



Vertrauensbildung durch Netzwerkbeobachtung

Motivation

Eine wichtige Aufgabe zukünftiger autonomer und intelligenter (Heim)-Netzwerke ist die Unterstützung von Sicherheit und Mobilität. Nutzer müssen sich darauf verlassen können, dass ihre Anwendungen gegenüber Bedrohungen von außen sowie Fehlverhalten innerhalb des Netzwerkes (Viren, Spam, DoS-Angriffe...) geschützt sind. Das Netzwerk muss deshalb die Fähigkeit haben, Bedrohungen zu erkennen und damit umgehen zu können. Mobilität ist gerade im Hinblick auf die Sicherheit eine Herausforderung. Was passiert, wenn ein Besucher in das Heimnetz kommt? Welche Dienste darf er nutzen und welche Zugriffe sollen ihm erlaubt, welche verwehrt werden? Welche Dienste des Heimnetzwerkes sollen von außen für wen zugänglich sein? Ein Ansatz für die Erteilung von Zugriffsrechten für mobile Benutzer basiert auf dem Vertrauen in die Benutzer. Es gilt also Fragen nach der Vertrauensstellung zwischen dem Heimnetz und potenziellen Besuchern zu klären, sowie Entscheidungen konkret in Zugriffsrechte umzusetzen.



Aufgabenstellung

In dieser Arbeit soll eine Metrik entwickelt werden die es erlaubt, Vertrauen in einen Netzwerkteilnehmer abzubilden. Als eine Möglichkeit soll untersucht werden, wie Vertrauen aus Beobachtungen des zurückliegenden Verhaltens eines Benutzers abgeleitet werden kann. Diese Metrik soll als Grundlage für die Unterstützung von Nutzermobilität im Projekt AuthoNe dienen. In einer anderen Arbeit soll dann das Vertrauen in konkrete Zugriffsrechte umgesetzt werden um kritische Dienste von potentiell böstigen Knoten abzuschirmen.



Voraussetzungen

Grundkenntnisse in Netzwerken, Spaß am Arbeiten in einem größeren Gesamtprojekt

Stichworte

Autonomic Networking, Trust Reputation, Access control, Monitoring

