Modellbasierte Sicherheitsanalyse mit UMLsec: Ein biometrisches Zugangskontrollsystem

Robert Schmidt, LMU München
robert.schmidt@informatik.uni-muenchen.de
Jan Jürjens, TU München
juerjens@in.tum.de

Abstract: Im Rahmen des Verisoft-Projekts [ver03] entsteht in Zusammenarbeit mit T-Systems [SL04] ein biometrisches Zugangskontrollsystem, dessen Sicherheitseigenschaften von zentraler Bedeutung sind. In dieser Fallstudie wird UMLsec, eine Erweiterung von UML, verwendet, um das zu entwickelnde System zu modellieren und auf Modellebene die sicherheitskritischen Aspekte zu untersuchen.

UMLsec

Die Unified Modelling Language (UML,[RJB99]) stellt einen de-facto Industriestandard zur Modellierung von Softwaresystemen dar. In ihrer Erweiterung UMLsec([Jü04]), wird die UML mit Hilfe von *stereotypes*, *constraints* und *tagged values* so erweitert, dass die sicherheitsrelevanten Aspekte eines Systems modelliert werden können. Die Stärke von UMLsec liegt allerdings in der zugrundeliegenden Semantik, so dass Sicherheitsanforderungen auf Modellebene durch Toolunterstützung validiert werden können.

Biometrie

Biometrische Verfahren basieren darauf, dass bei verschiedenen Menschen dieselben Körperteile unterschiedliche biometrische Eigenschaften besitzen. Ein biometrisches System, das solche Verfahren einsetzt, überprüft in einem *Authentifizierungsvorgang*, ob die von einem Biometrie-Scanner eingescannten biometrischen Daten (*biometrisches Template*) einer Person, zu den Daten im Speicher (*Referenztemplate*) passen. Dann entscheidet es, ob diese Person Zugang erhalten soll oder nicht. Als Speicher wird hier, auch aus Gründen des Datenschutzes, eine Smartcard eingesetzt. Für den Vergleich und die Zugangsentscheidung ist ein Hostsystem zuständig.

Sicherheitsaspekte

Die Entwendung der Smartcard und der Versuch, an die dort befindlichen Daten zu kommen, gilt als Angriff gegen ein Biometriesystem. Eine Smartcard gilt im Allgemeinen als *tamper-proof*, so kann sich der Angriff gegen die Übertragungsverbindung zwischen Kartenterminal und Hostsystem richten, indem die übertragene Daten mitgelesen werden. Die auf diese Art gewonnene Daten kann ein Angreifer für die Erstellung einer eigenen Smartcard missbrauchen, um damit unberechtigten Zugang zu erhalten.

Für umfassende Informationen über Bedrohungen biometrischer Systeme und deren sichere Entwicklung im Rahmen der *Common Criteria* siehe beispielsweise [gvc01].

Folgende Maßnahmen werden zum Schutz des Biometriesystems ergriffen. Die Smartcard muss sich beim Hostsystem unter Verwendung kryptographischer Algorithmen authentifizieren. Das qualitativ hochwertige Referenztemplate wird verschlüsselt übertragen. Signaturverfahren werden eingesetzt, um eine Personenidentität, das Referenztemplate und die Karten-ID zu verknüpfen. Fehlbedienungszähler verhindern *brute-force*-Angriffe.

Sicherheitsanalyse

Das System wird mit UML modelliert: es kommen Verteilungs-, Aktivitäts-, Klassen- und Sequenzdiagramme zum Einsatz, so dass der grundlegende physikalische Aufbau, der Authentifizierungsvorgang, die sicherheitskritischen Elemente und die kryptographischen Protokolle als UML-Diagramme mit in UMLsec ausgedrückten sicherheitsrelevanten Aspekten vorliegen. Es werden Angriffszenarios für unterschiedliche Angreifertypen anhand der in den Modellen verwendeten UMLsec-*stereotypes* für die Komponenten des Systems untersucht. Die Protokolle zur Datenübertragung werden aus den Sequenzdiagrammen durch Abstraktion in Formeln der Logik erster Stufe (Horn-Klauseln) übersetzt. Diese abstrakte Darstellung modelliert dann den Informationszugewinn, den ein Angreifer während der Ausführung des Protokolles durch Abhören, Entfernen und Einfügen von Nachrichten auf ungeschützten Informationsverbindungen, sowie geeigneten Rekombination von Nachrichtenteilen, maximal erhalten kann. Mithilfe von automatischen Theorembeweisern für Logik erster Stufe (wie Setheo oder Spass) oder von Logikprogrammiersprachen (wie Prolog) kann nun automatisch geprüft werden, ob eine bestimmte Information einem möglichen Angreifer bekannt werden kann. Werkzeugunterstützung für die Übersetzung von Sequenzdiagrammen in Horn-Klauseln und die automatische Auswertung sind in Arbeit [JSA+03]. Für eine effektivere Betrachtung der Operationen auf den Fehlbedienungszählern ist auch ein Constraint-Logischer Ansatz möglich.
Weitere Informationen können auf Anfrage dem Bericht [RJ04] entnommen werden.
Besonderer Dank für die Unterstützung gilt an dieser Stelle Matthias Schwan (T-Systems).

Literatur

[gvc01] *Biometric Technology Security Evaluation Unter the Common Criteria*. Government of Canada, Commutications Security Establishment. Version 1.2. September 2001.

[JSA+03] Jürjens, J., Shabalin, P., Alter, E., Meng, S., Schwaiger, M., Kokavecz, G., Schwarzmüller, S., und Shen, S. UMLsec tool. 2003. Webinterface at http://www4.in.tum.de/~umlsec.

[Jü04] Jürjens, J.: *Secure Systems Development with UML*. Springer. 2004.

[RJ04] R.Schmidt und J.Jürjens: Modellierung eines biometrischen Zugangssystems mit UMLsec. Technical report. Interner Bericht Verisoft-Projekt. Februar 2004.

[RJB99] Rumbough, J., Jacobson, I., und Booch, G.: *The Unified Modelling Language Reference Manual*. Addison-Wesley. 1999.

[SL04] Schwan, M. und Lassmann, G. Securing biometric systems using smartcards. 2004.

[ver03] *Verisoft*. Bundesminist. f. Bildung und Forschung. URL: http://www.verisoft.de. 2003.