Kurzfassung

A Secure Trust and Reputation System, Dissertation von M.Sc. Stefan Spitz, AG IIS

E-Commerce, Distributed Computing und Cloud Services sind weitverbreitete IT-Dienstleistungen, die immer intensiver von Firmen und Privatkunden genutzt werden. Bei der Auswahl der angebotenen Dienstleistungen spielen eine sichere Datenkommunikation (Kryptografie), sichere Hardware (Trusted Computing) und insbesondere die Vertrauenswürdigkeit des Dienstleisters (Vertrauens- und Reputationssysteme) eine zentrale Rolle bei der Entscheidung, wem in welchem Umfang vertraut werden soll. Diese Arbeit behandelt Vertrauens- und Reputationssysteme. Der Fokus liegt hierbei auf zwei zentralen Fragestellungen: wie können aussagekräftige Empfehlungen über andere Mitglieder bzw. Dienstleister im Vertrauens- und Reputationssystem gegeben werden, und wie schützt man die Mitglieder vor Angreifern oder warnt diese zuverlässig vor nicht vertrauenswürdigen Dienstanbietern.

Die Forschung konzentriert sich im Wesentlichen darauf, Systeme zu entwickeln, welche für einen speziellen Anwendungsfall eine möglichst genaue Vorhersage zukünftiger Verhalten der Mitglieder ermöglichen. In dieser Arbeit wird ein Vertrauens- und Reputationssystem entwickelt, welches nicht für eine spezielle Anwendung ausgelegt wurde, sondern in verschiedenen Anwendungsgebieten verwendet werden kann. Obwohl die wichtigsten Aspekte für die Modellierung von Verhalten bereits in einer Vielzahl entwickelter Vertrauens- und Reputationssystemen berücksichtigt werden, gibt es kein System, das alle Aspekte einbezieht. Das Vertrauens- und Reputationssystem, welches in dieser Arbeit vorgestellt wird, beinhaltet alle relevanten Aspekte für die Modellierung von Vertrauen. Dies schließt insbesondere die Alterung von Erfahrungen mit ein, welche in heutigen Systemen entweder unzureichend bzw. gar nicht berücksichtigt wird. Erstmalig wird in dieser Arbeit die Inaktivität von Mitgliedern für die Bestimmung der Vertrauens- und Reputationssysteme berücksichtigt, wodurch die Aussagekraft der Empfehlungen erheblich gesteigert wird.

Die Sicherheit von Vertrauens- und Reputationssystemen war bisher nur in geringem Maße Gegenstand der Forschung. Hierbei lag der Fokus fast ausschließlich auf dem Lösen einzelner Sicherheitsprobleme, wie z.B. der Sybil Attacke oder dem Problem der Newcomer. Dies birgt jedoch große Gefahren, da Methoden, welche Schutz gegen eine spezielle Attacke bieten, gleichermaßen die Effektivität eines anderen Angriffs erhöhen können. Im Verlauf der Bewertung und Analyse von Angriffen und bisher veröffentlichter Methoden zum Schutz vor Angreifern stellte sich heraus, dass die häufig verwendete Methode des Discounting (das Abwerten stark abweichender Meinungen) gravierende Schwachstellen in das zu schützende System einbringt. In dieser Arbeit werden daher ausschließlich Sicherheitsmethoden berücksichtigt, welche keine zusätzlichen Schwachstellen erzeugen bzw. Angriffe auf bestehende Schwachstellen vereinfachen. Zusätzlich zu den bisher bekannten Sicherheitsmethoden wurde eine neue, auf der Abweichung von Meinungen basierende, Methode entwickelt, welche ungewöhnliches Verhalten einzelner Mitglieder aufzeigt und es Angreifern erschwert, Angriffe unbemerkt, und somit erfolgreich, durchzuführen. Durch eine umfassende Sicherheitsanalyse des vorgestellten Systems wird nachgewiesen, dass die Kombination der verschiedenen Sicherheitsmethoden in dem vorgestellten Vertrauens- und Reputationssystem den Schutz gegen diverse Angriffe erhöht, bzw. bestimmte Angriffe unmöglich macht.