COLLEGE OF ENGINEERING AND COMPUTER SCIENCE

Unifying the Conceptual Levels of Network Security through Use of Patterns

Ajoy Kumar

College of Engineering and Computer Science, Florida Atlantic University

Faculty Advisor: Dr. Eduardo B. Fernandez

We analyze security mechanisms and the protocols at the different network layers and propose a unification of these levels using security patterns. We survey existing patterns and develop missing patterns. Three basic conceptual layers used for communication are the network layer, the transport layer and the user application layer. Each of these layers is subjected to security threats and we need to consider security defenses at each of these layers. Security threats are detected, stopped or mitigated by security policies which in turn lead to the development of security mechanisms described by patterns. Some of the specific mechanisms used for security are fire walls, Intrusion Detection Systems (IDS) and Virtual Private Networks (VPN). In this thesis, we look at the relevant security components of these conceptual layers and study the synergistic combination of these components. We also look at the different security protocols controlling these layers such as IPSec (at the network or IP layer), TLS (at the transport layer) and SOAP/SAML (at the application layer). We apply patterns, where a pattern is an encapsulated solution to a system problem in a given context. Our first goal is to identify already existing security patterns for these components and protocols and then fill in the gaps for the missing security patterns. We will also try to relate to each other the patterns developed at these layers in order to unify them. We have already developed patterns for Virtual Private networks and intrusion detection systems. The patterns will be presented in a catalog to help designers build and analyze secure networks. There are some patterns for networks, but several more are needed.