Sicherheit auf Basis Multikriterieller Spieltheorie

Stefan Rass[1] · Stefan Schauer[2] · Andreas Peer[3] · Johannes Göllner[3]

[1]Alpen-Adria Universität Klagenfurt
stefan.rass@aau.at

[2]Austrian Institute of Technology
stefan.schauer@ait.ac.at

[3]Bundesministerium für Landesverteidigung und Sport (BMLVS)
{andreas.peer | johannes.goellner}@bmlvs.gv.at

Zusammenfassung

Quantitatives Risiko-Management im Bereich sicherer Kommunikation ist ein relativ junger Ansatz der Systemsicherheit. Hierbei wird der Konflikt zwischen Angreifer und Verteidiger als mathematisches Spiel dargestellt, in welchem beiden Seiten versuchen, ihre Ziele optimal unter Berücksichtigung der Aktionen des jeweiligen Gegners umzusetzen. Solche Betrachtungen sind i.A. strikt eindimensional, d.h. fokussiert und spezifisch für ein Sicherheitsziel. Der vorliegende Beitrag beschreibt eine theoretische und praktische Verallgemeinerung des spieltheoretischen Ansatzes zur simultanen Betrachtung multipler Sicherheitsziele (Vertraulichkeit, Verfügbarkeit und Authentizität), insbesondere unter Rücksichtnahme auf Wechselwirkungen zwischen einzelnen Zielen. Hierdurch wird – ähnlich wie bei einem Virtual Private Network (VPN) – ein sicherer Kommunikationskanal geschaffen, dessen Sicherheit – anders als bei einem VPN – nicht in qualitativen Zusicherungen, sondern in quantitativen Maßstäben (Wahrscheinlichkeiten) ausgedrückt wird. Da die eingesetzten Verfahren ohne Public-Key Kryptographie auskommen, entfällt hierbei auch das sonst übliche Zertifikats- und Schlüsselmanagement.

1 Einführung

Die Sicherheit kryptographischer Basismechanismen wird zumeist qualitativ ausgedrückt, etwa in Form (unscharfer) Zusicherungen in Anbetracht des aktuellen Standes der Technik oder nominellen Schadens- bzw. Risiko-Bewertungen im Falle von (nicht kryptographischen) Bedrohungen. Risiko-Management dient im weiteren Sinne der Kontrolle und Limitierung des durch Bedrohungen für ein IT-System erwarteten Schadenspotentials. Im engeren Sinne wird hierbei quantitatives von qualitativem Risikomanagement abgegrenzt. Letzteres basiert auf den eingangs erwähnten nominellen Bewertungskategorien bzw. qualitativen Schutz-Zusicherungen auf Basis wissenschaftlicher Forschung, Erfahrungen und Best-Practices.

Quantitatives Risiko-Management versucht, Sicherheit im Hinblick auf Kosten-Nutzen-Entscheidungen über die Anschaffung bzw. den Ausbau der Sicherheitsfunktionalitäten einer vorhandenen IT-Infrastruktur „numerisch zu quantifizieren“, also zu messen. Dieser Ansatz

P. Schartner · P. Trommler (Hrsg.) · D•A•CH Security 2013 · syssec (2013) 289-301.

ist in der Praxis aufgrund des hohen Aufwandes und den schwierig zu beschaffenden Eingabegrößen für eine qualitativ gute Modellbildung eher selten anzutreffen. Er steht insbesondere nicht im Vordergrund der empfohlenen Herangehensweisen für IT-Risikomanagement.

Spieltheorie wird in jüngster Zeit in der IT, insbesondere der Systemsicherheit, eingesetzt, um die „natürliche" Konfliktsituation zwischen Angreifer und Sicherheitsexperten in konkreten Kommunikationsinfrastrukturen zu modellieren. Hierbei modelliert man die Gegebenheiten und Eigenschaften eines Kommunikationsnetzwerkes in einer Weise, welche eine Simulation von Angriffen und Gegenmaßnahmen innerhalb eines (spieltheoretischen) Modells ermöglicht, sodass optimale Verhaltensweisen sowohl für den Angreifer als auch für den (die) Verteidiger (z.B. Sicherheitsverantwortliche) ermittelt werden können.

Bei einer geeigneten Modellierung – Details hierzu folgen in Abschnitt 1.1 – wird hierdurch eine Abschätzung des zu erwartenden, maximalen Schadens ermöglicht. Diese Abschätzung ist unabhängig vom tatsächlichen Verhalten des Angreifers, solange dieser sich innerhalb einer, für das Szenario vorgegebenen, Menge der Angriffsmöglichkeiten (z.B. maximale Anzahl an Paket-Sniffer) bewegt. Diese Art der Modellierung ist inhärenter Bestandteil jedweder Sicherheitsauditierung und kann für die Modellbildung als verfügbare Information betrachtet werden.

Sowohl quantitativen als auch qualitativen Verfahren zum Risiko-Management ist gemeinsam, dass i.d.R. nur ein einzelnes Sicherheitsziel – etwa Vertraulichkeit – Gegenstand der Betrachtung ist. Wechselwirkungen zwischen Sicherheitszielen (etwa Verfügbarkeit vs. Vertraulichkeit) oder Implikationen einzelner Schutzmaßnahmen für andere Performanz-Parameter als Sicherheit (etwa Bandbreite) müssen gesondert berücksichtigt werden. Im Allgemeinen sind derartige Betrachtungen in existierenden Standards und Verfahrensempfehlungen (vgl. [Münc12]) nicht vorgesehen.

Der vorliegende Beitrag beschreibt die Grundlagen und Ziele des Projektes *Risiko-Management für simultane Bedrohungen* (RSB). Dieses, von der österreichischen Forschungsförderungsgesellschaft im Rahmen des KIRAS Programmes geförderte, Projekt (Projekt-Nr. 836287) wird vom Austrian Institute of Technology (als Projekt-Koordinator) in Zusammenarbeit mit der Firma SiteXs Databusiness IT-Solutions GmbH, der Alpen-Adria Universität Klagenfurt, als auch den Österreichischen Bundesministerien für Inneres bzw. für Landesverteidigung und Sport (Landesverteidigungsakademie Wien / Abteilung für Zentraldokumentation und Information) durchgeführt.

Ein geplantes Ergebnis der im RSB-Projekt entwickelten Methode und Prototypen ist der (technische) Aufbau von sicheren Kommunikationskanälen innerhalb von IT-Infrastrukturen eines Unternehmens, wobei *simultan* das Risiko für Ausfälle, Abhören oder das Einschleusen von nicht-authentischen Nachrichten optimiert werden soll. Dies bedeutet, dass für jedes dieser drei Sicherheitsziele eine individuelle Risiko-Abschätzung durchgeführt wird, welche explizit potentiell vorhandene Wechselwirkungen bei der Optimierung berücksichtigt. Somit kann – ähnlich einem Virtual Private Network (VPN)– ein Kommunikationskanal aufgebaut werden, welcher sowohl verfügbar, als auch vertraulich, als auch authentisch ist, mit der Besonderheit, dass hierbei keine Public-Key Kryptographie verwendet wird. Somit entfällt das sonst übliche Zertifikats- und Schlüsselmanagement für diese Art der Kommunikation.

Sicherheit wird in diesem Kontext als Wahrscheinlichkeit für eine Verletzung eines der drei Sicherheitsziele (Informationsverlust, Ausfall des Kanals oder Einschleusen von Nachrichten) gemessen, womit die Methode in den Bereich des quantitativen Risikomanagements fällt.

Der gesamte Ablauf ist grob in Abbildung 1 skizziert. Details zu den Blöcken „spieltheoretisches Modell“ und „Solver“ sind im nachfolgenden Abschnitt sowie in Abschnitt 3 zu finden.

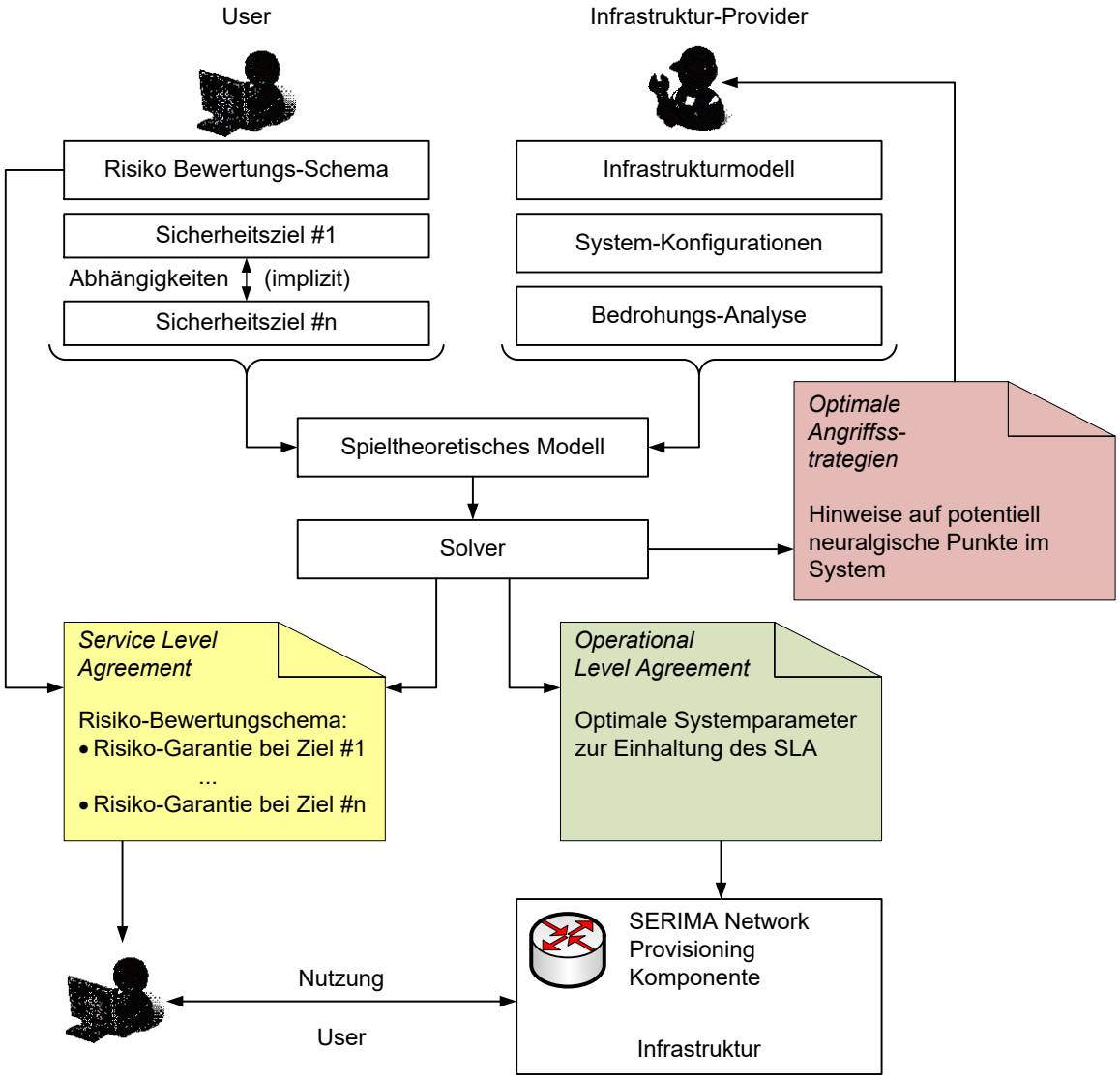

Abb.1: Ablauf der Risiko-Bewertung

1.1 Spieltheoretische Sicherheit und das SERIMA Projekt

Das Vorgängerprojekt SERIMA (IT-Security-Risk-Management based on Decision-Theory), war eine erste Umsetzung von risiko-minimaler Kommunikation auf Basis einer Mehrwege-Übertragung. Wir verweisen für Details auf [ScRR12] und betrachten nur die wesentlichen Ergebnisse, auf denen die im RSB-Projekt beschriebene Verallgemeinerung aufbaut.

Die Grundidee der in SERIMA verfolgten spieltheoretischen Methode besteht darin, die Kommunikationswege über ein Netzwerk in solcher Weise randomisiert zu wählen, dass ein Angreifer, welcher den Netzverkehr auf einer begrenzten Höchstzahl von Knoten mitliest, eine möglichst geringe Chance hat, Informationen aus den codierten Daten abzuleiten.

Der in SERIMA entwickelte Prototyp verwendet hierfür ein Graphenmodell des Kommunikationsnetzwerkes und steuert mit Hilfe aktiver Netzwerkkomponenten (Router) und Virtual LANs den Netzverkehr in geeigneter Art, um einem (oder mehreren) zufällig im Netzwerk platzierten Paket-Sniffern auszuweichen. Sowohl die Positionen der Sniffer, als auch die Auswahl der Kommunikationswege wird hierbei simultan optimiert. Formal liegt dieser Optimierung ein mathematisches Nullsummenspiel (Gewinn des Angreifers = Schaden des Senders) zu Grunde.

Die Struktur dieses Nullsummenspiels lautet wie folgt: Wir bezeichnen mit PS_1 die Menge aller Sende-Parameter (etwa Übertragungswege), und mit PS_2 die Menge aller möglichen Penetrationsstrategien (z.B. Platzierungen von Sniffern). Weiter seien x, y Wahrscheinlichkeitsverteilungen über PS_1 bzw. PS_2, welche eine zufällige Auswahl von Übertragungsparametern oder Angriffsstrategien bezeichnen. Abschließend sei $u(s_1, s_2)$ eine Indikatorfunktion, welche den Erfolg $(u = 1)$ oder Misserfolg $(u = 0)$ einer Übertragung im Szenario $(s_1, s_2) \in PS_1 \times PS_2$ misst. Dann liefert die Analyse eine Erfolgswahrscheinlichkeit

$$v \coloneqq u(x^*, y^*) \geq u(x^*, y) \text{ für } \textit{beliebiges } y, \tag{1}$$

d.h. der zu erwartende Gewinn im Nullsummenspiel ist stets größer oder gleich dem Gewinn, welcher sich ergibt, wenn der Angreifer sich anders verhält als durch das Nullsummenspiel prognostiziert. Obgleich eine Nullsummenspielannahme dem Angreifer ein sehr bestimmtes (und in Folge dessen wahrscheinlich nicht reales) Verhalten unterstellt, kann gezeigt werden [Rass09], dass Ungleichung (1) eine *scharfe* Schranke darstellt, welche auch bei anderem Verhalten des Angreifers erreicht werden kann.

Der Wert $1 - v =: \rho$ stellt somit eine quantitative Risiko-Schätzung für die Wahrscheinlichkeit eines Angriffes auf die gegebene Kommunikationsbeziehung dar (vgl. [Aven07] für einen verwandten Ansatz). Dieser Wert wird durch den SERIMA-Prototypen ermittelt und die dafür erforderliche randomisierte Bewirtschaftung der Kommunikationsinfrastruktur von eigens hierfür entwickelten Protokollen und Network-Provisioning-Komponenten umgesetzt.

1.2 Multikriterielle Spiele

Die in Abschnitt 1.1 skizzierte Methode wurde für Vertraulichkeit entwickelt, kann jedoch auf andere Sicherheitsziele wie etwa Verfügbarkeit oder Authentizität ausgedehnt werden (siehe [RaSc10]). Die Betrachtung ist jedoch in allen Fällen strikt eindimensional, d.h. es können keine Wechselwirkungen zwischen Sicherheitszielen berücksichtigt werden.

Auf theoretischer Ebene lässt sich die in SERIMA verwendete Modellierung nicht auf mehrere Dimensionen ausweiten, da die benötigten Eigenschaften der „≤“-Relation verlorengehen (Ungleichung (1) besteht nicht mehr).

Um dies zu beheben, wurde Ungleichung (1) in [Rass13] nicht als Folge eines Modells, sondern als geforderte bzw. definierende Eigenschaft einer multikriteriellen Risiko-Bewertung festgelegt. Der sich daraus ableitende, axiomatische Ansatz beschreibt das Kommunikationsrisiko für n Sicherheitsziele als einen Vektor$(v_1, v_2, \dots, v_n)$. Analog zu den Ausführungen in Abschnitt 1.1 gehen wir wieder von einer (Indikator-)Funktion u_i für das i-te Sicherheitsziel aus, welche den jeweiligen Erfolg bzw. Misserfolg misst (etwa die erfolgreiche Rekonstruktion geheimer Informationen durch einen Angreifer, gemessen durch u_1, oder eine erfolgte Denial-of-Service (DoS) Attacke auf dem Kanal, gemessen durch u_2, etc.).

Eine sog. *effiziente Risiko-Zusicherung* $(v_1, v_2, \dots, v_n)$ im Sinne von n gegebenen Zielen, gemessen durch $u_1, u_2, \dots, u_n$ bei jeweiligen Verhaltensprofilen $(x, y) \in PS_1 \times PS_2$ ist dann charakterisiert durch folgende Eigenschaften:

1. **Zusicherung:** Es existiert ein Verhaltensprofil x^* (eine Wahrscheinlichkeitsverteilung über PS_1), mit der Eigenschaft, dass $v_i \geq u_i(x^*, y)$ für beliebiges y (analog möge somit Ungleichung (1) für jedes Sicherheitsziel einzeln gelten), wobei für jedes Sicherheitsziel ein Angriffsprofil y_i existiert, bei welchem genau der Gewinn v_i erreicht wird (die Schranke soll scharf sein).
2. **Effizienz:** Es gibt kein Verhaltensprofil $x' \neq x^*$ für das in allen Belangen echt bessere Zusicherungen $v_1' > v_1, v_2' > v_2, \dots, v_n' > v_n$ existieren (d.h. die Zusicherung ist nicht gleichmäßig verbesserbar).

Die theoretischen Grundlagen betreffend die Existenz und Bestimmung einer so definierten effizienten Risiko-Zusicherung wurden in [Rass13] geschaffen (vgl. auch [Ghos91], [Voor99], [AcRa05] für verwandte Vorgängerarbeiten) und werden im Rahmen des RSB-Projektes mit geeigneten kryptographischen Verfahren umgesetzt. Diese werden in Abschnitt 2 genauer beschrieben. Man beachte insbesondere, dass für diese Definition von Risiko-Zusicherungen (und somit auch für deren Bestimmung) kein explizites Modell für die Wechselwirkungen zwischen einzelnen Sicherheitseigenschaften erforderlich ist. Diese Abhängigkeiten werden implizit durch die Spezifikation der Indikatorfunktionen berücksichtigt. Darüber hinaus besteht die Möglichkeit, einzelne Sicherheitsziele abhängig von deren Bedeutung individuell zu gewichten, um Präferenzen und Prioritäten zwischen verschiedenen QoS (Quality of Security/Service) Parametern abzubilden (siehe Schritt 3 der Analyse in Abschnitt 3.3).

2 Verfahren für risikominimale Kommunikation

In diesem Abschnitt skizzieren wir kurz die eingesetzten Verfahren, welche Vertraulichkeit, Authentizität und Ausfallssicherheit im Sinne einer quantitativen Risikobewertung zusichern.

2.1 Vertraulichkeit

Vertrauliche Kommunikation ohne Public-Key Kryptographie und ohne Rückgriff auf komplexitätstheoretische Annahmen über schwierige Probleme wird in RSB durch einfache Mehrwegeübertragung (vgl. etwa [FFGV07], [WaDe08]) realisiert. Hierbei werden redundante Übertragungskanäle ausgenützt, welche i.A. zum Zwecke der Ausfallssicherheit in Referenz-Netzwerkarchitekturen vorhanden sind. Die Idee der eingesetzten Mehrwegeübertragung besteht kurz gesagt darin, die im Netzwerk vorhandenen Kanäle wahlweise (zufällig gemäß der optimalen Verteilung x^* aus der spieltheoretischen Analyse) für eine Kommunikation auszuwählen, sodass ein Angreifer, der eine Menge von Knoten im Netzwerk (fester Anzahl aber variabler Platzierung) kompromittiert hat, nur eine minimale Wahrscheinlichkeit (gemessen durch die Indikatorfunktion u_1) für einen erfolgreichen Abhörangriff besitzt. Der Informationsschutz geschieht durch Verfahren des Secret-Sharing (vgl. etwa [FFGV07]). Für Details zur Umsetzung der Mehrwegeübertragung möchten wir an dieser Stelle auf [ScRR12] verweisen.

2.2 Authentizität

Analog zur Mehrwege-Übertragung verfolgt Mehrwege-Authentifizierung die Idee, Ende-zu-Ende Authentizität aus Punkt-zu-Punkt Authentizität zu erzeugen. Dazu nehmen wir an, Alice hat mit N (direkten) Nachbarn geheime Schlüssel $k_1, k_2, \dots, k_N$ ausgetauscht. Um ihrem Empfänger Bob, mit welchem Alice keinen Schlüssel teilt, eine Nachricht m authentisch zukommen zu lassen, führt Alice folgendes Protokoll durch: Sie erzeugt mit jedem der N„Nachbar-Schlüssel" einen Message-Authentication Code $MAC(H(m), k_i)$ für den Hash-Wert $H(m)$ der Nachricht m. Der Empfänger Bob kann nun die Nachbarn von Alice kontaktieren und um eine Verifikation des Hashwertes und MACs ersuchen. Dabei ist hervor zu heben, dass keiner der Nachbarn die Nachricht selbst kennt, sondern lediglich deren Hashwert erhält. Somit bleibt m geheim und Bob akzeptiert die Nachricht als authentisch, genau dann, wenn alle Verifizierungsanfragen positiv beantwortet werden (Indikator-Funktion u_2).

Dieses Verfahren lässt sich sehr einfach als Spiel modellieren und bietet auf Grundlage der Kollisionsresistenz der Hash-Funktion, welche im Falle von universellen Hash-Funktionen [CaWe81] als gegeben angenommen werden kann, Authentizitätssicherheit gegen bis zu $N - 1$ kompromittierte Knoten (siehe [RaSc10] für Details).

2.3 Verfügbarkeit

Verfügbarkeit wird i.A. durch redundante Kanäle erreicht. Dies ist trivial als Spiel zwischen einem DoS-Angreifer und dem Netzwerk modellierbar. Ergebnis des Spiels ist die maximale Ausfallswahrscheinlichkeit (Funktion u_3). Die Entscheidung über den Spielausgang in jedem Szenario wird hierbei durch die Fähigkeit der eingesetzten Codierung bestimmt, eine Menge von fehlenden bzw. manipulierten Nachrichtenblöcken unter den (durch das Szenario gegebenen) Umständen zu korrigieren. In [FFGV07] etwa kommen hierfür lineare Block-Codes zum Einsatz, deren Korrekturleistung bekannt ist, und die Basis hierfür liefert.

3 Modellbildung und Analyse

Für die Modellbildung gehen wir von einem Graphenmodell als Abstraktion der Kommunikationsinfrastruktur aus. Hierbei handelt es sich um einen annotierten Graphen, in welchem jedem Knoten eine Liste von Eigenschaften (etwa Administrationspersonal, Zugriffschutzmaßnahmen, physikalische Position, Hersteller und Firmware-Version, etc.) beigefügt wird. Aus einer Spezifikation möglicher Angriffsstrategien im Sinne dieser Eigenschaften (etwa bekannte Sicherheitslücken bestimmter Firmware-Versionen oder mangelnder bzw. nicht spezifizierter physikalischer Zugriffsschutz) bildet das System die Menge PS_2 der Angriffsstrategien, mit welcher später das spieltheoretische Multi-Kriterien-Modell erzeugt und analysiert wird. Für die Analyse und Definition der benötigten Strategiemengen wird auf das *Doppelvektor-Modell* [GMPP11a] zurückgegriffen.

3.1 Das Doppel-Vektor Modell

Die Komplexität von Systemen und die Etablierung einer gemeinsamen Terminologie machen Kategorisierungsmodelle erforderlich, um Systemkomponenten und -elemente klassifizieren zu können. Dieser Ansatz garantiert einen normierten und analytischen Prozess, um Ergebnisse und verschiedene Elemente und Komponenten miteinander vergleichen zu können. Dazu wurde das sogenannte Doppelvektorenmodell auf Basis einer ersten Kategorisierungsebene

(Metakategorisierungsebene) im Rahmen des BMLVS-internen Forschungsprojektes „Szenarioplanung und Wissensmanagement im ÖBH“ im Zeitraum 2010 – 2013 durch Johannes Göllner, Klaus Mak, Christian Meurers, Andreas Peer und Günther Povoden entwickelt.

Die Kategorisierungs-Systematik des Doppelvektorenmodells ist in der nachfolgenden Abbildung dargestellt.

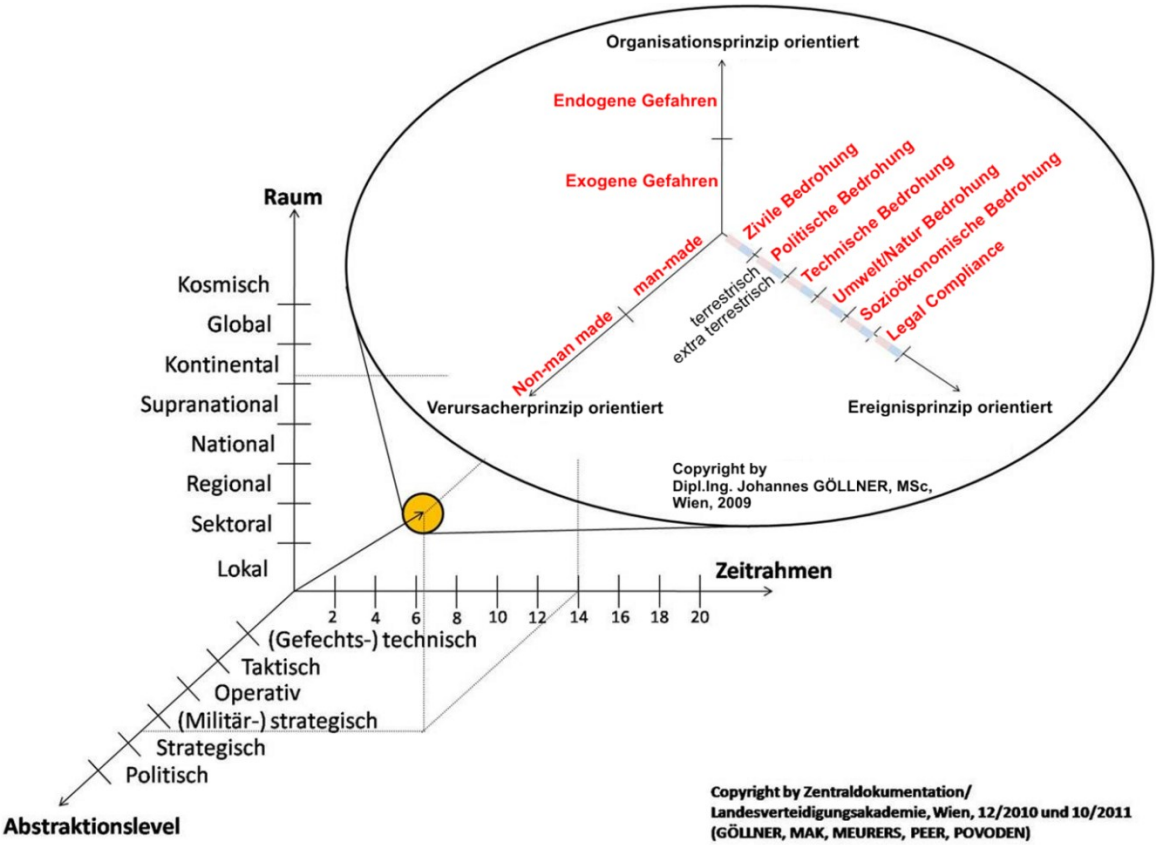

Abb.2: Doppelvektorenmodell

Das Doppelvektorenmodell stellt ein dreidimensionales, mehrstufiges Meta-Klassifikationssystem darstellt, in dem jedes Element über die vektorielle Zuordnung von definierten Eigenschaften und Attributen dargestellt und beschrieben werden kann.

Der eine Vektor unterscheidet die Ordinaten nach zeitlichen und räumlichen Aspekten und bietet einen organisations- bzw. ebenenspezifischen Abstraktionslevel an (politisch, strategisch, militärstrategisch, operativ, taktisch, gefechtstechnisch).

Der andere Vektor kategorisiert das Ereignis hinsichtlich des Verursachers und ob organisationsimmanente Gefahren einwirken oder resultieren. Zusätzlich kann/muss das Ereignis im Rahmen der Ereignisprinzip-Achse auch unter Berücksichtigung des Ursprunges (terrestrisch, extraterrestrisch) weiter kategorisiert werden.

Das Doppelvektorenmodel bietet somit eine normierte Basis für weitere Analysen.

Nachfolgend sind die beiden Vektoren (Vektorenebenen) detailliert beschrieben:

Vektor 1 [GMPP11a, GMPP11b, GMPP11c, GöPe11,MaGö11,Göll12] :

- Raum: Lokal, Sektoral, Regional, National, Supranational, Kontinental, Global, Kosmisch

- Abstraktionslevel: (Gefechts-)technisch, Taktisch, Operativ, (Militär-) strategisch, Strategisch, Politisch
- Zeitrahmen: Sekunde, Minute, Stunde, Tage, Wochen, Monate, Jahre, Jahrzehnte, Jahrhunderte

Vektor 2 [Göll09]:

- Organisationsprinzip-orientiert: Exogene Gefahren, Endogene Gefahren
- Verursacherprinzip-orientiert: Man-made, Non-man-made
- Ereignisprinzip-orientiert (terrestrisch/extraterrestrisch): Zivile Bedrohung (die Bezeichnung „Bedrohung“ kann stellvertretend auch für die Bezeichnungen Ereignis, Gefahr und Bedrohung stehen), Politische Bedrohung, Technische Bedrohung, Umwelt/Natur Bedrohung, Sozioökonomische Bedrohung, Legal Compliance.

Das Doppelvektorenmodell wurde in mehreren Anwendungsfällen erarbeitet, weiterentwickelt sowie getestet und stellt die Möglichkeit dar, ereignisrelevanten Inhalt zu dokumentieren und für weitere Analysen abrufbar zur Verfügung zu stellen. Auch lassen sich Muster zu diversen Ereignissen in spezifischen Kategorien damit erkennen, was einen weiteren Mehrwert im Rahmen des KIRAS Forschungsprojektes *Risiko-Management für simultane Bedrohungen* (RSB) darstellt.

3.2 Modellbildung

In abstrahierter Form besteht das Infrastrukturmodell aus einem ungerichteten Graph, in welchem die Knoten Kommunikationspunkte (also potentielle Nachrichtenquellen bzw. –senken) und deren direkte physikalische Verbindungen bezeichnen. Jeder Knoten ist mit einer Liste von Attributen, wie etwa der physikalischen Position, dem Zugangsschutz (versperrter Raum, Zugangskontrolldetails, etc.), dem zuständigen Administrationspersonal, dem zuständigen Reinigungspersonal, der Firmware- bzw. Betriebssystemversion und ähnlichem versehen. Basierend auf diesen Attributen werden Angriffsstrategien als hinreichende Bedingungen für einen Angriff formuliert. Konkret könnte etwa eine Angriffsstrategie in der Kombination aus mangelndem Zugriffsschutz (z.B. ein unversperrter Raum) und veralteter Firmware-Version (z.B. Versionsnummer zu klein, daher aktuell kein Schutz gegen bekannte Bedrohungen) bestehen. Innerhalb der Modellbildungssoftware werden solche Szenarien als logische Ausdrücke über der Menge der bekannten Attribute definiert, z.B.:

```
room_locked = isnotset,
os_version <= 1.6
```

wobei jede Zeile einem Attribut entspricht und die Zeilen UND-Verknüpft zu interpretieren sind. Die Menge angreifbarer Knoten, die sich aufgrund dieser Bedingungen ergibt, bildet einen Eintrag in der Strategiemenge PS_2. Die gesamte Menge PS_2 wird gemäß den formulierten Angriffsstrategien automatisch ermittelt.

Die Menge PS_1 der Übertragungsstrategien ist abhängig von den definierten Kommunikationsendpunkten. In der vorliegenden Version ermittelt das System das Risiko der Kommunikation für zwei beliebige (aber fest vorgegebene) Endstellen A und B. Die Menge PS_1 ergibt sich durch eine Enumeration der Kommunikationspfade von A nach B innerhalb des Netzwerkgraphen. Sollten redundante Wege vorhanden sein, so können auch zwei oder mehr Pfade zu einem Bündel zusammengefasst werden. Einzelne Pfade oder Pfad-Bündel (Mehrwegeübertragung) bilden dann die Einträge der Strategiemenge PS_1.

Jedes der drei betrachteten Sicherheitsziele (Vertraulichkeit, Authentizität und Verfügbarkeit) führt hierbei zu einem individuellen, spieltheoretischen Modell, welches durch sukzessive Szenario-Analyse über der Menge $PS_1 \times PS_2$ in drei Spielmatrizen übersetzt wird. Abbildung 3 skizziert dieses Vorgehen und stellt die Positionierung der Abläufe innerhalb des Systems dar.

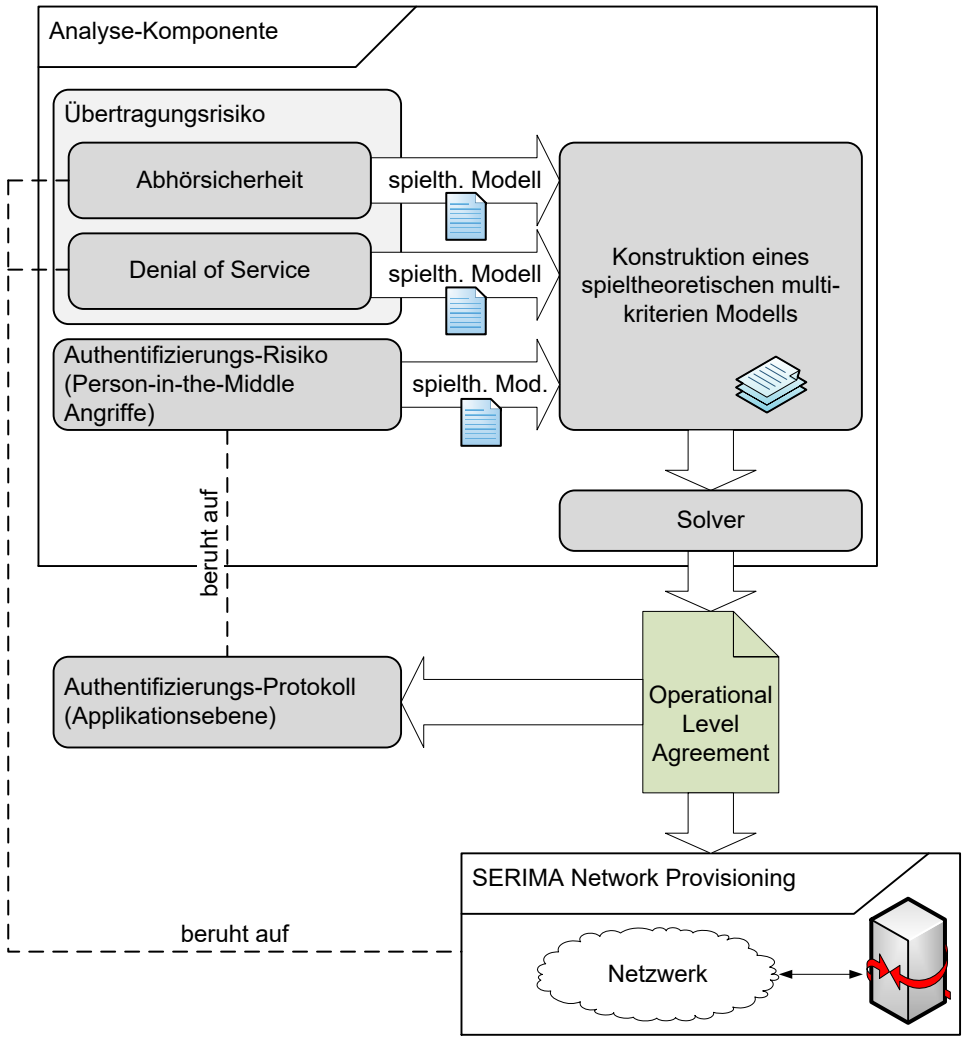

Abb. 3: Architektur des RSB-Prototypen (Auszug)

3.3 Durchführung der Analyse

Das spieltheoretische Modell besteht in der Form, welche in die Analyse eingeht, aus drei Komponenten:

1. Die Liste PS_1 der Übertragungsstrategien.
2. Die Liste PS_2 der Angriffsstrategien.
3. Eine Menge von Spielmatrizen; je eine für jedes der gewählten Sicherheitsziele.

Für jedes Sicherheitsziel ist die Spielmatrix von der Form $A \in \{0,1\}^{|PS_1| \times |PS_2|}$, wobei die Werte $a_{ij} = 0$ bzw. $a_{ij} = 1$ für das Scheitern bzw. den Erfolg der Übertragungsstrategie $i \in PS_1$ unter Berücksichtigung der Angriffsstrategie $j \in PS_2$ ermittelt werden. Die Bewertung der

einzelnen Szenarien erfolgt für jedes Sicherheitsziel gesondert innerhalb der Simulationskomponente (das Vorgehen ist hierbei analog zum SERIMA Projekt, vgl. auch [ScRR12]).

Die gesuchte effiziente Risiko-Zusicherung für k Sicherheitsziele ergibt sich gemäß den Ergebnissen von [Rass13] als Pareto-Nash Gleichgewicht eines, aus den obigen Eingaben abgeleiteten, multikriteriellen k-Personenspiels. Numerisch wird das gesuchte Gleichgewicht durch ein Iterationsverfahren (*fictitious play*) ermittelt. Dieses Verfahren bildet das Kernstück der Solver-Komponente, deren interner Ablauf sich grob wie folgt darstellt:

1. Aufstellung des multikriteriellen 2-Personenspiels gemäß [Rass13], aus welchem sich die gesuchte Risiko-Bewertung ableiten lässt.
2. Transformation in ein skalares k-Personenspiel, gemäß dem in [LSZ05] angegebenen Verfahren. Die Transformation besteht im Wesentlichen aus einer herkömmlichen gewichteten Summe der einzelnen Sicherheitsziele. Die hierbei einfließenden Gewichte sind frei wählbar und vom Benutzer in Form einer Priorisierung der Sicherheitsziele beliebig im Rahmen der Modellbildung vorgebbar. Eine Vorgabe durch den/die Anwender/in ist allerdings nicht zwingend erforderlich, da die Wahl der Gewichte lediglich Einfluss darauf nimmt welches konkrete Nash-Gleichgewicht berechnet wird, jedoch nicht darüber entscheidet, ob überhaupt eine Lösung gefunden wird (es wird stets ein Gleichgewicht gefunden).
3. Lösung des entstehenden skalaren k-Personenspiels mittels „fictitious play“ gemäß [Sel99]. Hierbei handelt es sich um ein Iterationsverfahren, welches zwar garantiert, jedoch ggf. nur langsam konvergiert. Dieser Schritt wird durch besonders leistungsfähige Hardware unterstützt, um eine entsprechende Beschleunigung des Vorgangs zu ermöglichen.

Das Ergebnis der Analyse ist eine effiziente Risiko-Zusicherung im Sinne der axiomatischen „Definition“ wie in Abschnitt 1.2 beschrieben und in Abbildung 1 skizziert.

4 Testfälle und Anwendungsbeispiele

Zur Evaluation der Methodik und zur Bewertung der Praxistauglichkeit wurde als Testumgebung eine „künstliche“ Kommunikationsinfrastruktur geschaffen. Dies dient (neben Datenschutzaspekten) einer möglichst allgemeinen (generischen) Beschreibung der Infrastruktur, sodass mit einem Minimum an Eignungsbedingungen für die Modellbildung ein möglichst breites Spektrum an realen Infrastrukturen modelliert werden kann. Zu diesem Zweck wurde die Testumgebung unter Berücksichtigung von Best-Practices und Referenz-Netzwerkarchitekturen gebildet, sodass ähnliche Strukturen in einer Vielzahl realer Netzwerke zu erwarten sind.

Es handelt sich bei dieser künstlichen Kommunikationsinfrastruktur um die IT-Infrastruktur eines global agierenden Konzernes mit ca. 20.000 Mitarbeitern und auf allen Kontinenten verteilten Standorten. Die Analyse liefert hierbei eine Risiko-Bewertung der Datenkommunikation sowohl innerhalb als auch zwischen Standorten (etwa beim Austausch von Forschungsergebnissen oder Produkten kurz vor Markteintritt, etc.). Für Details sei an dieser Stelle auf [GPR13] verwiesen, wo eine ausführliche Beschreibung der verwendeten Infrastruktur zu finden ist.

5 Resümee und Ausblick

Die in RSB betrachteten Sicherheitsziele sind aktuell Vertraulichkeit, Authentizität und Verfügbarkeit. Die Betrachtung anderer Sicherheitsziele wie Anonymität oder Nicht-Zurückweisbarkeit ist Gegenstand laufender Forschung. In jedem Fall setzt die Analyse die Möglichkeit der Ausnützung von „Freiheitsgraden" bei der Durchführung eines Protokolls voraus, welche jedoch über den üblichen Einsatz von Zufallszahlen im kryptographischen Kontext hinausgeht. Somit bestehen zwar Möglichkeiten, Anonymitätsprotokolle im vorgeschlagenen Sinne zu untersuchen, jedoch ist eine analoge Behandlung qualitativer Ziele wie Nicht-Zurückweisbarkeit ein gänzlich ungelöstes Problem.

Aktuell existieren Ansätze für spieltheoretische Risiko-Betrachtungen im Bereich der Netzwerksicherheit und Kryptographie (vgl. etwa [AlBa10], [ABE+06] oder [ACN+07]), jedoch gelingt keinem bestehenden Ansatz eine multikriterielle Bewertung. Die theoretischen Grundlagen hierfür sind zwar bekannt, jedoch aktuell wenig verbreitet; insbesondere fehlt eine umfassende Umsetzung, welche das Potential der (bislang nur in der Theorie vorhandenen) Verfahren praktisch ausloten lässt. Die vorliegende Arbeit soll einen ersten Grundstein hierfür legen. Ein besonderer Vorteil der Risiko-Bewertungsmethode liegt insbesondere in der Ersparnis, weder das Verhalten des Angreifers (sondern nur dessen Möglichkeiten), noch die Wechselbeziehungen zwischen einzelnen Sicherheitszielen modellieren zu müssen. Beides wird automatisch und implizit durch die spieltheoretische Betrachtung optimiert bzw. abgedeckt.

Literatur

[ABE+06] E. Altman, T. Bolougne, R. El-Azouzi, T. Jiménez, L. Wynter: A survey on networking games in telecommunications. In: *Elsevier Journal on Computers & Operations Research*, 33 (2006), 286–311.

[ACN+07] J. Alwen, C. Cachin, J. B. Nielsen, O. Pereira, A.-R. Sadeghi, B. Schomakers, A. Shelat, I. Visconti: D.PROVI.7 Summary Report on Rational Cryptographic Protocols. *Tech. Rep. IST-2002-507932, ECRYPT European Network of Excellencein Cryptology*, University of Aarhus (BRICS) (2007).

[AcRa05] F. Acosta Ortega, C. Rafels Pallarola: Security Strategies and Equilibriain Multiobjective Matrix Games. *Working Papers in Economics 128*,Universitat de Barcelona.Espai de Recerca en Economia (2005).

[AlBa10] T. Alpcan, T. Başar: Network Security: A Decision and Game Theoretic Approach.*Cambridge University Press* (2010).

[Aven07] T. Aven: A unified framework for risk and vulnerability analysis covering bothsafety and security. In: *Reliability Engineering & System Safety*, 92, 6 (2007),745-754.

[CaWe81] J. Carter, M. Wegman: Universal classes of hashing functions, in: *Journal of Computer and System Sciences*, vol. 22, (1981), 265-279.

[FFGV07] M. Fitzi, M. K. Franklin, J. Garay, S. H. Vardhan: Towards Optimal and EfficientPerfectly Secure Message Transmission. In: S. Vadhan (Hrsg.), *4th Theoryof Cryptography Conference (TCC)*, Lecture Notes in Computer Science LNCS4392, Springer (2007), 311-322.

[Ghos91] D. Ghose: A necessary and sufficient condition for Pareto-optimal security strategies in multicriteria matrix games. In: *Journal of Optimization Theory and Applications*,68, 3 (1991), 463–481.

[Göll09] J. Göllner: Eigendefinition von 06/2009 iRd LVA Risikomanagement, Vorlesungspräsentation an der Donau Universität Krems und Integraler Bestandteil der internen Publikationen und Vortragsreihen der LVAk, 2009

[Göll12] J. Göllner: Beispiel- und modellhafte Darstellung einer Risikoanalyse, Raiffeisen Akademie-LG für Bankmanager an der Landesverteidigungsakademie Wien, 2012

[GöPe11] J. Göllner, A. Peer: Staatliche Sicherheit und Versorgungssicherheit am Beispiel Energie: Beispiel- und modellhafte Darstellung Kritischer Infrastrukturen und deren Inter-aktionen mit Fokus Energie, In: *World Energy Council-Landesverteidigungsakademie- Symposion*, 2011

[GMPP11a] J. Göllner, C. Meurers, A. Peer, G. Povoden: Hybridisation of Social Network Analysis in Context with other Methods for a Scenario Based Risk Analysis-Case Study: Critical Infrastructure for Energy Security in Austria. In: *7th Social Network Conference,* 2011.

[GMPP11b] J. Göllner, C. Meurers, A. Peer, G. Povoden: Systemdefinition, Systembeschreibung und Systembegrenzung zur Szenarioentwicklung und Szenariomodellierung – Teil 2: Darstellung von ausgewählten Methoden und möglichen Teilsystemen, Schriftenreihe der National Defence Academy 13/2010, S.7, Vienna, Austria, Feber 2011, ISBN: 978-3-902670-53-3.

[GMPP11c] J. Göllner, C. Meurers, A. Peer, G. Povoden: Wissensmanagement im ÖBH, Systemdefinition, Systembeschreibung und Systembegrenzung zur Szenarioentwicklung und Szenariomodellierung – Teil 3.A: Einführung in Szenarioentwicklung und Szenariomanagement-Grundlagen, Szenariotechnik und Szenarioplanung, Schriftenreihe der National Defence Academy 15/2010, S.37, Vienna, Austria, September 2011, ISBN: 978-3-902670-55-7.

[GPR13] J. Göllner, A. Peer, S. Rass: RSB Deliverable D1.2 Beschreibung einer fiktiven Unternehmensinfrastruktur, [online] http://www.syssec.at/rsb-project; http://www.ait.ac.at/research-services/research-services-safety-security/ict-security/referenzprojekte/rsb/

[LSZ05] D. Lozovanu, D. Solomon, A. Zelikovsky: Multiobjective Games and Determining Pareto-Nash Equilibria, in: *Buletinul Academiei de Stiinte a Republicii Moldova Matematica*, 2005, 3, 115-122.

[MaGö11] K. Mak, J. Göllner: Soziale Netzwerkanalyse –SNA iRd Wissensmanagement-Forschungsprojektes „Szenarienplanung und WM“ des ÖBH: Beispiel- und modellhafte Darstellung Kritischer Infrastrukturen unter Berücksichtigung der SNA, geladener Vortrage am Bundeskriminalamt des BMI, 2011

[Münc12] I. Münch: Wege zur Risikobewertung. In: P. Schartner, J. Taeger (Hrsg.), *DACH Security 2012*, syssec (2012), 326-337.

[Rass09] S. Rass: *On Information-Theoretic Security: Contemporary Problems and Solutions*, Dissertation, Alpen-AdriaUniversität Klagenfurt, 2009.

[RaSc10] S. Rass, P. Schartner: Multipath Authentication without shared Secrets and with Applications in Quantum Networks. In: *Proceedings of the International Conferenceon Security and Management (SAM)*, CSREA Press (2010), Bd. 1, 111-115.

[Rass13] S. Rass: On Game-Theoretic Network Security Provisioning. In: Springer Journalof Network and Systems Management, 21, 1 (2013), 47-64.

[ScRR12] S. Schauer, S. Rass, B. Rainer: IT-Security Risiko Management mit Elementen der Spieltheorie. In: P. Schartner, J. Taeger (Hrsg.), *DACH Security 2012*, syssec(2012), 106-117.

[Sel99] A. Sela: Fictitious play in 'one-against-all' multi-player games, In: *Economic Theory*, Springer Berlin / Heidelberg, 1999, 14, 635-651.

[Voor99] M. Voorneveld: Pareto-Optimal Security Strategies as Minimax Strategies of a Standard Matrix Game. In: *Journal of Optimization Theory and Applications*,102, 1 (1999), 203–210.

[WaDe08] Y.Wang, Y. Desmedt: Perfectly Secure Message Transmission Revisited. In: *IEEE Transactions on Information Theory*, 54, 6 (2008), 2582-2595.