Zusammenfassung

Die Entwicklung plattform-unabhängiger XML-Datenformate hat eine große Zahl von Spezifikationen hervorgebracht, die jeweils für ein spezielles Anwendungsgebiet entworfen wurden. Darunter finden sich auch die Spezifikationen der Web Services, die in jüngster Zeit große Aufmerksamkeit erreicht haben. Die Web-Services-Technologie wurde speziell für die Realisierung netzwerkbasierter Kommunikation in heterogenen Computersystemen konzipiert, und wird heutzutage in den meisten Großorganisationen eingesetzt, etwa in der Finanz- und Versicherungsbranche, in Zulieferer- und Logistikbetrieben, in der Kommunikation mit Behörden und Ämtern, und sogar im militärischen Bereich.

Wie jede Technologie, die über verteilte Netzwerke wie das Internet bereitgestellt wird, können auch die Web Services zum Ziel externer Angreifer werden, die die darüber realisierte Funktionalität missbrauchen wollen. Sowohl die Web-Services-Spezifikationen als auch ihre bekanntesten Implementierungen weisen hier zahlreiche Schwachstellen auf, die sehr einfach über das Netzwerk ausgenutzt werden können. Angesichts der weiten Verbreitung und hohen Sensibilität der mit dieser Technologie realisierten Anwendungen liegt es also nahe, die Web-Services-Plattform einer angemessenen Analyse hinsichtlich dieser Sicherheitsprobleme zu unterziehen.

Diese Arbeit befasst sich entsprechend mit der Analyse der schwerwiegendsten bekannten Angriffstechniken auf die Web-Services-Plattform. Jede Angriffstechnik wird einzeln erläutert, analysiert, und hinsichtlich Auswirkungen, Anforderungen an den Angreifer und möglicher Gegenmaßnahmen untersucht. Darüber hinaus werden alle Angriffe im Kontext eines neuartigen Angreifermodells für Web Services klassifiziert. Dieses Angreifermodell wurde exakt für die Analyse von Angriffen auf die Technologie der Web Services konzipiert. Es basiert auf der Definition zweier Mengen von sogenannten *Befähigungen* (engl. *capabilities*): Solchen, die ein Angreifer benötigt, um eine Attacke durchzuführen, und solchen, die der Angreifer aus der Durchführung erlangt. Entsprechend eignet sich das Web-Services-Angreifermodell sowohl für die Analyse von tatsächlichen Angriffsvorfällen als auch zur Diskussion von Gegenmaßnahmen in einem formalen Kontext.

Darüber hinaus werden in dieser Arbeit neue Methoden für die Abwehr der vorgestellten Angriffstechniken eingeführt, und eine neue, generische Architektur für die schnelle Identifizierung und Abweisung maliziöser Web-Services-Nachrichten zur Laufzeit vorgestellt. Die wichtigsten Ergebnisse dieser Arbeit sind folglich die Formalisierung des Modells zur Angriffsklassifikation, die Analyse des Bedrohungszustandes für Systeme der realen Welt, und die Erarbeitung diverser Methoden zur Entwicklung von gesicherten Web Services, die unanfällig für die vorgestellten Angriffstechniken sind.