DCNDS

Distributed and Cloud-based Network Defense System for NRENs

Objectives of the Project

The Distributed and Cloud-based Network Defense System (DCNDS) project began on 1 June 2018, and runs for 24 months, with Malaysia and Bangladesh as co-PIs. Four countries - Malaysia, Bangladesh, Indonesia and the Philippines - are the Asian partners for the project, with European collaborators from the University of Hamburg and the FIWARE Foundation.

The main objectives of the project are two-fold

1. Firstly, to setup a Distributed and Cloud-based Network Defense System, which enables NREN operators in the four partner countries to detect malicious botnet behaviour, and to introduce a cloud-based web security service platform for managing web security.
2. Secondly, to conduct two capacity building workshops in each of the Asian partner countries. These aim to train NREN and academic personnel on current topics such as building and securing cloud-based service offerings and security best practices for managing distributed botnet threats.

In addition, the deliverables for the project include the development of network security dashboards for botnet detection and security monitoring using the FIWARE platform, as well as the curation of a research dataset consisting of anonymised web-usage metadata and botnet traffic statistics for security research use. The overall architecture of DCNDS is shown in Figure 1.

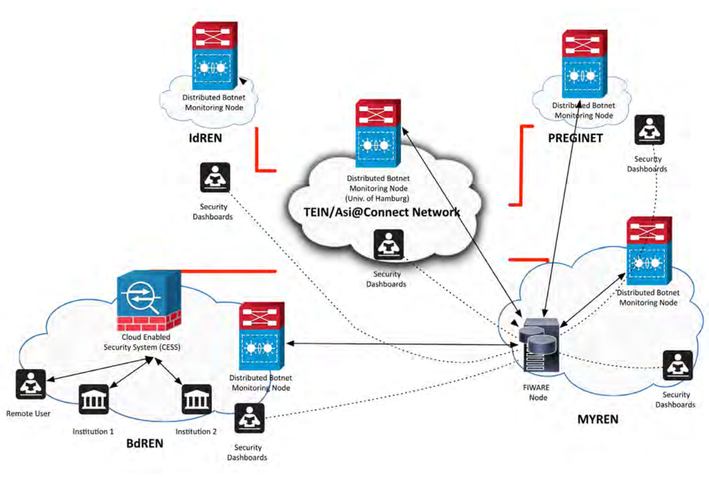

Figure 1: Distributed and Cloud-based Network Defense System (DCNDS) for NRENs

New NREN Services Deployment and Development

2.1 Emerging Cloud-based Services

The first objective of the project is to introduce new NREN services within the participating countries. This will improve the level of support within the NREN for emerging technologies to underpin the wider academic and research community, both in their respective countries and for the Asian region. This is important as Security-as-a-Service is still a very new concept for most NREN organisations. A proof-of-concept cloud-based web security platform, Cloud Enabled Security System (CESS) is now being deployed in Bangladesh to support secure internet and web services for NREN affiliated educational institutions and users.

By using an integrated service, the NREN can provide high quality security services to its users. Projects and researchers can gain access to valuable real usage metadata, enabling them to carry out advanced research in fields such as network security and data analytics. In addition, using CESS ensures that security policies can be managed and updated for participating institutions within the NREN in real-time. Metadata and web usage statistics will be captured and kept by the BdREN cloud as datasets for cybersecurity researchers.

Associated with the focus on emerging cloud-based services is the deployment of a FIWARE node in Malaysia to support the development of distributed botnet traffic monitoring and security dashboards and analytics. This leverages the rapid development and deployment capabilities of the open FIWARE platform. In addition, the FIWARE node in Malaysia will be federated with the wider FIWARE community to allow other interested parties such as researchers and Small and Medium Enterprises (SMEs) from the region to prototype their services and conduct research using the FIWARE platform.

2.2 Distributed Botnet Monitoring

Botnets are a serious problem on the internet today, resulting in economic damage to organisations and individuals. Recent trends have seen the use of alternative communication channels between the command and control (C&C) servers and infected hosts (bots), as well as the rise of distributed peer-to-peer (P2P) botnets. The use of alternative communication channels has allowed botnets to bypass common network filters.

In this project, distributed botnet detection nodes are placed in the respective NOCs of the DCNDS partners, and used to provide different vantage points in detecting P2P botnets that are residing in the networks where the nodes are being deployed. Based on their distinct communication patterns, the presence of existing and new (undiscovered) botnets in a network can be detected. The TEIN/Asi@Connect network is essential for supporting the distributed data gathering and analysis capabilities of the new botnet monitoring system, since suspicious network activity extracted from as many interconnected networks as possible provides a better picture of the extent and severity of ongoing distributed botnet attacks.

Each distributed botnet monitoring node in the respective partner NOC will tap into the NREN backbone to capture and analyse network traffic, as well as to perform data anonymisation. Only anonymised data will be sent to the cloud-based service for detailed analysis and to support the network security dashboard for NOC operators. On-site raw traffic analysis is important for reducing the amount of data forwarded to the cloud-based botnet analytics and network dashboards.

The DCNDS project has adopted a two-tier cloud model, which is an emerging cloud architecture paradigm. It incorporates the use of edge processing to provide real-time data capture and alerts, as well as to support the development of more advanced cloud-based prescriptive analytics tools in the future. The FIWARE-based analytics and network dashboards will be used by each NREN for the distributed botnet monitoring system. In addition, all botnet monitoring nodes will coordinate distributed detection and botnet monitoring activities with each other, via the TEIN/Asi@Connect network interconnecting the NRENs.

Capacity Building Workshops

One of the challenges of capacity building is how to increase the reach of activities to a wider audience within NREN communities. The DCNDS project addressed this by holding decentralised capacity building workshops, with their primary audience being in-country participants.

Given that the main partners in the DCNDS project are from four different Asian countries, namely, Bangladesh, Malaysia, Indonesia and the Philippines, four in-country workshops were planned for each of the focus areas:

- Cloud-based network security and FIWARE platform development
- Distributed botnet monitoring and security best practices

The first series of capacity building workshops (on Cloud-based network security and FIWARE platform development) have begun. The first workshop was held on 28-29 November 2018 in Subang Jaya, Selangor, Malaysia. A total of 19 participants (out of 26 registered) completed the training. The workshop achieved the objective of providing training to NREN-related staff, academics and postgraduate researchers, focusing especially on universities and academic organisations outside Malaysia's major urban areas, such as Johor, Melaka, Pahang, Kelantan, and Sarawak. Overall, the challenge for many of these participating organisations is a lack of access to training workshops that are relevant to their needs. Additionally, training materials and videos of the sessions are made available to the participants and other interested parties via the project website (https://dcnds.asia).

Planning and preparation for hosting subsequent workshops in the first series is underway, with the Bangladesh workshop scheduled for 6-7 February 2019, and the Indonesian and Philippines workshops set for March and April 2019 respectively.

Forum/Dialogue with Stakeholders

In conjunction with the capacity building workshops, a forum/dialogue session was used to engage with stakeholders and provide NREN participants with additional insight into issues that may impact them. Colocating the forum/dialogue session with the capacity building workshop helps bridge the gap between policymakers and practitioners in a more informal environment.

Mr. Navaneethan Arjuman, IPV6 Forum Malaysia, facilitated the Discussion Forum at the Malaysian workshop, entitled Personal Data Protection Act: Privacy and Security Implications to Organisations in Malaysia. The focus of the forum was to educate the participants on the significance of the Malaysian Personal Data Protection Act (PDPA), personal data privacy generally, and how it may impact network operators and cloud-based services.

Three out of the four invited speakers were able to participate in the discussions, with one speaker having to withdraw at the last minute due to work issues. Of the three speakers, two were academics with a security background, while the third speaker was the Cyber Forensics Manager for a multinational banking group. The participants had a lively discussion with the forum members and gained new insights into how PDPA affects network operations and management.

Other forum/dialogue sessions are planned for the respective country workshops, where topics of local significance will be addressed.

Conclusion

The main goals of the project - the introduction of new and emerging technology and services to Asian NRENs and engaging NREN participants from a wider geographic region within each country - are being achieved via current and upcoming project activities. Despite some initial delays, and the fact that the project has been running for only six months, the expected outcomes for the project remain on target.

Project Publicity Information

- Project website: https://dcnds.asia
- Publicity brochure

This activity has received funding from Asi@Connect project which is the European Union co-funding project under Grant contract ACA 2016-376-562.