IT-Security Risiko Management mit Elementen der Spieltheorie

Stefan Schauer[1] · Stefan Rass[2] · Benjamin Rainer[1]

[1]AIT Austrian Institute of Technology GmbH
stefan.schauer@ait.ac.at, benjamin.rainer@itec.aau.at

[2]Alpen-Adria-Universität Klagenfurt
stefan.rass@syssec.at

Zusammenfassung

In diesem Artikel beschreiben wir die Entwicklung eines Systems für die Risiko-Analyse bei der Kommunikation in Rechner-Netzwerken. Durch den Einsatz von Werkzeugen aus der Spieltheorie wird das Abhör-Risiko in dem zugrundeliegenden Netzwerk mittels individuell definierbaren Taxonomien analysiert. Dabei dienen die entsprechenden Ergebnisse der Analyse als Risiko-Abschätzung (Service Level Agreement) und liefern gleichzeitig Regeln für einen optimalen Betrieb des Netzwerks (Operational Level Agreement), um die Risiko-Garantien einzuhalten. Als Nebenprodukt liefert die hier beschriebene spieltheoretische Analyse auch optimale Angriffsszenarien und liefert somit wertvolle Entscheidungshilfen für Verbesserungen an einer gegebenen Kommunikationsinfrastruktur.

1 Einleitung

Risiko Management hat im Allgemeinen die Aufgabe, Betriebsvermögen zu schützen, sowie Kosten bei Betriebsausfällen zu minimieren, und stellt somit ein zentrales Werkzeug für die Sicherheit innerhalb von Organisationen dar. In den letzten Jahren hat sich eine Reihe von Risiko-Management Werkzeugen für den Schutz von Security-Systemen entwickelt. Allerdings sind die verwendeten Analyse-Methoden meist nicht auf die zugrunde liegende Sicherheitsarchitektur zugeschnitten. So müssen Gegebenheiten und Fakten aus den Unternehmen eventuell an die Analyse-Methode angepasst bzw. Ergebnisse für die bestehenden Strukturen interpretiert werden, da sich die Terminologien der Analyse-Methoden und der Entscheidungsträger unterscheiden. Hierbei gehen oft wichtige Informationen verloren, und der Nutzen einzelner Maßnahmen relativ zum Aufwand der Umsetzung ist nicht mehr klar ersichtlich.

Wir stellen hier den SERIMA-Ansatz für die Risiko-Analyse für Kommunikationsbeziehungen in Netzwerken vor, der neben individuell definierbaren Taxonomien für Risiko-Bewertung (beispielsweise monetäre Verluste, nominale Schadensbemessungen wie „niedrig/mittel/hoch“, etc.) eine auf Abhörsicherheit bezogene Analyse von Rechner-Netzwerken sowie eine Optimierung der Kommunikation in diesen Netzwerken im Hinblick auf risikominimalen Betrieb ermöglicht. Das Verfahren basiert auf Algorithmen der Spieltheorie und bietet als Resultat ein *Operational-Level Agreement* für den optimalen Betrieb von Netzwerken sowie eine Risiko-Garantie (*Service Level Agreement*) bzgl. der Abhörsicherheit. Durch die

P. Schartner · J. Taeger (Hrsg.) · D•A•CH Security 2012 · syssec (2012) 106-117.

Integration von Elementen der Spieltheorie liefert der SERIMA-Ansatz auch Worst-Case Angriffsszenarien und somit eine Liste neuralgischer Knoten eines Netzwerks, woraus sich eventuell wertvolle Entscheidungshilfen für Verbesserungen an einer gegebenen Netzwerk-Infrastruktur ergeben.

Im nächsten Abschnitt motivieren wir den vorgestellten Ansatz durch einen Vergleich mit unterschiedlichen Ansätzen im Bereich Risiko-Management. Hierbei werden wir vor allem auf das Problem der unterschiedlichen Taxonomien der Entscheidungsträger und der Security-Spezialisten eingehen. Im Abschnitt 3 wird die SERIMA-Methode, die sich aus dem gleichnamigen Forschungsprojekt entwickelt hat, im Detail beschreiben. Im Zuge dessen werden die Basiskonzepte der Spieltheorie, die in der SERIMA-Methode zur Anwendung kommen, diskutiert und deren Vorteile gegenüber den herkömmlichen Risiko-Management Methode skizziert. Ein Überblick über die praktische Umsetzung wird in Abschnitt 4 gegeben. Hier werden die einzelnen Komponenten des SERIMA-Systems beschrieben.

2 Ansätze im Risiko-Management

Das Problem des Risiko-Managements wurde in der Literatur in zahlreichen Artikeln behandelt. Die Wahl des richtigen Werkzeuges ist jedoch im Allgemeinen schwierig. Die wichtigste Aufgabe des Risiko-Managements ist hierbei die Abschätzung der durch das Eintreten einer Bedrohung entstehenden Kosten. In den meisten Ansätzen wird für diese Abschätzung lediglich die Faustregel *Risiko = Schaden × Eintrittswahrscheinlichkeit* herangezogen (siehe [RAM10] für eine umfangreiche Aufstellung von Risiko-Management Methoden). Diese monetäre Bewertung des Risikos wurde bereits 2001 von Peltler [Pelt01] und später von Schechter [Sche04] angewendet und hat in weiterer Folge auch Einzug in den Security-Standard ISO/IEC 27005:2009 gehalten [3]. Allerdings sind, wie beispielsweise in der NIST Richtlinie [StGF02] oder bei der MEHARI Methode [MEHA04], die Begriffe und Skalen für die Bemessung des Schadenspotentials und der Eintrittswahrscheinlichkeiten i.d.R. fest vorgegeben. Diese starren Vorgaben lassen sich in der Realität oft nur schwer auf die konkreten Anforderungen bzw. Sachverhalte eines Unternehmens abbilden. Daher muss bei der praktischen Anwendung von Werkzeugen zur Risiko-Bewertung in den meisten Fällen ein Kompromiss zwischen der real vorliegenden Terminologie der Anwendung und der fix vorgegebene Terminologie der Risiko-Bewertungsmethode gefunden werden. Neben dem dadurch verursachten Aufwand bei der Modellbildung besteht auch die Gefahr, dass hierbei wichtige Informationen verloren gehen und die Risiko-Abschätzung verfälscht wird.

In der Literatur existieren bereits diverse Ansätze, die versuchen, diesem Problem der vordefinierten Taxonomien entgegen zu wirken [KoWS08] [ChKC09]. So stellt etwa das AURUM System [EkFN09] ein graphisches Werkzeug zur Modellbildung mit Hilfe von Ontologien, also allgemeingültigen Repräsentationen von Wissen, dar. Darin wird ein Ansatz für die Bestimmung von Bedrohungswahrscheinlichkeiten verwendet, der auf dem Bayes'schen Theorem beruht (in [Foro08] ist eine vergleichbare Methode beschrieben). Allerdings fließt in diesen Ansatz ein wesentliches, subjektives Element in Form eines a-priori Modells für den Angreifer ein. Dies kann zu einer Verzerrung der Risiko-Abschätzung führen, da es im Allgemeinen nicht möglich ist, das Verhalten eines Angreifers vorauszusehen. Ein Ansatz, der ohne Angreifer-Modell und ohne Trainingsdaten auskommt, ist der Minimax-Ansatz. Dieses Konzept, das teilweise auf Elementen der Spieltheorie basiert, ermöglicht es, Risiko-Abschätzungen objektiv zu bestimmen. Dieser Weg wird auch im SERIMA-System verfolgt.

Im Allgemeinen versuchen Risiko-Management Methoden, die auf Elementen der Spieltheorie basieren, aus dem Verhalten von Angreifern zu lernen, um die Abwehrmethoden kontinuierlich anzupassen und zu optimieren [CaRY08]. So werden zum Beispiel spezielle Systeme und Netzwerke aufgebaut, die bestimmte Schwachstellen, aber keine wichtigen Daten enthalten. Diese Systeme, sogenannte *Honeypots*, dienen quasi als „Köder" für Hacker. Wird ein solcher Honeypot angegriffen, so kann das Verhalten des Angreifers innerhalb des Netzwerks aufgezeichnet und analysiert werden. Die daraus gewonnenen Informationen über die Angriffsstrategien fließen in weiterer Folge in die Abwehrmechanismen des echten Produktiv-Systems mit ein, um einen optimalen Schutz zu bieten.

Ein entscheidender Nachteil dieses Ansatzes ist, dass das Verhalten eines Angreifers im System bzw. im Netzwerk beobachtbar sein muss. Dies gilt zwar für den Einbruch in ein Honeypot-Netzwerk, wie im vorherigen Absatz beschrieben, nicht aber für einen reinen Lauschangriff. Das Abhören einer Kommunikation über einen Kanal an sich kann – naturgemäß – nicht erkannt werden (Quantenkryptographie bildet eine Ausnahme hierzu, stellt jedoch auch lediglich einen a-posteriori Erkennungsmechanismus für Abhörangriffe beim Schlüsselaustausch zur Verfügung). Ein Hinweis darauf, dass eine Nachricht abgehört wurde, lässt sich häufig erst an den Auswirkungen des Angriffes erkennen, zumeist an dem Schaden, der aus dem Verlust der Information entsteht. Somit kann eine Identifikation eines Angriffs im Nachhinein oft höchstens noch zur Schadensbegrenzung herangezogen werden, womit keine proaktive Maßnahme zur Abwehr eines Lauschangriffs gegeben ist und kaum Möglichkeiten zur Risiko-Abschätzung geliefert werden.

Durch die Aspekte der Spieltheorie, die in der SERIMA-Methode eingesetzt werden, können wir derartige Probleme umgehen, da wir explizite Worst-Case Szenarien betrachten. Dadurch werden für die Risiko-Bewertung lediglich jene Fälle herangezogen, welche die größtmögliche Bedrohung für das zugrundeliegende System darstellen. Ein verwandter Ansatz ist in [CaRY08] beschrieben, allerdings basiert die SERIMA-Methode auf einer stark verallgemeinerten theoretischen Grundlage.

3 Die SERIMA-Methode

Im Folgenden gehen wir in Grundzügen auf die im SERIMA Projekt umgesetzte Risiko-Schätzungsmethode und das zugrunde liegende Verfahren für sichere Kommunikation ein. Für mathematische Details sei an dieser Stelle auf die (zitierte) Literatur verwiesen.

3.1 Grundidee und Zielsetzung

Die in diesem Artikel beschriebene Methode zur Risiko-Analyse wurde im Zuge des Forschungsprojekts *SERIMA* (security risk management based on decision-theory) gemeinsam vom Austrian Institute of Technology (AIT), der Alpen-Adria-Universität Klagenfurt und der Firma SiteXs Databusiness entwickelt. Die Methode beschränkt sich auf die Analyse des Abhörrisikos innerhalb eines Netzwerks und soll zur Lösung zweier Probleme von klassischen Ansätzen im Risiko-Management beitragen. Dies sind einerseits die Verwendung von (oft auf subjektiven Einschätzungen beruhenden) Annahmen über das Verhalten bzw. die Absichten eines Angreifers sowie andererseits das Problem der durch die Risikobemessungsmethode vorgegebenen Taxonomien. Um beide Probleme zu lösen, weicht die SERIMA-Methode von den klassischen Ansätzen des Risiko-Managements ab und führt die Risiko-Analyse mit Methoden der Spieltheorie durch.

Durch den Einsatz der Spieltheorie ist das Verhalten eines Angreifers für die Risiko-Analyse nicht mehr relevant und muss nicht über statistische Verfahren oder subjektive Annahmen modelliert werden. Wie erwähnt, verwendet die SERIMA-Methode Worst-Case Szenarien, um die größtmögliche Bedrohung für ein System abschätzen zu können. Insbesondere findet die Betrachtung von Sender und Angreifer in Form eines 2-Personen Nullsummenspiels statt, d.h. wir behandeln die beiden Spieler in einem *Angreifer-Verteidiger-Szenario* (mathematisches Spiel), in welchem der Gewinn für die Kontrahenten der Wert (gemessen in einer für die Anwendung bedarfsgerechten Taxonomie) der geheimen Botschaft ist, welche der Sender übermitteln möchte. Dies hat zur Folge, dass das Verhalten von Sender und Angreifer *simultan* analysiert und optimiert wird, wodurch die Analyse neben Bedrohungspotentialen auch jene Angriffsstrategie liefert, bei der ein Angreifer den meisten Schaden anrichten würde. Dies ist eine direkte Konsequenz der Modellierung als Nullsummenspiel, welches unterstellt, dass der Gewinn des Angreifers dem Schaden des Senders entspricht und umgekehrt. Obgleich dies die Absichten des Angreifers implizit festschreibt und aus den Bewertungen der ehrlichen Instanz (Sender) ableitet, womit die realen Absichten des Angreifers mit hoher Wahrscheinlichkeit nicht korrekt modelliert werden, so kann dennoch gezeigt werden, dass der zu erwartende Schaden in einem solchen Nullsummenszenario maximal ist, im Vergleich zu alternativen Szenarien. Anders ausgedrückt unterstellt das Nullsummenspiel dem Angreifer die Absicht, größtmöglichen Schaden zufügen zu wollen, was zu einer *Worst-Case Betrachtung* führt und eine obere Schranke für den Schaden liefert, sollte der Angreifer andere Absichten hegen. Die Analyse des Spiels liefert als Ergebnis nicht nur jene Knoten des Netzwerks, die am gefährdetsten sind, sondern zusätzlich auch die optimale Angriffsstrategie auf das zugrundeliegende Netzwerk. Dadurch fallen aber auch die entsprechenden Gegenmaßnahmen für die optimale Angriffsstrategie gleichermaßen als Ergebnis der Analyse an.

In der Praxis bedeutet dies, dass bei der SERIMA-Methode die Analyse eines Netzwerks nicht nur eine Risiko-Abschätzung bzgl. der Übertragungssicherheit, sondern zugleich auch die nötige Network-Provisioning-Strategie liefert, um diese Abschätzung zu garantieren. In dieser Strategie werden jene Kommunikationspfade definiert, mit denen gefährdete Knoten im Netzwerk bis zu einem gewissen Grad umgangen werden können. Insbesondere erfordert dies ein aktives Eingreifen in das Routing des Netzwerkes, welches durch im SERIMA Projekt entwickelte aktive Netzwerkkomponenten ermöglicht wird.

Das Problem der vordefinierten Begriffe und Skalen für Schadensbewertung wird in der SERIMA-Methode durch die Verwendung von individuell definierbaren Taxonomien gelöst, mit denen der Wert der übertragenen Nachrichten und damit der Gewinn der Spieler in der Nullsummen-Auseinandersetzung festgelegt wird. Die konkrete Bewertungs-Skala ist ohne Einfluss auf die theoretischen Eigenschaften der Methode. Sie ist damit austauschbar und kann auf anwendungsspezifische Gegebenheiten optimal zugeschnitten werden. Somit kann einer übertragenen Nachricht etwa ein monetärer Wert zugewiesen werden, zum Beispiel bei der Übertragung von Produkt-Informationen wie Bauplänen oder ähnlichen wirtschaftsrelevanten Informationen. Aber auch die Zuweisung von abstrakten Werten, wie zum Beispiel die Einteilung von Informationen in mehrere Sicherheitslevels (nominale Schadensbewertungsskalen), kann berücksichtigt werden. Alternativ ist in der SERIMA-Methode grundsätzlich auch die Definition einer komplexen, bedarfsgerecht anpassbaren Bewertungsfunktion möglich, die unterschiedliche Zusatzinformationen mit einbezieht. Dies wird in Form von entsprechenden Interfaces im System ermöglicht, welche eine benutzerdefinierbare Bewertungslogik verwenden lassen.

Auf diese Weise erlaubt das System bereits von Beginn der Analyse an eine entsprechende individuelle Bewertung des Verlustes von Informationen. Diese Bewertung zieht sich in weiterer Folge konsequent und konsistent durch die gesamte Risiko-Analyse hindurch. Dadurch wird Unstimmigkeiten entgegengewirkt, und die Vor- und Nachteile einer Investition im Security-Bereich können unter konkreten wirtschaftlichen, d.h. quantitativen, Gesichtspunkten gegeneinander abgewogen werden. Ein besonderer Vorteil hierbei ist, dass der Kunde die ihm vertraute Terminologie seiner Risiko-Bewertung nicht aufgeben muss und die Ergebnisse der Risiko-Schätzung in *denselben* Einheiten vorliegen, in denen der Wert der übertragenen Informationen bemessen wurde.

3.2 Sichere Datenübertragung

Bei der Übertragung von Nachrichten verwendet der SERIMA-Ansatz Verfahren mit informationstheoretischer Sicherheit, um eine maximale Sicherheit gewährleisten zu können und insbesondere keine empirischen Belege oder unbewiesene mathematische Vermutungen als Grundlage einzuführen. Das Paradigma der informationstheoretischen Sicherheit wurde 1949 von Claude Shannon vorgeschlagen [Shan49] und beruht auf dem Grundgedanken, dass ein Angreifer, der eine verschlüsselte Nachricht (Chiffrat) abfängt, nicht mehr Informationen über die eigentliche Nachricht besitzt, als er vor Abfangen des verschlüsselten Textes hatte. Dabei ist es essentiell, dass diese Annahmen nicht auf den technologischen Möglichkeiten basieren, die einem Angreifer zugesprochen werden, wie es etwa bei der Public-Key Kryptographie oder der AES-Verschlüsselung der Fall ist. Ein Beispiel für eine informationstheoretisch sichere Verschlüsselung ist der sogenannte One-Time-Pad (OTP).

Um eine informationstheoretisch sichere Ende-zu-Ende Kommunikation zwischen zwei Parteien, in einem Netzwerk garantieren zu können, ist sogenannte *Mehr-Wege-Kommunikation* (MWK) die einzige geeignete klassische Art der Übertragung [KGSR02] [WaDe08] [FFGV07]. Dabei wird eine Nachricht mit n Schlüsseln verschlüsselt – zum Beispiel mittels OTP – und über $n + 1$ Pfade in einem Netzwerk übertragen (siehe Abbildung 1). Sofern sich die Pfade nicht kreuzen, wird der Angreifer hierdurch gezwungen, wenigsten n+1 Knoten im Netzwerk zu kompromittieren, um die geheime Nachricht rekonstruieren zu können. Die informationstheoretische Sicherheit folgt aus der Aufteilung der Nachricht in Blöcke gemäß einem konventionellen Secret-Sharing Verfahren; beispielsweise polynomiale Threshold-Verfahren oder gewöhnliches XOR-Secret-Sharing. Tatsächlich stellt die MWK mit XOR-Sharing eine Verallgemeinerung der üblichen symmetrischen Verschlüsselung mittels OTP dar: eine Verschlüsselung mittels OTP ist eine MWK mit genau 2 Wegen – einem für das Chiffrat und einem für den Schlüssel. Für eine MWK ist es von grundlegender Bedeutung, dass sich diese $n + 1$ Pfade nicht kreuzen. Wie auch vom OTP bekannt, könnte in diesem Fall die Nachricht von einem Angreifer wieder entschlüsselt werden. Gelingt es einem Angreifer allerdings nicht, alle Schlüssel abzufangen (wie in Abbildung 1 illustriert), so gibt es nachweislich keine Möglichkeit, die Nachricht aus dem Chiffrat zu rekonstruieren.

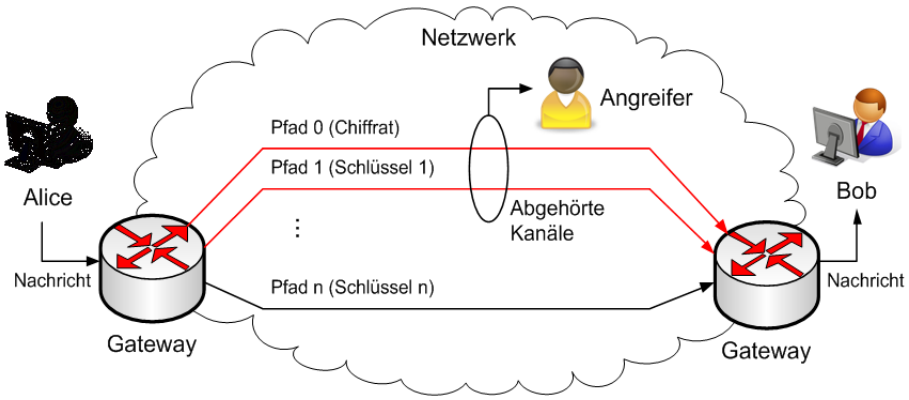

Abb. 1 Mehr-Wege-Kommunikation (schematisch)

Die Verwendung der MWK ist aufgrund ihrer guten Eignung zur Risiko-Abschätzung ein wesentlicher Baustein des SERIMA-Systems. Die Sicherheit der Datenübertragung ist somit – anders als bei herkömmlichen Verschlüsselungsverfahren – informationstheoretisch abgesichert und beruht auf keinen unbewiesenen mathematischen Vermutungen. Diese vermeidet insbesondere nicht-quantifizierbare Elemente in der Risiko-Abschätzung, wie etwa die Vermutung über die Schwierigkeit zahlentheoretischer Probleme. Ein weiterer Vorteil der MWK besteht darin, dass hier keine Verschlüsselung im herkömmlichen Sinne vorliegt. Somit entfällt auch das andernfalls erforderliche Key-Management, welches von grundlegender Wichtigkeit für die Sicherheit von konventionellen sicheren Kommunikations-Systemen ist.

3.3 Spieltheoretischer Ansatz

In der SERIMA-Methode wird als Risiko die Gefahr definiert, dass eine vertrauliche Nachricht von Alice an Bob von einem Angreifer abgehört wird. Basierend auf der Netzwerk-Topologie konzentriert sich die Methode hierbei vor allem auf jene Knotenpunkte (Router, Switches, etc.), die zwischen Alice und Bob liegen und von einem Angreifer geknackt bzw. für seine Zwecke verwendet werden könnten. Da in dieser Sicht beide Kommunikationspartner gleichermaßen das Risiko tragen, kann man sich bei der Bewertung des Risikos auf die Sicht des Senders (Alice) beschränken. Analog gelten hier aber alle Schlussfolgerungen auch für den Empfänger (Bob).

Um dieser Bedrohung durch einen Angreifer einen Zahlenwert zuweisen zu können, gehen wir von der einfachen Annahme aus, dass Alice nur die erfolgreich (vertraulich) übermittelten Nachrichten „zählt“. Das bedeutet, Alice weist jeder vertraulich übermittelten Nachricht den Wert 1 zu, und jede Nachricht, die abgehört wurde, erhält in unserem Modell den Wert 0. Um dies zu verdeutlichen, ist in Abbildung 2 ein Beispiel skizziert, bei dem Alice versucht, eine Nachricht *m* über zwei Pfade (hier fett markiert) an Bob zu übermitteln. Ein Angreifer wählt zufällig zwei Knoten aus (hier grau hinterlegt) und hört die Kommunikation an diesen Stellen ab. Nachdem auf der linken Seite die beiden Knoten (5 und 7) jeweils auf einem der Kommunikationspfade liegen, ist es für den Angreifer möglich, die Nachricht *m* abzuhören. Im Beispiel auf der rechten Seite liegt lediglich der Knoten 5 auf einem der Pfade, wodurch es dem Angreifer nicht möglich ist, die Nachricht zu entschlüsseln.

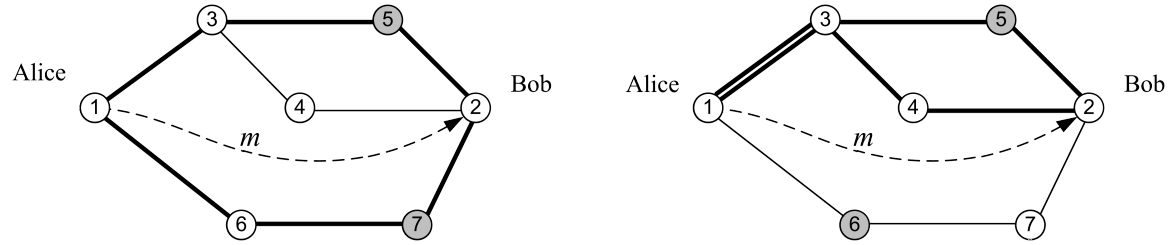

Abb. 2: Misserfolgs- und Erfolgsszenario für die Übertragung der Nachricht *m*

Obgleich die Bewertung der Übertragungen mit „1“ (erfolgreich) bzw. „0“ (abgehört) intuitiv einleuchtend erscheint, ist es im Falle der Übertragungssicherheit im Allgemeinen schwierig zu sagen, wann eine Nachricht tatsächlich abgehört wurde und wann nicht, da das Abhören einer Nachricht ein *rein passiver* Vorgang ist. Es gibt also für Alice keine technische Möglichkeit, um eine korrekte Aussage über den Erfolg oder Misserfolg der aktuellen Übertragung zu tätigen. Ebenso ist die genaue Strategie eines Angreifers im Allgemeinen nicht bekannt. Glücklicherweise besteht aufgrund der Nullsummenspielannahme jedoch *kein* Bedarf an diesen Informationen. Um keine Annahmen über die Strategie eines Angreifers machen zu müssen, verwendet die SERIMA-Methode zur Berechnung des Abhör-Risikos das *(asymptotische) Mittel* über alle möglichen Angriffsstrategien bei wiederholten Übertragungen. Dafür werden Wiederholungen der Übertragung unter zufällig ausgewählten Übertragungspfaden (multiple und sich nicht kreuzende Kommunikationswege von Alice zu Bob) und Angriffen simuliert. Dies liefert eine durchschnittliche Erfolgswahrscheinlichkeit für eine vertrauliche Übertragung, wobei das Verhalten für beide Spieler (Sender und Angreifer) simultan optimiert wird. Optimal bedeutet in diesem Fall, dass Alice jene Kommunikationspfade durch das Netzwerk verwendet, welche das geringste Abhörrisiko haben, wobei auch der Angreifer die kompromittierten Knoten optimal für einen Lauschangriff wählt. Aufgrund der Bewertung des Erfolges auf einer 0/1-Skala entspricht die mittlere Erfolgsrate bei einer Übertragung genau der *Wahrscheinlichkeit* für eine erfolgreiche Übertragung. Somit besteht eine direkte Interpretation des Abhör-Risikos in Form einer Wahrscheinlichkeit, welche sich wiederum problemlos in *erwartete Maximal-Verluste*, gemessen in Vermögenswerten oder anderen Skalen, umrechnen lässt.

Bei der Analyse wird nun die gegebene 0/1-Bewertungsfunktion verwendet, um den Versuch der vertraulichen Übertragung einer Nachricht von Alice zu Bob zu gewichten. Im Falle unseres Beispiels aus Abbildung 2 wird, wie oben beschrieben, eine erfolgreiche Übertragung mit 1 bewertet, und ein Misserfolg bei der Übertragung erhält den Wert 0. Hierfür ist die Topologie des zugrundeliegenden Netzwerkes, also die möglichen Verbindungen zwischen Alice und Bob, ausschlaggebend. Basierend auf dem Prinzip der Mehr-Wege-Kommunikation ist es Alice’s Strategie, eine Anzahl von Pfaden in dem Netzwerk auszuwählen, über welche die Kommunikation erfolgen soll.

Im Detail ist die optimale Übertragungsstrategie für Alice eine Menge an Pfaden und entsprechenden Wahrscheinlichkeiten, mit denen diese Pfade gewählt werden müssen. Wie bereits erwähnt, hat Alice keinen Einfluss auf das Verhalten eines Angreifers und kann dieses auch nicht voraussehen. Es ist nun Alice’s Bestreben, ihr Verhalten entsprechend der optimalen Strategie eines Angreifers anzupassen, um somit das Worst-Case Risiko für eine Übertragung zu minimieren. Exakt dieses Problem löst die Spieltheorie durch die Bestimmung von Nash-

Gleichgewichten in dem modellierten Kommunikationsspiel (Verteidiger-Angreifer Szenario) [NeMo44]. Dadurch entfallen bei der SERIMA-Methode, im Gegensatz zu anderen Ansätzen, die Spekulationen über das tatsächliche Verhalten eines Angreifers.

Aus mathematischer (spieltheoretischer) Sicht nehmen in der SERIMA-Methode Alice die Rolle des Spielers und ein Angreifer die Rolle des Gegners ein. Der Spielverlauf wird durch eine Auszahlungsmatrix beschrieben, welche den Spielausgang unter jeder möglichen Kombination von Verhaltensstrategien beschreibt; sie ergibt sich somit aus allen Übertragungsmöglichkeiten für Alice und den entsprechenden Angriffsstrategien des Gegners. Dabei werden Erfolg und Misserfolg der Übertragung in jedem Szenario in einer beliebigen und für die Anwendung wählbaren Taxonomie gemessen. Weil keinerlei Angaben über die Absichten des Angreifers bekannt sind und auch keine Annahmen darüber getroffen werden sollen, ist eine Modellierung des Problems als Nullsummenspiel die beste Lösung. Die Lösung des Spiels besteht nun in der Bestimmung eines Nash-Gleichgewichtes, welches folgende Informationen beinhaltet:

- Die optimale Strategie x^* um die Kommunikation über das Netzwerk durchzuführen. Dies ist ein Vektor von Wahrscheinlichkeiten, mit denen die verfügbaren Kommunikationskanäle für die Übertragung gewählt werden sollten.
- Die optimale Angriffsstratgie y^*, welche ebenso ein Vektor von Wahrscheinlichkeiten ist und Wahrscheinlichkeiten für Angriffe auf gewisse Knotenmengen angibt.
- Die mittlere Auszahlung $v(A) = (x^*)^T A y^*$ an Spieler 1, wobei die Matrix A eine 0-1-Matrix ist, in welcher das Element a_{ij} genau dann 1 ist, wenn die Kommunikation über die Pfade gemäß Übertragungsstrategie i bei einem Angriff auf die Knoten gemäß Angriffsstrategie j erfolgreich war.

Die wesentliche Eigenschaft des Wertes $v(A)$ liegt in der *Gleichgewichts-Ungleichung* $x^T A y^* \leq (x^*)^T A y^* \leq (x^*)^T A y$, welche bei einer Abweichung eines der beiden Spieler vom optimalen Verhaltensprofil (x^*, y^*) eine Verschlechterung der Erfolgsbilanz prognostiziert. Hieraus folgt unmittelbar die Gültigkeit des Modells als Worst-Case Szenario, wie in [Rass09] auch formal bewiesen wird. Der Vektor x^* stellt somit eine Regel zur optimalen Wahl von Übertragungspfaden dar (dies ist das Operational Level Agreement), welche zu der Einhaltung der Risiko-Schranke $v(A)$ notwendig ist (diese stellt das Service-Level Agreement dar). Die neuralgischen Punkte im System lassen sich aus den optimalen Angriffsstrategien, codiert durch y^*, direkt ablesen. Alle drei Variablen lassen sich effizient durch Methoden der linearen Optimierung berechnen.

4 Das SERIMA-Toolset

Aus den obigen Ausführungen ist ersichtlich, dass eine spieltheoretische Risiko-Schätzung ihre Gültigkeit verliert, sobald die tatsächlichen Übertragungen vom optimalen Verhaltensprofil x^* abweichen. Somit ist ein aktives Eingreifen in das Routing des Netzwerkes erforderlich. Dies ist Aufgabe des sog. *Defender-Systems*; die Bestimmung der optimalen Strategie selbst ist Sache der *Analyse-Komponente*.

4.1 Analyse und Network-Provisioning

Das SERIMA-System stellt ein Toolset dar, das in zwei große Bereiche aufgeteilt ist (vgl. auch Abbildung 3): dem *Analyse&Reporting*-Tool und dem *Defender*. In Ersterem wird zu-

nächst die Topologie des zu untersuchenden Netzwerks auf einer abstrakten Ebene nachgebildet. Das Hauptaugenmerkt liegt hierbei auf Kommunikationskanälen zwischen einzelnen Netzwerk-Komponenten (Switches, Router, Server, etc.). Zusätzliche Informationen über die Hard- und Software sowie deren genaue Konfiguration werden im Prototypen-Stadium des Systems der Einfachheit halber vernachlässigt. Allerdings können bei der Modellierung jedem Knoten individuelle Sicherheitseigenschaften zugewiesen werden. Dies erleichtert die Abbildung der realen Gegebenheiten innerhalb des Netzwerks und erlaubt, unterschiedliche Sicherheitsstrukturen direkt im Modell zu erfassen. Für eine bessere Darstellung von großen Netzwerk-Strukturen ist die hierarchische Modellierung von Subnetzen möglich. Dies erleichtert in weiterer Folge auch die Analyse des Gesamtnetzwerks, sowohl im Hinblick auf die Modellierung, als auch im Hinblick auf die Komplexität der Analyse. Die Informationen aus dem Modellierungstool werden dem *Analyzer* übergeben (server-seitiges Modul), welcher das Netzwerk entsprechend dem oben beschriebenen Algorithmus aus der Spieltheorie analysiert. Vor allem durch den hierarchischen Aufbau einer Netzwerk-Topologie wird die Analyse drastisch beschleunigt, da Subnetze separat untersucht werden.

Das gesamte *Analyse&Reporting*-Tool liefert zwei Ergebnisse: Erstens, einen Bericht über die potentiellen Schwachstellen des Netzwerks für die Entscheidungsträger. Hierin sind jene Knoten enthalten, die bei einem Angriff die größte Bedrohung für das Gesamtsystem darstellen und am besten geschützt werden sollten. Dieser Bericht stellt zugleich die optimale Angriffsstrategie eines Gegners dar. Diese Strategie ist die Basis für das zweite Ergebnis: eine Network-Provisioning Strategie für den *Defender*.

Die durch das SERIMA System ermittelte Network-Provisioning-Strategie, d.h. die Art und Weise, wie das Netzwerk für die Übertragung durch den *Defender* konfiguriert und genützt wird, ist eine Sammlung von Pfaden, über die eine Nachricht sicher von Alice an Bob übermittelt werden kann. Diese Strategie x^* wird direkt aus der Analyse abgeleitet und in Form von Regeln für das Routing im Netzwerk an den Defender übergeben. Der Defender kann als aktive Netzwerk-Komponente oder als Software-Lösung implementiert sein und setzt diese (Network-Provisioning-)Gleichgewichts-Strategie x^* um. Dafür werden die entsprechenden Veränderungen in den Routern und Switches des Netzwerks vom Defender automatisch durchgeführt. Er stellt somit sicher, dass die Routing-Strategie für die Kommunikation zwischen Alice und Bob im Netzwerk auch eingehalten wird.

4.2 Ergebnisse

Das SERIMA-System liefert als endgültiges Ergebnis für den User eine optimale Network-Provisioning Strategie für die Kommunikation von Alice mit Bob. Befolgt Alice diese Strategie, so ist das Risiko, dass die Nachricht abgehört werden kann, beweisbar minimal. Diese Schranke für das Abhörrisiko kann als *Service-Level Agreement* (SLA) für das aktuelle Netzwerk angesehen werden, wodurch eine Risiko-Garantie für ein bestehendes Netzwerk ausgegeben werden kann. Somit wird einem Netzwerk-Provider ermöglicht, einem Kunden eine garantierte Obergrenze für das Abhörrisiko in seinem Netzwerk anzubieten. Die Kommunikationspfade, die in der Network-Provisioning Strategie definiert sind, stellen in diesem Fall ein Operational-Level Agreement (OLA) dar. Wird das OLA eingehalten, was in der SERIMA-Methode durch den Defender automatisch realisiert wird, so ist sichergestellt, dass auch die Beschränkung des Abhörrisikos (SLA) eingehalten wird.

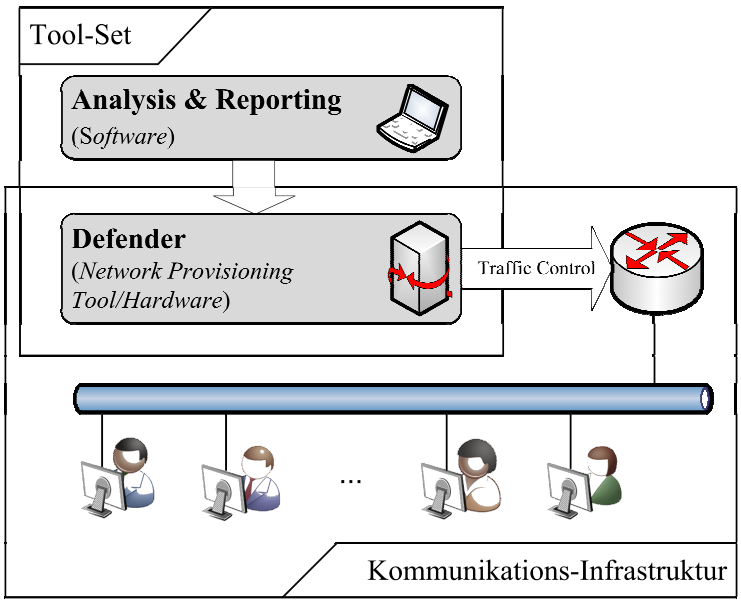

Abb. 3: Architektur des SERIMA-Systems

Zusätzlich zu dem OLA liefert die SERIMA-Methode eine Liste an neuralgischen Knoten im Netzwerk, die besonders schützenswert sind. Dies ergibt sich wiederum direkt aus der optimalen Strategie y^* für einen Angreifer. Ein Angriff auf diese neuralgischen Knoten mit den durch y^* angegebenen Wahrscheinlichkeiten würde dementsprechend einen maximalen Schaden im Netzwerk verursachen. Gleichermaßen stellt die Gleichgewichts-Ungleichung sicher, dass ein Angriff, der sich auf bestimmte Knoten im Netzwerk konzentriert, nur geringeren als den ermittelten Schaden verursachen kann. Anders ausgedrückt wäre ein Angreifer – um maximalen Schaden zu verursachen – gezwungen, seine Strategie ständig zu wechseln, was in der Realität nur schwierig durchführbar wäre. Dennoch existieren neben der optimalen Angriffsstrategie im Allgemeinen noch andere Gleichgewichts-Strategien (also gültige Lösungen für das Kommunikationsspiel), bei denen andere Knoten im Netzwerk attackiert werden könnten. Da keine direkten Annahmen über die Intention eines Angreifers getroffen werden, können solche Mehrdeutigkeiten nicht ausgeschlossen werden. Durch die Eigenschaften des zu Grunde liegenden spieltheoretischen Kommunikationsmodells wird jedoch sichergestellt, dass diese alternativen Optima keinen größeren Schaden verursachen können, als jenen, der durch die Analyse ermittelt wurde. Dieser Umstand kann also weder theoretisch noch praktisch zu einer falschen Risikobewertung führen.

5 Zusammenfassung und Ausblick

Ein effektives Risikomanagement ist vor allem für Entscheidungsträger in Organisationen ein wichtiger Faktor, um einerseits Betriebsvermögen zu schützen, und andererseits, um Kosten zu reduzieren, sollte es zu Betriebsausfällen kommen. In der Praxis existieren zwar eine Reihe entsprechender Werkzeuge für die Risiko-Analyse, diese sind jedoch nicht immer adäquat einsetzbar. Die Bedrohungen werden oft lediglich subjektiv spezifiziert, und das Gefahrenpotential für das zu schützende Betriebsvermögen kann in vielen Fällen nur qualitativ und heuristisch bemessen werden.

Die SERIMA-Methode verbindet die klassischen Ansätze zur Risiko-Analyse von Kommunikationsnetzwerken mit Elementen der Spieltheorie und stellt dadurch einen Schritt in Richtung einer stärker objektivierten Risiko-Bemessungsmethode dar. Subjektive Eingaben und Einschätzungen sind zwar in Form der Angriffsstrategien-Identifikation und der Auszahlungsmatrix für das Kommunikationsspiel weiterhin erforderlich, jedoch ist die errechnete Risiko-Aussage objektiv und optimal im Rahmen der Gegebenheiten. Insbesondere basieren die errechneten Sicherheitsaussagen auf *keinen* anderen oder zusätzlichen (impliziten) Annahmen, als jenen, aus denen das spieltheoretische Modell gebildet wurde. Diese sind jedoch vom User für die Anwendung vollumfänglich vorgegeben und bei Bedarf veränderbar. Die SERIMA-Methode stellt bei der Analyse Worst-Case Szenarien in den Mittelpunkt der Betrachtung, um eine maximale Risiko-Abschätzung geben zu können. Auf diese Weise wird ein optimaler Schutz im Hinblick auf den größtmöglichen Schaden, den ein Angreifer in dem analysierten Netzwerk verursachen kann, ermöglicht.

Einen weiteren großen Vorteil der SERIMA-Methode stellen die individuell spezifizierbaren Bezugsgrößen dar. Dadurch kann etwa der direkte Bezug zu den monetären Kosten für das Unternehmen beim Eintritt einer bestimmten Bedrohung hergestellt werden. Alternativ können die Ergebnisse in abstrakten Skalen angegeben werden, die ebenfalls individuell gestaltet werden können.

Um im Risiko-Management die unterschiedlichen Herangehensweisen quantitativ bewerten zu können, werden in der Praxis für gewöhnlich *Security-Benchmarks* herangezogen. Weil in der SERIMA-Methode eine quantitative Bewertung eines definierten Sicherheitsziels erfolgt, kann diese Methode auf natürliche Weise als Security-Benchmark angesehen werden. Basierend auf den Ergebnissen der Analyse mit der SERIMA-Methode können Security Service Level Agreements und zugehörige Operation Level Agreements einfach formuliert werden. Diese bieten sowohl für Kunden als auch Betreiber eines Netzwerks eine objektive Garantie über die Sicherheit und Verfügbarkeit eines Netzwerkes.

Die entwickelte Methodik ist keinesfalls auf die Abhörsicherheit beschränkt. Das Modell kann auf die Betrachtung anderer Angriffe wie Denial-of-Service oder die Authentifizierung ausgeweitet werden. Darüber hinaus können etwa auch der Bedarf an Bandbreite, Kosten-, preispolitische Überlegungen o.ä. Bestandteile in die Risiko-Analyse mit einfließen. Die zugrunde liegende Modellierung ist entsprechend erweiterbar.

Danksagung

Die Autoren möchten Christian Kollmitzer, Oliver Maurhart für aufschlussreiche Diskussionen und Denkanstöße sowie Matthias Vavti für die Umsetzung der Modellierungssoftware, danken. Diese Arbeit wurde von der österreichischen Forschungsförderungsgesellschaft (FFG) als Projekt Nr. 829570 finanziert.

Literatur

[CaRY08] H. Cavusoglu, S. Raghunathan und W. T. Yue, Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment, Journal of Management Information Systems, Bd. 25, Nr. 2, pp. 281-304, 2008.

[ChKC09] T. J. Chiang, J. S. Kouh und R. I. Chang, Ontology-based Risk Control for the Incident Management, International Journal of Computer Science and Network Security, Bd. 9, Nr. 11, p. 181, 2009.

[EkFN09] A. Ekelhart, S. Fenz und T. Neubauer, Automated Risk and Utility Management, Proceedings of the Sixth International Conference on Information Technology: New Generations, IEEE Computer Society, 2009, pp. 393-398.

[FFGV07] M. Fitzi, M. K. Franklin, J. Garay und S. H. Vardhan, Towards Optimal and Efficient Perfectly Secure Message Transmission, 2007.

[Foro08] F. Foroughi, Information Security Risk Assessment by Using Bayesian Learning Technique, Proceedings of the World Congress on Engineering, Bd. 1, International Association of Engineers, 2008, pp. 2-6.

[ISO09] ISO/IEC, The ISO27k FAQ, [Online]. Available: http://www.iso27001security.com/html/faq.html.

[KGSR02] M. Ashwin Kumar, P. R. Goundan, K. Srinathan und C. P. Rangan, On perfectly secure communication over arbitrary networks, Proceedings of the twenty-first annual symposium on Principles of distributed computing, 2002.

[KoWS08] S. Kollarits, N. Wergles und H. Siegel et al., MONITOR - An ontological basis for risk management, 2008. [Online]. Available: http://www.monitor-cadses.org.

[MEHA04] Clusif Methods Commission, MEHARI V3 Risk Analysis Guide, 2004.

[NeMo44] J. von Neumann und O. Morgenstern, Theory of games and economic behavior, Princeton University Press, 1944.

[Pelt01] T. R. Peltier, Information security risk analysis, Auerbach Publications, 2001.

[RAM10] European Network and Information Security Agency, Inventory of Risk Management / Risk Assessment Methods, 2010. [Online]. Available: rminv.enisa.europa.eu/rm_ra_methods.html.

[Rass09] S. Rass. On Information-Theoretic Security: Contemporary Problems and Solutions, PhD thesis, Alpen-Adria Universität Klagenfurt, Institute of Applied Informatics, June 2009

[Sche04] S. E. Schechter, Computer security strength and risk: a quantitative approach, Harvard University, 2004.

[Shan49] C. Shannon, Communication Theory of Secrecy Systems, Bell System Technical Journal, Nr 28, pp. 656-715, 1949

[StGF02] G. Stoneburner, A. Goguen und A. Feringa, Special Publication 800-30: Risk Management Guide for Information Technology Systems, National Institute of Standards and Technology, 2002.

[WaDe08] Y. Wang und Y. Desmedt, Perfectly Secure Message Transmission Revisited, IEEE Transactions on Information Theory, Bd. 54, Nr. 6, pp. 2582-2595, 2008.