Summary on *Cyber Threat Intelligence* -By Bob Stasio

Sourav Bhowmik

Saturday, February 6, 2016

Talk on Cyber threat Intelligence -By *Bob Stasio*
The talk session started with a brief introduction of Bob's experience and work. Bob is currently working as Senior Product Manager at IBM. He has years of experience with the military and government intelligence body- *National Scurity Agency*(also known as NSA). Then came Bob, who started off with an introduction to cyber threat intelligence. He talked about the difficulty of detecting and tracking cyber crimes and threats.According to him, the cyber world is constantly under attack by various kinds of hackers be it novice or the expert ones. But the shocking part of this fact is that out of all the attacks, he claimed NSA can only detect about 1

Further elaborating on the nature of threats he said that cyber threats can be very *asymmetric* in nature. This essentially means that once a weak spot is discovered in the security layer, it can be breached with a minimal effort in most cases. As an analogous example he said it was possible for the Iraqi adversaries to destroy US tanks(which are worth say 80 million dollars each) using handmade bombs which would cost them a ridiculous 80 dollars only provided they knew the right spots to plant them on. Bob also compared cyber security with the field of medicine. He discussed many analogies between medical and cyber threat on a high level and non technical manner. The IBMer next moved on the topic of cyber analysis which basically consists of three components namely:

1. *Information Security*: deals with the protection of information assets as a set of business practices.

2. *Intelligence analysis*: involves analysing and observing operational, tactical and strategic situations

3. *Forensic Science*: means gathering and examining scientific evidences for civil or court investigation

Before conclusing he discussed about the "*pain points in Cyber Security*" that are:

1. Hidden threats in networks

2. Where should Analysts look: giving examples of evolution of ISIS

3. Lack of actionable intelligence
4. Too much data, too many sources

Clearly, cyber security is not a cake walk for anyone. It is a tough nut to crack. The talk ended with an interactive Question and Answer session.