MASC – Monitoring and Security of Containers

Jens Ove Lauf, Dieter Gollmann, Volker Turau
Technische Universität Hamburg-Harburg
masc@lauf.cc

1 Einführung

Der Containertransport hat sich in den letzten Jahrzehnten stark gewandelt. Automatisierung, höhere Stückzahlen, Packungsrichtlinien und eine Vielzahl neuer Vorschriften beeinflussen die tägliche Praxis der Transporteure. Diese Neuerungen verhindern jedoch nicht, dass den Versicherungen noch immer viele Frachtschäden gemeldet werden [Kap04].

Ein weltweiter Containertransport durchläuft im Rahmen der gesamten Transportkette typischerweise eine Vielzahl von Verantwortungsbereichen. Bei den Interchanges (Übergabe von Conatiner und Verantwortlichkeit) werden lediglich Containerverlust und deutliche Außenschäden entdeckt. Häufig kommt die Ware zerstört beim Empfänger an, obwohl der Container unversehrt ist und alle Interchanges ohne Beanstandungen durchlaufen wurden. Versicherungen entscheiden sich wegen der vielen Parteien oftmals für das direkte Auszahlen der Beträge, weil Ermittlungen zu kostenintensiv und wenig erfolgversprechend sind. Hohe Versicherungssummen sind die Folge.

Eine Überwachung des Container-Inneren ist notwendig, um das Auftreten von Frachtschäden exakt zu ermitteln. Schwitzwasserbildung, Türöffnung, der Sturz eines Containers, Vibration und Temperatur können leicht durch Sensoren ermittelt werden. Zusatzeinrichtungen wie RFID-Sensoren helfen herauszufinden, wann welche Ware die Containertür passiert hat. Dieses Papier stellt eine mögliche Variante der Containerüberwachung vor, bei der nicht nur die Daten im Container gespeichert, sondern gleichzeitig direkt Shipper und Versicherer zur Verfügung gestellt werden.

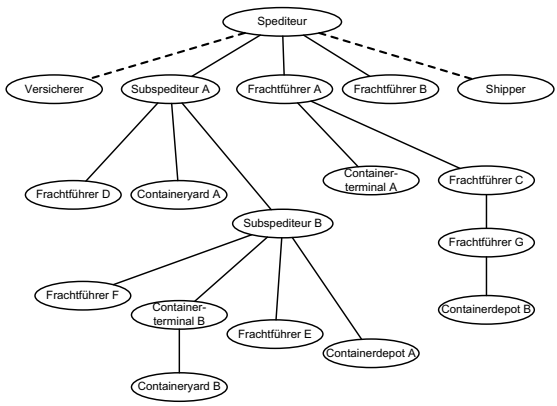
2 Motivation

Das MASC (Monitoring and Security of Containers) Projekt zielt auf eine Lösung für die Verbesserung des Containertransportes ab, ohne dabei die aktuellen Geschäftsabläufe zu sehr zu beeinflussen. Die besondere Herausforderung liegt dabei in der komplexen Vertragsstruktur, die letztendlich den Transport dezentral organisiert.

Die MASC-Anwendung sieht vor, dass einige zentrale Datenbanken alle wichtigen Informationen bezüglich eines Transportes sammeln. Da einerseits die Container Transportinformationen an diese Datenbanken senden und andererseits die am Transport beteiligten

LSPs (Logistik Service Providers) auf diese Datenbanken zugreifen, ist es notwendig, dass die Datenbanken bei gleichermaßen vertrauten Dritten untergebracht sind. Da das Logistikwesen mit den RSOs (Recognised Security Organisations) bereits über solche „Trusted Third Parties“ verfügt, ist es logisch, die Datenbank-Server bei diesen Verifizierungsorganisationen zu platzieren. Die Aufgabe der Datenbanken ist es aber nicht nur, die Sensorinformationen zu bündeln, sondern zusätzlich als verteiltes Transport-Manifest zu dienen. Hierfür ist eine dezentrale Autorisierungsstruktur notwendig.

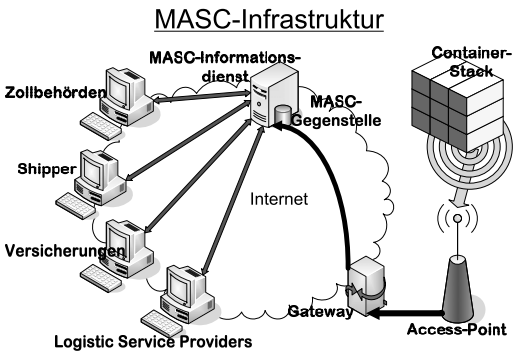
Vertragsstruktur Da viele Partner an einem Transport beteiligt sind und jeder Spediteur Unterspeditionen mit Teiltransporten oder jeder Frachtführer Unterfrachtführer beauftragen kann, existiert keine zentrale Stelle, die alle Transportbeteiligten kennt. Vielmehr ensteht eine Baumstruktur der Vertragsabhängigkeiten. Hinzu kommt, dass manchmal Schiffe ausfallen oder mehr Platz haben als angenommen. So wird oft kurzfristig entschieden, ob der Container in diesem oder dem folgenden Schiff befördert wird. Hier einen Überblick über den gesamten Transport zu haben ist wünschenswert. Natürlich haben Reedereien und Speditionen oft bereits eigene Software, aber es gibt keine Standards und übergreifende Schnittstellen.



MASC-Informationsdienst Der MASC-ID regelt den Kontakt zwischen Datenbank und LSPs und stellt ein Programm zur Verfügung, welches die dezentrale Transportorganisation unterstützt. Die MASC-Anwendung besteht aus offenen Schnittstellen, so dass jede Firma auch ihre eigenen Softwarelösungen an den MASC-ID anschließen kann. Das bereitgestellte Programm ist also mehr für die kleinen Logistiker gedacht, die keine eigenen Softwarelösungen haben.
Der Spediteur registriert als erstes den MASC-Transport bei einer RSO seiner Wahl. Ihm wird ein MASC-Container vom nächstgelegenen Depot zugewiesen. Gleichzeitig bekommt er Zugriffsrechte auf die Datenbank für diesen Transport. Diese Rechte sind delegierbar. So kann er zum einen die Leserechte für die Sensorinformationen an Shipper und Versicherung weitergeben und zum anderen die dezentrale Transportorganisation verwalten. In der Datenbank kann der Spediteur im Folgenden Teilstrecken anlegen, deren Organisation er an Sub-Speditionen oder Frachtführer delegiert. Deren Aufgabe ist es nun, alle organisatorischen Informationen zum Transport einzupflegen. Auf diese Weise kann der organisierende Spediteur zu jeder Zeit die komplette Transportkette überwachen. Das System kann in der Folgezeit ständig aktualisierte Container-Manifeste erstellen, die alle notwendigen Informationen zum Transport bereitstellen. Es wäre ein Leichtes den Zollbehörden der am Transport beteiligten Länder Zugriff auf die Container-Manifeste zu

gewähren, um so die Container-Einfuhr zu optimieren.

Container-Monitoring Die Container werden mit Sensoren bestückt und eine steuernde Zentraleinheit in einer Deckensicke hinter der Containertür installiert. Die Container-Einheit vergleicht die aktuellen Sensordaten mit den zuletzt erhaltenen. Weichen die aktuellen Werte signifikant ab, wird ein Ereignis generiert, im lokalen Speicher gesichert und gleichermaßen über die drahtlose Verbindung übermittelt. Ist die Verbindung gestört, werden die Ereignisse aufgereiht und gesendet, sobald sie wieder verfügbar ist.



Für den Datentransport ist es notwendig, jede Container-Einheit mit einer Antenne im Türbereich auszustatten, die die Datenpakete über Radiowellen in die Catwalks zwischen die Container-Stapel sendet. Dazu muss, zumindest für Schiffe, Depots und Yards, ein wenige Euro teurer Access-Point (AP) in jedem Catwalk bereitgestellt werden. Bei LKWs und Zügen ist ein Empfänger pro Trailer erforderlich. Diese Empfänger sind mit einem Gateway verbunden, der eine Verbindung in das Internet herstellt. Bei Schiffen kann die existierende Satellitenverbindung verwendet werden, bei Yards und Depots ist es unproblematisch, eine Modem- oder DSL-Verbindung herzustellen. Bei LKWs oder Eisenbahnen kann das lokale Mobiltelefon-Netzwerk verwendet werden.

Terrorismusabwehr Seit den Terroranschlägen im September 2001, die mit Transportmitteln durchgeführt wurden, sind die USA hinsichtlich Einreise- und Einfuhrbestimmungen extrem sensibel. So hat U.S. Customs and Border Protection (US-CBP) eine Vielzahl von Regeln in Kraft gesetzt, die bei der USA-Einfuhr zu beachten sind. Im Rahmen der Container-Sicherheits-Initiative (CSI) [U.S06, CP05] wurde eine Regel eingeführt bei der das Manifest jedes Einfuhr-Containers 24 Stunden vor Beladung im Abfahrtshafen, gemeldet werden muss. Das von der US-CBP bereitgestellte automatisierte Manifest-System (AMS) empfängt die elektronischen Manifeste. Ein automatisches Bewertungssystem weist den Containern einen Risikowert zu. Überschreitet dieser eine bestimmte Schwelle, muss der Container noch vor dem Beladen inspiziert werden. Hierfür haben die großen Häfen eigens Container-Röntgengeräte eingeführt. Allerdings gewährleistet diese aufwändige und zeitintensive Prüfung an wenigen Zwischenpunkten des Transportes keineswegs eine hohe Sicherheit [U.S05]. Parallel zu der CSI hat die IMO (International Maritime Organisation) durch die SOLAS-Erweiterungen (Safety of Life at Sea) den physischen Zugang zum Schiff stark eingeschränkt, jedoch ist die sichere Überprüfbarkeit dieser neuen Regeln fraglich. [Int06]. Ein Umgehen der Röntgenüberprüfung ist also nicht ausschließbar.

Viel sinnvoller ist eine permanente Überwachung, die durch gezielte punktuelle Nach-

kontrolle ergänzt wird. Dies hat die US-CBP ebenfalls so gesehen, als sie im Rahmen der Einführung der CSI schrieb: „Use smarter, more secure containers, which will allow CBP officers at United States ports of arrival to identify containers that have been tampered with during transit“ [U.S06]. Den zurzeit statischen Risikowert, der vom AMS aus den Manifest-Daten gewonnen wird, könnte man mit einem geeigneten Containerüberwachungssystem dynamisch gestalten, indem man die Sensorwerte des Containers mit in die Berechnung einfließen lässt. Neben einem Türöffnungssensor ließen sich ein Radioaktivitätssensor und ein CO_2-Sensor in den Container implantieren, die neben der atomaren Strahlung möglicher schmutziger Bomben auch Lebewesen (im Besonderen Menschen) im Container entdecken könnten. Natürlich ist es für die Terrorismus-Prävention von Bedeutung, dass die Sensoren zuverlässige Werte abgeben und dass unbefugter Zugriff entdeckt wird.

3 Informationssicherheit

Ein Containerüberwachungssystem muss sicherstellen, dass nur Befugte Zugang zu den Daten erhalten. Information über den Zustand oder das Beinhalten spezieller Waren darf nicht in die Hände von Konkurrenten gelangen. Daher müssen die Informationen vom Sensor bis zum Rechner des Shippers durchgehend abgesichert werden.

MASC-Einheit Die im Container implantierte MASC-Einheit muss speziell abgesichert werden. Dazu muss das Gehäuse vor Fremdzugriff geschützt werden. Das Batteriefach sollte zwar extern zugänglich sein, aber eine Sicherheits-Batterie ist zwingend erforderlich, um bei Stromverlust noch eine Warnmeldung abzusenden. So kann ein „Denial-of-Service“-Angriff[1] nicht verhindert, aber zumindest erkannt werden. Sollten innerhalb eines gewissen Zeitintervalls keine neuen Batterien eingesetzt werden oder jemand versuchen, unberechtigten Zugriff auf die Einheit zu erlangen, tritt eine Art Selbstzerstörung in Kraft. Einerseits muss verhindert werden, dass Unbefugte an die gespeicherten Daten gelangen, andererseits sollen diese für Befugte jederzeit abrufbar sein. Mit einfachen kryptographischen Mitteln kann erreicht werden, dass keine vollständige Selbstzerstörung erfolgt. Jede MASC-Einheit hat einen geheimen Schlüssel, den nur die Einheit selbst und der Betreiber der korrespondierenden Datenbank (also die zugeordnete RSO) kennen. Die Ereignisse, die die MASC-Einheit bei sensorischen Auffälligkeiten generiert, werden verschlüsselt im lokalen Speicher gesichert. Ein Zugriff ist nur möglich, wenn der gemeinsame Schlüssel bekannt ist. Da sich dieser aber im Speicher der Einheit befindet, könnte ihn jeder Angreifer dort auslesen. Die Selbstzerstörung muss so wirken, dass genau dieser Schlüssel unwiederbringbar vernichtet wird.

Sicherer Datentunnel Das lokale sichere Speichern der Daten ist eine Sache, das Übertragen eine andere. Der MASC-SecureTunnel sorgt dafür, dass die Daten verschlüsselt über den Äther gehen. Damit die MASC-Einheit batteriebetrieben möglichst

[1] DoS-Angriff: ein Angriff gegen die Funktionsfähigkeit.

mehrere Jahre funktioniert, ist ein energieeffizientes Protokoll zu verwenden. Der meiste Strom wird gespart, wenn die Einheit schläft. Vor allem sollte die stromhungrige Sende-/ Empfangseinheit meistens abgeschaltet sein. Nur wenn ein Ereignis auftritt, begibt sich die Einheit in den Sende-Modus. Ist ein Access-Point (AP) in Reichweite, schickt die MASC-Einheit eine Zufallszahl an den AP. Wird diese zur RSO durchgeleitet, kann dort mit Hilfe des gemeinsamen Schlüssels eine Bestätigung zurückgesendet werden. Wird diese korrekt empfangen, weiß die MASC-Einheit, dass es sich um die richtige Gegenstelle handelt, da nur diese Nachrichten mit dem gemeinsamen Schlüssel versenden kann. Danach übermittelt die Einheit die Ereignisse verschlüsselt an die Gegenstelle. Die Daten werden extrahiert und in die Datenbank gestellt. Ein kurzes verschlüsseltes Bestätigungspaket quittiert den korrekten Empfang der Nachricht. Das nächste Ereignis kann nun verschickt werden, oder die Einheit kehrt in den Schlafmodus zurück.

MASC-Informationsdienst Die Problematik bei diesem Dienst liegt in der korrekten Autorisierung, da durch die komplexe Vertragsstruktur die Parteien bei Transportregistrierung noch nicht identifiziert sein müssen. Es ist daher eine delegierbare Rechtevergabe erforderlich, die von den Zugriffsystemen SPKI/SDSI [Ell99, EFL+99] und AMANDA [BDF02] ermöglicht wird. Beide erlauben die Weitergabe von Rechten, wobei bei AMANDA Restriktionen die genaue Weitergabe definieren. Die Struktur der Datenbank und die Rechte für die einzelnen Parteien wäre bei SPKI und AMANDA grundsätzlich identisch.

Bei **SPKI** erhält der Spediteur, der den Transport registriert, ein SPKI-Zertifikat mit Zugriffsrechten auf die Datenbank. Diese Rechte kann er selber nutzen und nach eigenem Ermessen weitergeben. Ebenso ist die Übertragung von Teilrechten an verschiedene Kunden möglich. Sub-Spediteure und Frachtführer müssen nicht als solche registriert sein, sondern werden vom Spediteur in das System initial „eingeladen“ und nehmen in Folge dessen daran teil.

Bei **AMANDA** müssen alle Teilnehmer bei einer RSO registriert und kategorisiert sein bevor sie ein Recht delegiert bekommen. Ausgehend von dieser Kategorisierung können Restriktionen bei der Rechtevergabe durchgeführt werden. Ähnlich wie bei SPKI bestimmt der Spediteur bei jeder Rechtvergabe das Zielobjekt. Es kann allerdings durch global festgelegte Regeln bestimmt werden, dass das Zugriffsrecht auf Sensordaten etwa nur von einem Spediteur an einen Shipper oder einen Versicherer gegeben werden darf. Das Recht, einen Teiltransport in der Datenbank anzulegen, hat nur der Spediteur. Sub-Spediteure können dann weitere Unter-Teiltransporte anlegen. Frachtführer dürfen nur Daten bezüglich ihrer zugewiesenen Teiltransporte einschreiben.

4 Schlussbemerkung

Die Anforderungen bei der Containerüberwachung unterscheiden sich von den üblichen Anforderungen an Sensor-Netzwerke[2] in einigen Punkten. Während die Forderung nach

[2] Sensor-Netzwerk nennt man ein Netzwerk aus Sensor-Knoten.

Energie-Effizienz und das Auslesen von Sensoren gleichermaßen auftreten, ist bei der Containerüberwachung keine Miniaturisierung notwendig. Viel spezieller sind aber die Vertragsstrukturen und die verschiedenen Parteien, die im Containertransportwesen auftreten. Im Besonderen die Existenz vertrauenswürdiger Dritter wurde in der MASC-Anwendung berücksichtigt. Die gesamte MASC-Architektur ist für diese Anforderungen maßgeschneidert.

Das MASC Projekt ist eine Initiative zweier Institute der TU Hamburg-Harburg. Das Institut für Sicherheit in verteilten Anwendungen entwickelt dabei die Sicherheitskonzepte für die MASC-Anwendung[3], während das Institut für Telematik die MASC-Einheit entwirft und mit Feldversuchen die Sensorik abstimmt.

Die MASC-Anwendung befindet sich zurzeit in ersten Feldversuchen. Als MASC-Einheiten werden an der FU Berlin entwickelte Sensor-Knoten eingesetzt [CSTG06]. Die besonderen Anforderungen an Energieeffizienz, Hardwaresicherheit und Robustheit erfordern es allerdings, serienreife Container-Einheiten im späteren Stadium mit speziell erstellter Hardware zu bestücken.

Literatur

[BDF02] Olav Bandmann, Mads Dam und Babak Sadighi Firozabadi. Constrained Delegations. In *Proceedings of the IEEE Symposium on Security and Privacy*, Seiten 131–140, 2002.

[CP05] U.S. Customs und Border Protection. Cargo security program aims to turn back a modern-day Trojan horse. Website — Customs Today, November 2005.

[CSTG06] FU Berlin Computer Systems & Telematics Gruppe. Homepage of ScatterWeb. Webpage, August 2006.

[EFL+99] Carl Ellison, Bill Frantz, Butler Lampson, Ron Rivest, Brian Thomas und Tatu Ylonen. RFC 2693—SPKI Certificate Theory. Bericht, Network Working Group, September 1999.

[Ell99] Carl Ellison. RFC 2692—SPKI Requirements. Bericht, Network Working Group, September 1999.

[Int06] International Maritime Organisation. FAQ on ISPS code and maritime security. Webpage, Januar 2006.

[Kap04] Kapitän AG Thomas Ziehn. Kriminalität im Containertransport. Schadenverhütungstagung des Fachausschusses Transport im GDV vom 14. bis 16. Juni 2004, Juni 2004.

[U.S05] U.S. Departement of Homeland Security—U.S. Coast Guard. Best Practice: 100% X-Ray Container Screening. USCG Port Security Assessment—Best Practices Bulletin, Januar 2005. PFSO: Capt. Ben Hassan.

[U.S06] U.S. Customs and Border Protection. CSI In Brief. Webpage, Januar 2006.

[3] `http://www.sva.tu-harburg.de/projects/MASC`