国的态度很不明朗!

THE VERGE

NSA paid $10 million to put their backdoor in RSA encryption, according to Reuters report

By Russell Brandom on December 20, 2013 04:54 pm

When leaked documents claimed to have caught the NSA inserting bad protocols into the national standards board NIST, it raised more questions than answers. Why would the NSA go to the trouble of inserting a inferior standard into NIST's set of four, when most cryptographers would simply ignore the bad algorithm in favor of the others? Even if foul play had occurred, what was the agency getting out of the deal?

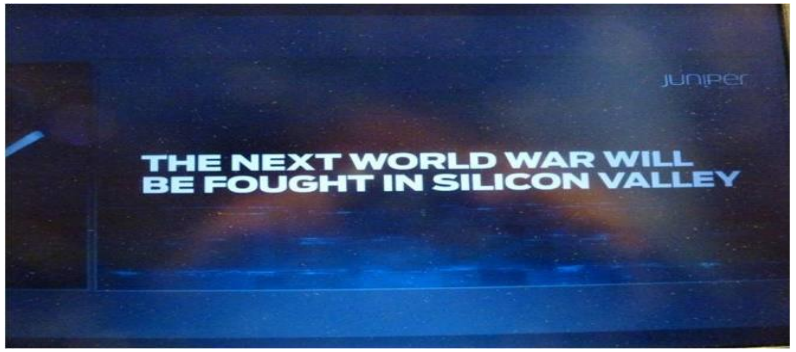
Now, a Reuters exclusive report is showing the other side of the story. The report details a

路透社揭露，NSA与RSA “狼狈为奸”

去年2月27日,Kevin Mandia 在RSA-2014 会议上做主题演讲:

State of the Hack: One Year After the APT1 Report

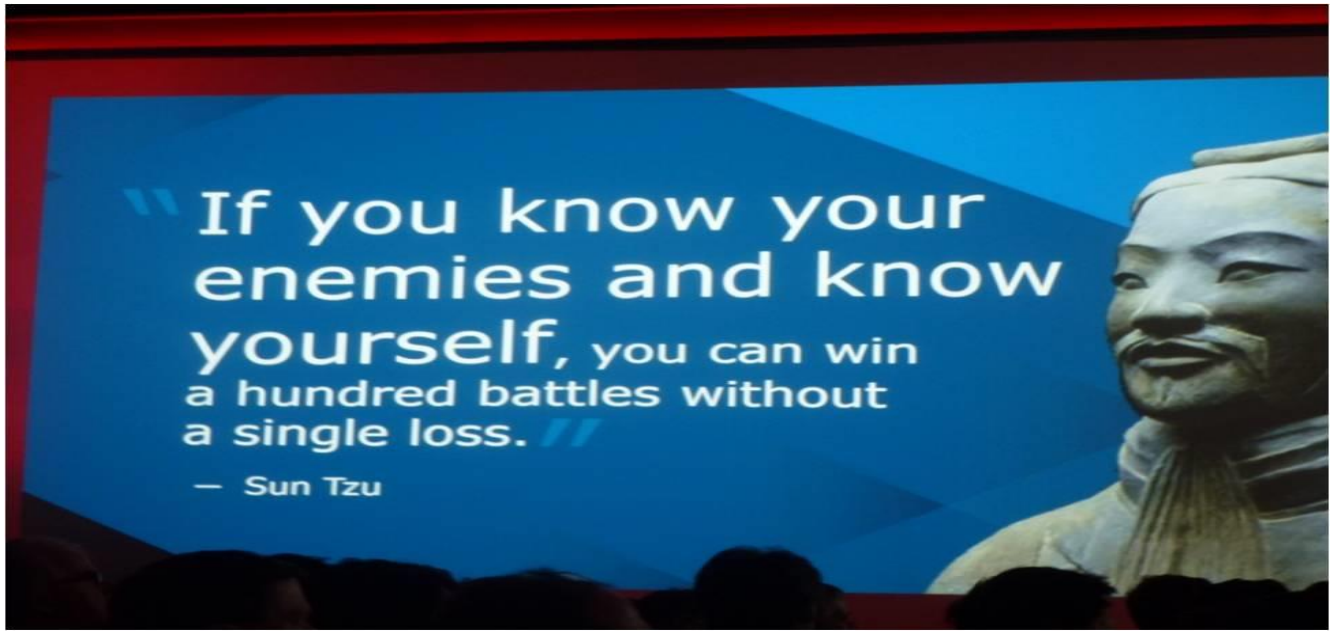
Kevin Mandia(美国空军退役军官)2004创建了Mandiant公司致力于帮助组织检测、响应并应对网络入侵，他使得Mandiant 成为首个将事件应急响应作为核心使命的公司,2013年他的公司被FireEye用10亿美元收购,他成为这个公司的高级副总裁。RSA-2013 前夕,他发表报告 “APT1”,指控“61398”对美国141家公司实施APT攻击。



今年的RSA会议对中国的攻击似乎冷却了一点点,我们的参会者在这几年的RSA会议上究竟得到了哪些实惠?我们是不是应该审视一下自己,给出自己一个更好的视角!

我们必须思考一个问题:我们的企业将RSA会议作为走出国门开拓国际市场的首选视角,是不是恰当?如果恰当,我们应该做些什么?

结束


"If you know your enemies and know yourself, you can win a hundred battles without a single loss."
— Sun Tzu