Internet of Things(IoT) Security: Need for a trust based framework.

Venue: Vivekananda Education Society's Institute of Technology (VESIT), Chembur, Mumbai.

Date: 31st March 2018.

IoT promises to significantly influence our technical, social and economic landscape. Projections for impact on IoT on the Internet and economy are impressive, with some anticipating as many as 100 billion IoT connected devices and a global economic impact of 11 trillion dollars by 2025. Although it has no single universal definition, IoT related projections and trends will result in a hyper connected world wherein the most common interaction with Internet will come through passive engagement with connected objects rather than active engagement with the content.

Although the idea of connecting objects to each other and the Internet is not new, IoT has still become a popular topic today. Its rise in popularity can be attributed to the confluence of several technology and market trends that make it possible to connect more things in a cheaper and easier manner.

To introduce engineering students of different branches to IoT and related security issues, ISOC India Mumbai had organised an interdisciplinary seminar at VESIT. Monica Jeshnani, Archana Kamath and Prateek Pathak represented the ISOC India Mumbai team. For the purpose of this seminar, IoT refers to scenarios wherein network connectivity and computing capabilities extends to 'things' including objects, sensors and everyday items which are not considered as computers. These things then interact with each other, exchange and consume data i.e. they privately communicate with each other in an ecosystem to perform specific actions.

How do we ensure that things within IoT efficaciously communicate with each other in a private, secure manner? For this purpose, it is essential to draw parallels from human communication. Over years, humans have developed various languages to communicate with each other. Vocabulary and grammar ensure that communication is structured and adheres to a consensually agreed protocol of specific syntax and semantics. Thus, syntax and semantics within different languages cater to different individuals groups and facilitate secure, private communication between them.

Merely knowing the words in a specific language is not sufficient to hack or comprehend any confidential communication of significant value. In addition to verbal and written cues, non- verbal cues like gestures, tone etc. can ensure that language based communication is private, efficacious and conveys the desired outcome. Indeed, a broader understanding of context in a language driven communication is equally important as we build a framework to evaluate the efficacy of any language based on syntax or semantics. Indeed, context, syntax and semantics provide a framework to evaluate whether any language is being used efficaciously to facilitate secure, private communication.

The design of evaluative frameworks for a language driven private communication between different humans is a shared responsibility of all stakeholders i.e. language consumers (e.g. individuals engaging in communication) and language developers (e.g. linguists, translators, grammarians etc.).This limits the possibility of misinterpretation and prevents logomachy. It enables individuals to focus on their desired actions without being confused about the nature of desired outcome. Achievement of outcome via a well-defined, private driven communication process between different stakeholders that is based on consensually agreed evaluative framework builds trust in the communication process and society. Considering that our knowledge economy is driven by trust; well defined evaluative frameworks for secure, private communication are critical to create business value and prosperity in our society.

As different things are connected over the Internet in an IoT ecosystem and as they intend to efficaciously communicate with each other in a secure manner, it is essential that there is an evaluative framework to overcome these communication challenges irrespective of the nature of respective programming languages. This evaluative framework should be innovative and collaborative. Whether it is safeguarding wine bottles in a cellar through a connected cork or securing smart gadgets connected to mobile devices, this evaluative framework should guide stakeholders to design and use their IoT devices in a secure and an effective manner.

One such set of evaluative frameworks are being developed by Online Trust Alliance, an Internet Society Initiative. Thorough an 18 month consensus driven process with over 100 stakeholders, OTA identified 31 criteria initially focussed on connected home, office and wearable technology. Adoption of OTA frameworks by important stakeholders like companies can help them to assess risk and address privacy as well security issues in evaluating their deployed IoT technologies.

Students were introduced to OTA frameworks in the seminar for different stakeholders. They were asked to use it for evaluating their IoT products like smart watches, smart phones etc. Though most of these students were not aware of IoT technologies and associated evaluative frameworks, they promised to make themselves more aware about it.

The session ended with Prof. Nagananda thanking the ISOC India Mumbai team for their time and effort.

Some moments from the event:-

Prateek, an ISOC India Mumbai volunteer, explaining the nuances of communication to VESIT engineering students.

Prof. Nagananda concluding the seminar with a vote of thanks to ISOC India Mumbai volunteers.

ISOC India Mumbai volunteers, Archana Kamath and Monica Jeshnani, at the entrance of the venue.