Takeaways from RSA 2016

Farhad Hussain
Technical Specialist at the
Leveraging ICT for Growth Employment and Governance Project under Bangladesh Computer Council

I had an opportunity to attend the 25th annual RSA Conference, which took place in March 2016. The world's leading information security conference saw more than 40,000 IT experts descend on San Francisco to connect with like-minded professionals and learn about modern IT security tactics. Over 500 cyber security firms were at Moscone Exhibition Center to promote their latest products and solutions. The theme of the conference was "Cyber Security + Machine Learning + Artificial Intelligence".

Over five days, the event saw 691 different seminars and speakers. Luminaries from RSA, Palo Alto, Microsoft, Intel, IBM, HP, Dell, Symantec, Kaspersky Lab, FireEye, PayPal, Cisco, Google and many others spoke alongside security experts from academia, government and small innovative firms. Here are some of the key takeaways from RSA 2016.

Palo Alto's CEO Mark McLaughlin said that education must remain at front and center of all cyber security efforts. Calling on the government, employers and parents to do their bit in educating their citizens, employees and children, McLaughlin said that systems would cease to be secure or productive without savvy users – and that if people were to lose trust in digital networks it could have disastrous consequences for the industry.

In his keynote speech, Martin Fink, Director of Hewlett Packard Labs, noted that breaches continue to rise – despite cyber security funding rising 43% to $3.7bn. "The adversary only needs a laptop", he said and so IT must find a way to turn the "asymmetry" of IT security "on its head". That meant utilizing big data to make spotting data breaches and weaknesses faster than ever before.

Amit Yoran, President of the RSA, said that security analysts need to be innovative in order to investigate wrongdoing in their organization. "Our problem isn't a technology problem. Our adversaries aren't beating us because they have better technology," he said in the opening keynote speech. "They're beating us because they're being more creative, more patient, and more persistent. They're single-minded."

Intel Security Group head Chris Young said that competition between organizations wasn't conducive to a healthy IT security landscape. Threat intelligence, he said, is an issue that could be addressed collectively because they "rise above anything that individual people or companies are involved in".

Noting that threats have risen exponentially in the last 10 years, Young stated that the only way to scale an equal response is to work with competitors.

Bill Mann, Chief Product Officer at Centrify, warned that consumer trends towards wearable technology represented a risk for IT security. A poll at the conference and later presented by Mann documented how 70% of wearable users don't use passwords or secure pass codes, despite more than half using them for business purposes. Mann went on to warn that only IT departments who treated wearable technology with the requisite respect would be best placed to offer leading levels of protection.

At a panel discussion titled "Lessons Learned from Real World CISOs," Tom Baltis, CISO of Blue Cross Blue Shield, told of his company's efforts in this respect after a rogue employee sold client data to identity thieves. "The level of trust our customers have in us has eroded," said Baltis in a conference blog post. "We're spending a lot of time engaging with our customers to ensure we have a continuing dialogue with them."

Another idea floated at the conference was the importance of collaboration among good actors: security vendors, businesses, government agencies, and law enforcement. "I would like to see security companies agreeing to work much closer together to strengthen cyber security postures for all customer organizations by collaborating on initiatives like threat information sharing," McLaughlin said in an RSA blog post.

Along these lines, Intel announced an expansion of its cyber security partnerships, trumpeting collaboration deals with BT and Siemens, and saying that its Intel Security Innovation Alliance had added 30 new members, to bring the total to more than 150.

Of course, increased cooperation sounds perfectly reasonable in theory, but these efforts can get complicated in real life. This was clear from the controversy between Apple and the FBI over the San Bernardino terrorists' iPhone. This issue over whether Apple should or shouldn't assist the FBI in accessing the iPhone's data was debated at the conference.

RSA Conference is a cryptography and information security-related conference. Its flagship event is held annually in San Francisco, California, United States. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who invented an algorithm for public-key cryptography in 1977. The algorithm is called RSA algorithm, which is used in internet encryption and authentication systems. The inventors of the RSA algorithm founded RSA Data Security in 1983. The company was later acquired by Security Dynamics, which was in turn purchased by EMC Corporation in 2006. The RSA algorithm was released to the public domain by RSA Security in 2000.

Microsoft’s president and chief legal officer Brad Smith sided with Apple, as did a panel of cryptography experts. Meanwhile, Admiral Michael S. Rogers, director of the NSA, didn’t address the Apple controversy specifically but did make a plea for increased and improved cooperation between government and the private sector. Meanwhile, U.S. Attorney General Loretta Lynch expressed support for the FBI and was critical of Apple’s stance.

Among many companies demonstrating at the show, Nuix executives Keith A. Lowry and Christopher Pogue demonstrated two upcoming products that bring a law enforcement approach to the enterprise. Insight Adaptive Security was described as “a continuous-protection platform for end-to-end threat prevention, detection, response, and remediation”, and Nuix Insight Analytics and Intelligence, which it calls “a four-dimensional security intelligence platform for breach investigations, deep-dive forensics, and analysis.”

Startup Terbium Labs was at the show announcing the closing of its Series-A funding round ($6.4 million) and talking about its MatchLight product, which is designed to alert clients whenever their stolen data appears on the so-called dark web. Terbium’s founder and CEO Danny Rogers told that the technology is aimed at early discovery of breaches.

Armorway was at the show promoting its Trust product, which uses artificial intelligence and is designed to address, investigate, and respond to internal threats. Armorway co-founder and CEO Zare Baghdasarian told that their technology was innovative in the use of game theory to enhance behavioral analytics. Behavioral analytics is important because it allows for greatly narrowing results in big data sets, making big data analytics less cumbersome.

The harsh reality of this year’s RSA Conference was perhaps best embodied by one product at the show. Vysk spokesman Hector Nieto said his company’s products operated under the assumption that your phone has been compromised. Aimed at big enterprise and government, Vysk’s products are hardware and software applications that work in tandem to encrypt all data and communications.

At the end of the conference I polled my colleagues and peers for their overall observations and takeaways. Their input is melded together with my own take on the following areas:

Perimeter Security is dead; firewalls cannot keep the bad guys out any more. The gates have been stormed and IT security has to regroup. Most big enterprises are in a constant state of breach, so new strategies and technologies are needed. First assume that your network is, or will be breached, detect it, minimize the impact and recover quickly. For example, I heard people to talk about keeping the “blast radius” as small as possible (i.e. contain the damage any one breach can make) or backup every ten minutes so the restore point can be very recent.

Cloud is now; there is rapid adoption and the cloud is different from the real world in that it moves so fast. Dozens or even hundreds of new servers can be spun up in the blink of an eye. New “born in the cloud” companies have a strategic advantage over companies with established bricks and mortar IT in that they can scale up almost instantly without capital outlays, and have access to vast resources at relatively cheap by-the-hour rates. There is a lot of automation underlying this scalability and where there is automation there are opportunities for things to go wrong at scale. It makes me think that the famous saying “To err is human, but to really foul things up you need a computer” will soon be modified to add a next level of mess that can only be achieved with a cloud. With the security concerns there are new technologies and companies popping up to deal with them because in the end while you can move your data and processing into a third party cloud, the enterprise still has bottom line responsibility for keeping information safe.

IoT is next; I heard the 50 billion IoT devices in 2020 prediction at least a dozen times. I heard people question whether everyone on the planet really needs an internet enabled tooth brush. The benefit of buying and deploying the device has to outweigh the risk of the harm it could cause. If not 50 billion there will still be billions of IoT devices in the near future and authentication, attestation and encryption have a role to play in securing them.

AI is the future; it may take 10 to 20 years but human intelligence will be matched by artificial intelligence. Once it is, AI capabilities could quickly shoot past humans to the super intelligence level as argued by Professor Nick Bostrom, Director at the Future of Humanity Institute. The idea, unlike the Internet, is to explicitly build “safety” or “security” into the AI from the very beginning.

> “Global cyber security spending is expected to reach $170 billion by 2020”

Global cyber security spending is expected to reach $170 billion by 2020. Startups and legacy companies alike are competing for this ever growing pie. However the cyber security landscape is ever changing. The key to survive in this dynamic world is the ability to adapt, adjust and manage change, as the greatest evolutionary biologist of all times Charles Darwin said, “It is neither the strongest of the species that survives, nor the most intelligent, but the one most responsive to change.”

On a personal level, I experienced the RSA Conference as a big party for the cyber security industry, where I met many people from all over the world. The networking opportunities over breakfasts, lunches, dinners, parties and over coffee were unparalleled. During those conversations, I heard much more than just the latest sales pitches, security threats or technology trends and solutions. I learned about the many different roads that various people have taken. I heard about the good, the bad and the ugly — and the changes and new opportunities that people are considering in the domain of cyber security