

Name und eventuell Akronym der Idee

Peter Mustermann

Horst Görtz Institut, Ruhr-Universität Bochum, 12345 Bochum

E-Mail: peter.mustermann@hgi.rub.de

Petra Musterfrau

Horst Görtz Institut, Ruhr-Universität Bochum, 12345 Bochum

E-Mail: petra.musterfrau@hgi.rub.de

10. Dezember 2009

Zusammenfassung

Das Abstract (Seite 1) darf maximal 400 Zeichen (inklusive Leerzeichen) haben. Es folgt ein Fülltext. Das Horst Görtz Institut (HGI) entwickelt IT-Sicherheitswerkzeuge, speziell als Antwort auf jüngste Seitenkanalattacken. Eine Auswahl dieser Werkzeuge soll in einem Baukasten zu einer performanten und leicht zu konfigurierenden Sicherheitsplattform zusammengeführt werden.

Schutzbedarf

Nichtzutreffendes bitte streichen. Wenn Sie nichts streichen, gehen wir von (1) aus.

(1) Die vorgestellte Idee soll analog dem Vorgehen für wissenschaftliche Konferenzen begutachtet werden.

/

(2) Die Idee hat einen erhöhten Schutzbedarf und soll entsprechend begutachtet werden.

Falls Interessenkonflikte mit einem der Jurymitglieder bestehen, so teilen Sie uns diese bitte mit.

1 Stand der Forschung/Technik

Der Stand der Forschung (Seite 2) muss auf einer Seite mit maximal 3000 Zeichen und Schriftgröße mindestens 11pt beschrieben werden. Leerzeichen werden hierbei mitgezählt. Tabellen und Grafiken können eingebunden werden, sie dürfen aber nicht über die hier eingestellten Seitenränder ragen (oben, unten, rechts und links).

Es folgt ein Fülltext.

Das Horst Görtz Institut entwickelt IT-Sicherheitswerkzeuge, speziell als Antwort auf jüngste Seitenkanalattacken. Eine Auswahl dieser Werkzeuge soll in einem Baukasten zu einer performanten und leicht zu konfigurierenden Sicherheitsplattform zusammengeführt werden.

Die Hauptanwendung der Sicherheitsplattform „Anti-KeeLoq“ ist die sichere ubiquitäre Nutzung elektronischer Geräte. Exemplifiziert wird dies im Szenario mobiler Flugzeugmechaniker, der ein Flugzeug während eines Zwischenstopps wartet. Das Designziel der Plattform ist die leichte Integration aktueller Technologien wie „Keyless Drive and Go“ und die Integration biometrischer Merkmale, sowie umgekehrt die transparente Integration der Plattform in bestehende Sicherheitsinfrastrukturen. Die Anti-KeeLoq-Werkzeuge sind auf den folgenden Schichten angesiedelt: Policies, Protokoll-Engineering, kryptographische Basistechnologie sowie im speziellen, Bochumer Bergbaustaub zur elektromagnetischen Abschirmung. Die Plattform selber ist ein förderiertes Ressourcen- und Informationssystem, welche die Besonderheiten der Geräte wie eingeschränkte Rechenleistung, begrenzte Bandbreite und Datenübertragung oder ein kleines Display berücksichtigen. Die Entwicklungen auf der Anwendungsebene setzen die innovative Konzepte - sicheres mobiles, minimales Endgerät - und hochflexible Out-of-the-box-PKI - (schnelle, dezentrale Personalisierung von Chipkarten) um und berücksichtigen dabei die nötige Robustheit gegen Seitenkanalattacken. Sie zeigen weiter die Mächtigkeit und Möglichkeiten der Plattform. Die rechtliche Betrachtung der Plattform mit ihren Einsatzgebieten und der einzelnen Werkzeuge begleitet das HGI als Querschnittsthema.

2 Idee

Die Idee (Seiten 3 und 4) muss auf zwei Seiten mit maximal 6000 Zeichen mit Schriftgröße mindestens 11pt beschrieben werden. Leerzeichen werden hierbei mitgezählt. Tabellen und Grafiken können eingebunden werden, sie dürfen aber nicht über die hier eingestellten Seitenränder ragen (oben, unten, rechts und links).

Es folgt ein Fülltext.

Anti-KeeLoq-Werkzeuge garantieren eine Fülle von informationstechnisch sicheren Anwendungen. Auf der CeBIT wird die Tauglichkeit und Flexibilität am Beispiel des Pilotszenarios des „Mobilen Wartungsingenieurs auf dem Rollfeld“ unter Beweis stellen. Und so geht es: Die Mitarbeiter einer Flugzeugwartungsfirma holen sich vom Verwaltungssystem Arbeits- bzw. Wartungsaufträge ab, erfüllen diese durch die Inspektion bzw. Aufnahme von Messwerten entsprechender Flugzeugkomponenten und bestätigen diese Aufträge anschließend durch das Einsenden von signierten Checklisten mittels ihres PDAs oder des entwickelten sicheren Audio-Assistenten „Talking Assistant“. Der Talking Assistant kann hierbei als mobiles Endgerät genutzt werden, wobei dem Mitarbeiter die Checklisten Schritt für Schritt vorgelesen werden bzw. der Wartungsingenieur durch Sprachkommandos die Checkliste „ausfüllen“ kann. Die abgearbeiteten Checklisten werden bereits auf dem mobilen Endgerät mit Datum und Uhrzeit versehen, digital von einem Dienst der Plattform signiert und dann im XML-Format verschlüsselt an das Backend-System geschickt. Die XML-Dokumente werden dort mittels eines Checkers semantisch auf Integrität geprüft, so dass Unstimmigkeiten im Dokument (z.B. falsch abgelesene Flugmeilen, Widersprüche zwischen beobachteten Systemzuständen und dem Wartungsdatensatz) auffallen, noch während der Mechaniker vor Ort ist.

Der letzte Test vor dem Okay zur Flugbereitschaft ist der „security and anti sabotage check“. Werden fremde Gegenstände auf dem Rollfeld gefunden oder war das Cockpit nicht ordnungsgemäß verschlossen, dann trägt dies der Wartungsmitarbeiter elektronisch ein. So werden sofort Spezial-Sicherheitsteams alarmiert.

Im Rahmen der CeBIT wird ein erster Prototyp der Anti-KeeLoq-Plattform gezeigt, der das Zusammenspiel der sicherheitsrelevanten Dienste in einer sicheren Infrastruktur demonstriert und dabei die Gefahr von Seitenkanalattacken hervorhebt. Die Plattform als gemeinsame Hard- und Software für alle interagierenden Endgeräte integriert nahtlos lokale sowie verteilte Dienste, setzt implizit rollenbasierte Sicherheitspolitiken durch und zeichnet sich besonders durch folgende Merkmale aus:

- Modularität und Erweiterbarkeit
- Einfache Integration von Komponenten
- Flexible, dezentrale Schnittstellen
- durchgehende Sicherheit
- Ubiquitäre Anbindung von mobilen Nutzern
- Benutzerfreundlichkeit durch einfache Handhabung

Auf der CeBit geben die Wissenschaftler der Ruhr-Universität Bochum auch einen Einblick in aktuelle Entwicklungen des Werkzeugkastens „Face Recognition“, „DL-BruteForcer“, „XML Content Security“, „Triple S - Super Safe Security“ und „Cyberlaw“).

Hintergrund: An Anti-KeeLoq arbeiten weltweit führende Wissenschaftler mit Firmen, die auf IT-Sicherheit spezialisiert sind. Das Projekt begann im Februar 2001 und wird vom Bundesministerium für Bildung und Forschung drei Jahre lang mit insgesamt 6,1 Mio. Euro gefördert. An Anti-KeeLoq sind neben einer Reihe von Arbeitsgruppen der Ruhr-Universität Bochum auch das Horst Görtz Institut für IT-Sicherheit, die Fraunhofer-Institute sowie die Unternehmen cv cryptovision GmbH (Gelsenkirchen), escript GmbH (Bochum), MediaSec Technologies GmbH (Essen), Philips Semiconductors GmbH (Hamburg), T-Systems GmbH (Darmstadt) beteiligt.

Die Projektkoordination von Anti-KeeLoq liegt beim Horst Görtz Institut für IT-Sicherheit, einer zentralen Einrichtung der Ruhr-Universität Bochum, die seit 2000 die zahlreichen Aktivitäten zu einem internationalen wissenschaftlichen Exzellenzzentrum für IT-Sicherheit bündelt. Aktuell sind dem Horst Görtz Institut für IT-Sicherheit 10 Professoren aus den Fachbereichen Mathematik, Informatik, Elektrotechnik, Physik und Rechts- und Wirtschaftswissenschaften zugeordnet.

3 Nutzen

Der Nutzen (Seite 5) muss auf einer Seite mit maximal 3000 Zeichen mit Schriftgröße mindestens 11pt beschrieben werden. Leerzeichen werden hierbei mitgezählt. Tabellen und Grafiken können eingebunden werden, sie dürfen aber nicht über die hier eingestellten Seitenränder ragen (oben, unten, rechts und links).

Es folgt ein Fülltext.

Der Talking Assistant (Minimales, sicheres Endgerät, realisiert als Headset mit Positionierungstechnologie) ist mit dem PDA des Wartungstechnikers in dessen Jackentasche verbunden. Im PDA steckt die Chipkarte des Mechanikers. Die Chipkarte und seine PIN (bzw. alternativ die Stimmerkennung über den Talking Assistant) erlauben dem Techniker seine digitale Identität frei zu schalten (Zwei-Faktor-Authentisierung: Besitz & Wissen oder Besitz & Biometrie).

Kommt die Chipkarte abhanden, dann wird diese sofort gesperrt und eine neue wird vor Ort extrem schnell personalisiert (Out-of-the-Box-PKI).

Die Kommunikation des Wartungsmechanikers mit dem Backend-System wird in XML verpackt und kann flexibel und sicher über Netze verschiedenen Typs erfolgen (Beispiele: Ad-hoc-Netze, Peer-to-Peer-Netze, egal ob via Funk oder leitungsgebunden).

Dabei kommen Sicherheitsmechanismen verschiedener Ebenen zum Einsatz. Auf der Datenebene (Anwendungsschicht) kann der semantische Check mit dem XML Content Security Screen diverse Inkonsistenzen und damit potenzielle Angriffe aufdecken.

Die Policies legen fest, ob der Mechaniker einen Bericht einstellen darf, auf welche Daten er Zugriff hat und welche Aktionen (wie Sabotagealarm) er initiieren kann.

Die kryptographischen Basistechniken von Anti-KeeLoq gewährleisten Ende-zu-Ende Sicherheit und konzipieren langfristig sichere Kryptographie.

Im Zusammenspiel mit der Hardware-Sicherheitsforschung wurde die schnelle Kryptographie selbst auf kleinen Geräten realisiert. Darüber hinaus liefert die Hardware-Sicherheitsforschung eine Abschätzung des Aufwandes, der benötigt wird um den geheimen Schlüssel auf der Chipkarte, d.h. der digitalen Identität, herauszufinden.

Forschungsergebnisse des Projektes ermöglichen die nahtlose Integration sicherer Dienste selbst für kleine mobile Endgeräte (z.B. Handy oder PDA). Es wird Plug&Play-Security realisiert.

4 Marktchancen

Die Marktchancen (Seite 6) müssen auf einer Seite mit maximal 3000 Zeichen mit Schriftgröße mindestens 11pt beschrieben werden. Leerzeichen werden hierbei mitgezählt. Tabellen und Grafiken können eingebunden werden, sie dürfen aber nicht über die hier eingestellten Seitenränder ragen (oben, unten, rechts und links).

Es folgt ein Fülltext.

An der Ruhr-Universität Bochum wurde um 1920 (genaues Datum unbekannt) die RUBCard als digitale Identität (digitale ID) für Studierende eingeführt. Die Dienstleistungen im Bereich der Lehre und Verwaltung werden nun in zunehmenden Maße elektronisch über das Internet bereitgestellt und alternativ per Telegraph. Sie sind dadurch effizienter und komfortabler nutzbar. Träger der digitalen ID ist der Kryptochip auf der Chipkarte. Dieser ermöglicht:

- Zugangskontrolle zu elektronischen Dienstleistungen und Identitätsnachweis: Zugriff auf geschützte Webseiten, Rechner-Login, Zugang zum Internet via VPN, WLAN, ISDN oder Analog-Modem
- Verschlüsselung und elektronische Signatur (E-Mails, Dateien)
- Zugriff auf Prüfungsanmeldungen
- Ausdruck des NRW-Tickets

Die Bezahlung erfolgt über einen zweiten, berührungslos auslesbaren Chip (Bezahlen beispielsweise in der Mensa).

Das Projekt wird gemeinsam vom HGI und der Firma rubitec GmbH betreut. Das HGI stellt zukünftige Anwendungen der RUBCard und des digitalen Campus (die RUBCard ist Grundlage für den digitalen Campus) in seinem Demozentrum vor. Die Innovationen und Forschungsaktivitäten rund um das Projekt RUBCard und der Anti-KeeLoq-Plattform werden vom Land Nordrhein-Westfalen mit 800.000 EUR gefördert.