Universität Karlsruhe (TH)
Institut für Telematik

TELEMATICS TECHNICAL REPORTS

Das ZeuS-Anreifermodell

Erik-Oliver Blass, Zinaida Benenson
benenson@tm.uka.de, zina@uni-mannheim.de

February, 5th 2008

TM-2008-1

ISSN 1613-849X

http://doc.tm.uka.de/tr/

Institute of Telematics, University of Karlsruhe
Zirkel 2, D-76128 Karlsruhe, Germany

Das ZeuS-Angreifermodell

Erik-Oliver Blaß und Zinaida Benenson

24. Juli 2007

Zusammenfassung

Dieses Dokument beschreibt das in ZeuS zugrundeliegende *Angreifermodell* – das sind die Fähigkeiten oder Möglichkeiten eines Angreifers, Einfluß auf das Sensornetz zu nehmen. Die Parameter des Angreifermodells werden dabei graduell abstufbar spezifiziert. Ein Standard-Angreifer wird definiert, gegen den die in ZeuS entwickelten Protokolle sicher arbeiten müssen. Die möglichen Auswirkungen eines stärkeren oder schwächeren Angreifers in Bezug auf beispielsweise Energieverbrauch oder Sicherheit sollten für die einzelnen Protokolle in ZeuS diskutiert werden.

1 Einleitung

Entwicklung und Verifikation der Kommunikationsprotokolle erfordern, daß ein formales Angreifermodell aufgestellt wird. Da die ZeuS-Protokolle nicht nur in Abhängigkeit vom Energieverbrauch, sondern auch in Abhängigkeit von der Mächtigkeit des Angreifers graduell abstufbar sein sollen, werden im Weiteren die Angreiferannahmen graduell abstufbar spezifiziert.

Insbesondere werden die Möglichkeiten zur Beeinflussung des Sensornetzes und der Protokollabläufe durch einen *Standard-Angreifer* festgelegt: Die im ZeuS entworfenen Protokolle müssen mindestens gegen diesen Standard-Angreifer sicher arbeiten. In wie weit sich Auswirkungen in Bezug auf beispielsweise Sicherheit und Energieverbrauch von Protokollen bei abweichenden (schwächeren oder stärkeren) Angreifern ergeben, soll im Rahmen der Protokollbeschreibungen immer mit untersucht werden.

Im Gegensatz zu vielen anderen Arbeiten, geht ZeuS von einem besonderen Angreifermodell aus: Ein Angreifer im Sensornetz hört nicht nur Kommunikation ab, sondern bringt auch eine gewisse Anzahl von Knoten unter seine Kontrolle. Solche korrumpierten Knoten verhalten sich nach außen zunächst protokollkonform, verfolgen aber in Wirklichkeit böswillige Absichten.

2 Ziele des Angreifers

Alle klassischen Angreiferziele werden in ZeuS als relevant angesehen. Dabei handelt es sich um die folgenden:

2.1 Vertraulichkeit

Anfallende Daten sollen im Sensornetz vertraulich, geschützt vor unbefugtem Zugriff durch den Angreifer und seine korrumpierten Knoten, verarbeitet werden. Korrumpierte Knoten sollen nicht an Daten gelangen, an die sie nicht durch einen *ordnungsgemäßen* Protokollablauf gelangen würden.

2.2 Integrität und Authentizität

In Zeus wird insbesondere auf die Authentizität der Informationen im Sensornetz geachtet. Im TP3 wird die Authentizität der aggregierten Daten auf ihrem Weg zur Senke gewährleistet, im TP4 werden Anfragen (Queries) authentisch im Netz verteilt. Außerdem soll die Authentizität der Netzmanagementinformationen gewährleistet werden.

2.3 Verfügbarkeit

Angriffe auf Verfügbarkeit, wie zum Beispiel *jamming* oder *battery-draining*, stellen in drahtlosen Sensornetzen eine besondere Herausforderung dar und sind aktueller Forschungsgegenstand im Teilprojekt 4. In ZeuS sollen die Protokolle in der Lage sein, bestimmte Angriffe auf Verfügbarkeit zu erkennen, beispielsweise durch einen rapiden Energieabfall. Für die Dauer des Angriffs sollen dann Dienstqualitäten auf Sensorknoten abgeschwächt werden. Dadurch wird zwar die Verfügbarkeit während des Angriffs nicht verbessert, es wird jedoch an Energie gespart, so daß nach der Beendigung des Angriffs wieder eine höhere Dienstqualität gewährleistet werden kann, und das Netz länger verfügbar bleibt.

3 Charakterisierung des Standard-Angreifers

Angreifer werden nach mehreren orthogonalen Kriterien unterschieden – wie im folgenden beschrieben. Sie basieren aus den Arbeiten Cramer und Damgård [3] sowie Benenson et al. [1], Blaß [2].

3.1 Korrumpieren von Knoten

Der Angreifer kann eine gewisse Anzahl $\mathcal{B}$ von Sensorknoten unter seine Kontrolle bringen.

Es werden folgende, aufeinander aufbauende Stufen der Kontrolle unterschieden:
Ein *beschränkt passiver* Angreifer hat Zugriff zu allen Informationen, über die der Sensorknoten verfügt. Allerdings muss der Angreifer, um an die Informationen zu kommen, den Knoten für immer aus dem Sensornetz entfernen.

Ein *passiver* Angreifer kennt alle internen Informationen des korrumpierten Knotens. Der korrumpierte Knoten verbleibt jedoch im Netz, so daß eine kontinuierliche Beobachtung des Informationsflusses in diesem Knoten möglich ist. Außerdem kann der Angreifer die Daten, die auf dem Knoten gespeichert sind, ändern.

Ein *aktiver* Angreifer kennt nicht nur alle internen Informationen des Knotens, sondern kann die korrumpierte Knoten re-programmieren. Dadurch können sich die korrumpierten Knoten teilweise wie *legitime*, das heißt nicht-korrumpierte Knoten, protokollkonform verhalten, können aber auch zwischendurch etwas Bösartiges machen, so zum Beispiel ein Aggregat falsch berechnen oder eine beliebige Nachricht verschicken. Daher wird an dieser Stelle auch angenommen, daß es den legitimen Knoten nicht ohne weiteres möglich sei zu erkennen, ob ein bestimmter Knoten korrumpiert worden ist oder nicht.

Standard-Angreifer: In ZeuS wird standardmäßig ein *aktiver* Angreifer angenommen. Die Basisstation kann nicht korrumpiert werden. Falls es dem Angreifer gelingen sollte, die Senke zu korrumpieren, könnte er sämtliche die Senke erreichenden Aggregate dem Benutzer gegenüber fälschen. Alle Informationen, die der Benutzer aus dem Sensornetz über die Senke bezieht, wären falsch.

Optionen: Auch der beschränkt passive und der passive Angreifer sind denkbar. Protokolle, die gegen einen solchen Angreifer schützen, sind voraussichtlich effizienter und sollen nach Möglichkeit untersucht werden.

3.2 Anzahl korrumpierter Knoten $\mathcal{B}$

Zunächst ist klar, daß $\mathcal{B} < n$ gelten muß, also nicht alle Sensorknoten im Netz korrumpiert sein dürfen. In einer Situation mit $\mathcal{B} = n$ kann es keine sinnvolle Sicherheit geben.

Die tatsächliche Anzahl korrumpierter Knoten $\mathcal{B}$ ist durch die Fähigkeiten des Angreifers, Knoten zu korrumpieren, beschränkt. Der Angreifer braucht Zeit und Ausrüstung, um Knoten zu korrumpieren, er benötigt Zeit, um einen Buffer-Overflow zu entwickeln usw. Über derartige Ressourcen verfügt der Angreifer allerdings nur beschränkt und kann dementsprechend nicht beliebig viele Knoten korrumpieren.

3.3 Gemeinsames Knotenwissen

Die korrumpierten Knoten arbeiten zusammen, um das Ziel des Angreifers zu erreichen. Dabei können die korrumpierten Knoten untereinander Daten austauschen. Die dafür notwendige Kommunikation zwischen den korrumpierten Knoten muß nicht zwangsläufig über protokollkonforme Nachrichten und die „normale“ Funkschnittstelle der Sensoren erfolgen, sondern *irgendwie* – beispielsweise über Out-of-Band-Mechanismen. Die Kommunikation der korrumpierten Knoten untereinander ist instantan: Sie benötigt keine Zeit. Sinn und Zweck dieser beiden Annahmen ist nur, daß der Angreifer und alle seine Knoten über einen gemeinsamen Wissensstand verfügen. Kennt ein korrumpierter Knoten ein bestimmtes Geheimnis, etwa einen Schlüssel, dann kennen ihn gleichzeitig auch alle anderen korrumpierten Knoten im Netz.

3.4 Präsenz des Angreifers

Ein Angreifer kann lokal, partiell oder global im Netz präsent sein.

Ein *lokaler* Angreifer korrumpiert eine gewisse Anzahl Knoten in einem kleinen, beschränkten, zusammenhängenden Teil des Netzes.

Ein *partieller* Angreifer hat Kontrolle über mehrere kleine zusammenhängende Teile des Netzes. Ein Beispiel ist ein Angreifer, der eine gewisse Anzahl Knoten *gleichverteilt* im gesamten Netz korrumpiert.

Ein *globaler* Angreifer kann das ganze Netz beeinflussen, zum Beispiel überall die Nachrichten abhören.

Der **Standard-Angreifer** ist eine Kombination aus einem partiellen und einem globalen Angreifer:

- Im Hinblick auf die *Korrumpierung* der Knoten ist der Angreifer partiell. Er kann Knoten an beliebigen Stellen im Netz korrumpieren – siehe Abschnitt 3.4.1.
- Im Hinblick auf das *Beobachten* des Netzes ist der Angreifer global: Er kann sämtliche Nachrichten, die zwischen Sensoren ausgetauscht werden, abhören. Er kann allerdings nur dann Chiffrate entschlüsseln, wenn einer seiner korrumpierten Knoten den dafür notwendigen Schlüssel kennt.

  Genauso kann der Angreifer beliebig im Netz neue Nachrichten injizieren, allerdings erzeugt er nur Chiffrate mit Hilfe von Schlüsseln, die seine korrumpierten Knoten kennen.

Optionen: Auch ein Angreifer, der das Netz nur zum Teil abhören und/oder die Knoten nur lokal korrumpieren kann, ist für die ZeuS-Protokolle von Interesse und soll diskutiert werden.

3.4.1 Verteilung der korrumpierten Knoten

Der **Standard-Angreifer** bewegt sich völlig *zufällig* und *wahllos* durch das Sensornetz und korrumpiert dabei ebenso zufällig Knoten. Da alle Knoten gleich leicht vom Angreifer zu erreichen sind und kein Knoten über besondere Schutzmaßnahmen verfügt, korrumpiert der Angreifer Knoten *gleichverteilt*. Er macht dies solange, bis seine Ressourcen erschöpft sind. Wenn der Angreifer fertig mit dem Korrumpieren ist, hat er insgesamt $\mathcal{B}$ Knoten korrumpiert.

Es bezeichnet $\beta = \frac{\mathcal{B}}{n}$ den Anteil oder Prozentsatz der korrumpierter Sensorknoten im gesamten Netz. Wenn sich der Angreifer aus den oben beschriebenen Gründen wahllos durch das Netz bewegt und damit zufällig und gleichverteilt Knoten korrumpiert, dann ist jeder Knoten im Netz mit $\beta\%$ Wahrscheinlichkeit korrumpiert.

Optionen: Im Prinzip kann die Verteilung der korrumpierten Knoten im Netz beliebig variieren. Es kann eine regelmässige Struktur sein, wie zum Beispiel eine Kette, ein Gitter oder völlig wahllos erfolgen. Diese und andere zusätzliche Möglichkeiten zur Verteilung von korrumpierten Knoten sollen in ZeuS-Protokollen untersucht werden.

3.5 Kryptographisches vs. Informationstheoretisches Modell

Weiterhin kann der **Standard-Angreifer** keine Nachrichten, zu denen er nicht den Schlüssel kennt, modifizieren. Modifiziert soll an dieser Stelle bedeuten, daß er nicht in der Lage ist, durch Modifikation des Chiffrats bewußt den sich dahinter verbergenden Klartext zu

verändern. Grundsätzlich kann der Angreifer in jedem Fall eine Nachricht verändern, beispielsweise durch gezieltes Stören eines Teils der Nachrichtenübertragung einzelne Bits der Nachricht und damit einzelne Bits eines Chiffrats manipulieren.

Diese Eigenschaft soll in ZeuS nicht variiert werden.

3.6 Adaptiv vs. Statisch

Der **Standard-Angreifer** verhält sich bzgl. der Korrumpierung von Knoten nicht adaptiv, sondern *statisch*: Er korrumpiert eine bestimmte Anzahl $\mathcal{B}$ von Knoten im Netz auf einmal und *vor* dem Beginn der normalen Arbeit im Sensornetz (Daten messen, verschicken, aggregieren, etc.). Irgendwann ist der Angreifer fertig mit dem Korrumpieren. Danach kann er oder will er keine Knoten mehr korrumpieren.

Das bedeutet, der Angreifer ist insbesondere nicht in der Lage, während der Ausführung eines Protokolls *adaptiv* neue Knoten zu korrumpieren. Diese Annahme wird üblicherweise auch deshalb getroffen, damit der Angreifer aus Erkenntnissen über den bisherigen Protokollverlauf, zum Beispiel den bisherigen Nachrichtenfluß zwischen verschiedenen Knoten, etwas über die Wichtigkeit bestimmter Knoten im Netz lernt und daraufhin gezielt die „wichtigen“ Knoten korrumpiert. Ein Angreifer, der beispielsweise mittels Analyse von Datenflüssen im Netz die Aufgaben verschiedener Knoten im Netz analysieren und daraufhin gezielt wichtige Knoten korrumpieren könnte, wäre äußerst unfair: Er würde genau die Knoten korrumpieren, die für das Erreichen seiner Ziele notwendig wären.

Optionen: Schutz gegen einen adaptiven Angreifer ist sehr aufwendig, soll aber nach Möglichkeit in Protokollen mituntersucht werden.

3.7 Synchrone vs. Asynchrone Kommunikationsmöglichkeit

Die Kommunikation im Sensornetz findet (auf Applikationsebene) *synchron* statt. Synchron bedeutet hier, daß der **Standard-Angreifer** nicht in der Lage ist, Nachrichten zwischen zwei Knoten unendlich lange zu „blockieren“. Der Einfachheit halber soll angenommen werden, daß Knoten, die auf den Empfang einer Nachricht warten, irgendwann über einen Timer darüber informiert werden, daß die Nachricht nicht angekommen ist. Umgekehrt merken Knoten, die eine Nachricht versendet haben über einen ablaufenden Timer, daß eine erwartete Quittierung der Nachricht ausbleibt. Die Nachricht kann dann neu geschickt oder ein „Alarm“ ausgelöst werden. Eine Nachricht, die Knoten a an Knoten b schickt, kommt – wenn auch zeitverzögert – immer bei b an.

Der Angreifer kann allerdings das Senden und Empfangen einer Nachricht voneinander entkoppeln und Nachrichten „abfangen“: Mit Hilfe geeigneter Funktechnik ist er in der Lage, die von a versendete Nachricht zu empfangen, gleichzeitig aber mittels eines Störsenders (sogenanntes *Jamming*) b am Empfang zu hindern. Bevor er nun die abgefangene Nachricht von a an b ausliefert, kann er noch schnell eine eigene Nachricht an b oder einen anderen Knoten verschicken. Ein Angreifer mit solchen Möglichkeiten heißt *rushing*.

3.8 Sicherer vs. Unsicherer Broadcast

Eine ganz ähnliche Annahme betrifft die Broadcast-Eigenschaft der Funkkommunikation. Wenn die Knoten a, b und c sich alle in gegenseitiger Funkreichweite befinden, dann erlaubt normalerweise das drahtlose Medium, daß eine Nachricht, die a an b verschickt, auch gleichzeitig von c mitgehört werden kann. Für den ZeuS-Standard-Angreifer soll allerdings angenommen werden, daß er, wiederum durch den Einsatz besonderer Funktechnologie, in der Lage ist, die Nachricht von a so zu stören oder abzuschirmen, daß b die Nachricht empfängt, Knoten c allerdings nicht. Weiterhin soll es dem Angreifer möglich sein, eine Nachricht eines seiner korrumpierten Knoten a' so an einen legitimen Knoten b zu verschicken, daß ein anderer legitimer Knoten c davon nichts mitbekommt – obwohl sich auch c in Funkreichweite von a' befindet. Folglich ist es für einen korrumpierten Knoten möglich, Protokollnachrichten mit der selben Sequenznummer, aber mit unterschiedlichem Inhalt, an die Knoten b und c zu schicken.

Optionen: Inwieweit sich ein schwächerer Angreifer, der keine Nachrichten selektiv vertauschen und einspielen kann, auf die Sicherheit und den Energieverbrauch auswirkt, soll in ZeuS untersucht werden.

3.9 Annahmen über die Messwerte

Ein Sensor, der ein aus Protokollsicht transzendentes, externes Phänomen oder Ereignis mißt, *kann* diesbzgl. alleine mit Mechanismen aus dem Protokoll heraus nicht überprüft werden.

Alle *Blätter* im Aggregationsbaum, das sind die Sensoren, die Meßwerte von „außerhalb“ des Protokolls messen, dürfen in dieser Arbeit vom Angreifer entweder gar nicht oder nur *eingeschränkt* korrumpiert werden, das heißt: Im Kontext sicherer Aggregation dürfen sie in Bezug auf ihre gemessenen Werte nicht *lügen*. Mißt ein Blatt x einen Wert X, dann muß x auch genau diesen Wert X an seinen Aggregationsknoten schicken. Es soll damit dem **Standard-Angreifer** nicht möglich sein, „protokollexterne“ Daten zu fälschen.

Optionen: Hier besteht eine Möglichkeit zur Variation, zur Verstärkung des Standard-Angreifers. Unter der Annahme, daß die Sensorknoten über gemessenen Werte lügen können, können entsprechende Protokolle zur überprüfung der gemessenen Werte entwickelt werden, beispielsweise unter der Annahme *redundanter* Messungen.

4 Zusammenfassung

In diesem Dokument wird das Standard-Angreifermodell für die ZeuS-Protokolle beschrieben. Außerdem werden mögliche Optionen zum Standard-Angreifer genannt, die in Protokollen nach Möglichkeit untersucht werden sollen. Folgende Annahmen über einen Angreifer sollen in ZeuS eine Rolle spielen:

- Korrumpieren von Knoten: Kontrolle über die korrumpierten Knoten (beschränkt passiv, passiv, aktiv), gemeinsames Knotenwissen, Präsenz des Angreifers (lokal, partiell, global), statischer vs. adaptiver Angreifer, und Verteilung der korrumpierten Knoten (uniform vs. andere Optionen);

- Ressourcen des Angreifers: begrenzte Anzahl korrumpierter Knoten und polynomiell beschränkte Berechnungskapazität;
- Kommunikation im Netz: synchrone Kommunikation und unsicherer lokaler Broadcast;
- Annahmen über die Messwerte.

Literatur

[1] BENENSON, Zinaida, CHOLEWINSKI, Peter M. und FREILING, Felix: *Vulnerabilities and Attacks in Wireless Sensor Networks*. In: *Wireless Sensors Networks Security*. IOS Press, to appear (Cryptology & Information Security Series)

[2] BLASS, Erik-Oliver: *Sicherer, aggregierender Datentransport in drahtlosen Sensornetzen*. Dissertation, Universitätsverlag Karlsruhe, 2007. ISBN 978-3-86644-142-2

[3] CRAMER, R. und DAMGÅRD, I.: *Introduction to Secure Multi-Party Computations*. In: *Contemporary Cryptology: Advanced Courses in Mathematics*. Birkhauser, 2005, Seiten 41–87. ISBN 3-7643-7294-X