Chair of Network Architectures and Services
Department of Informatics
Technical University of Munich

Thesis M.Sc.

Distributed Detection of SomeIP Anomalies

Motivation

SomeIP is a remote procedure call protocol. It is used today in, for instance, aircraft cabins and cars to control appliances such as lights, air conditioning, etc. As with every protocol, various protocol anomalies can occur. These anomalies include malformed packets or missing SomeIP responses to previously sent queries. Protocol anomalies are highly interesting as they indicate various types of problems. Root causes range from faulty devices (device is defective and cannot respond), to network problems, to attacks (device is under a DoS attack and cannot respond).
In a previous project we have created a centralized anomaly detection system, which is fed with a packet stream recorded at the monitoring port of the central aircraft cabin switch. However, future cabin network architectures do not have a central cabin switch anymore but are decentralized. This in turn removes the basis of our work, i.e., being able to capture all packets in the network from a central place.
Hence, we want to elaborate in this thesis how we can distribute SomeIP anomaly detection in the setting of an aircraft cabin.

Your Task

Your work begins with a thorough familiarization with the necessary background (SomeIP, anomaly detection, ...), related work in the field, our existing system, and the topology of the cabin network. As a next step you need to revise anomalies, features that can be used to detect those anomalies, and finally detection methods that we used in the old system. It is especially important to assess if additional or other features are needed in the distributed setting. As a third step, you create the design of a new prototype. You need to weigh pros and cons of the two possible design options: 1) Distribution of feature collection *and* of anomaly detection, or 2) distributed feature collection and *centralized* anomaly detection. An important further goal is to elaborate which kinds of anomalies can be detected locally or in cooperation. A further interesting question is if (additionally) collaboration of anomaly detection components can be leveraged to pin down the cause of an anomaly, e.g., to differentiate between a network fault and an attack.
This thesis is conducted together with Airbus.

Requirements

Solid knowledge in computer networking is required for this thesis. Virtualization (Xen) and Python/Java programming skills are recommended.

Contact

Dr. Holger Kinkelin, Stefan Liebald and Marcel von Maltitz
{kinkelin, liebald, vonmaltitz}@net.in.tum.de ,

http://go.tum.de/910260