www. CIDAS .org

Configurable Internet Directory and Authentication Service

Fachhochschule Brandenburg

Kolloquium zur Diplomarbeit

„Konzeption und prototypische Umsetzung von Authentifizierungsverfahren und Kommunikationsschnittstellen für das Identity-Management-System CIDAS unter besonderer Berücksichtigung mobiler identifizierbarer Datenträger“

Vorgelegt von:

Jan Tobias Mühlberg
<muehlber@fh-brandenburg.de>

Betreut von:

Prof. Dr. Friedrich-L. Holl und
Prof. Dr. Barbara Wiesner

Brandenburg, den 25. Mai 2004

Was ist eigentlich CIDAS?

CIDAS ist ein freies und universell einsetzbares Authentifizierungs- und Identity-Management-Framework. Im Gegensatz zu bereits am Mark verfügbaren Konkurrenzprodukten wie Microsoft Passport ermöglicht es die Verwendung von nicht-textuellen Verfahren zur Benutzerauthentifizierung. Zum Einsatz kommen beispielsweise kryptographische oder biometrische Verfahren. Da CIDAS nicht auf HTTP als Kommunikationsprotokoll angewiesen ist, kann es sehr flexibel eingesetzt werden. CIDAS wird an der Fachhochschule Brandenburg unter Leitung von Herrn Prof. Dr. Holl entwickelt.

Die Aufgabenstellung

Ausgangssituation:
Es existierte ein Konzept für CIDAS und die Idee, passive Datenträger – primär USB-Sticks – als Authentifizierungsgeräte nutzbar zu machen.

Daraus resultierende Aufgabenstellung:

1. Entwicklung eines Kommunikationsprotokolls für den Datenaustausch zwischen CIDAS-Server und -Client
2. Überprüfung der Einsetzbarkeit passiver Speichermedien für die Authentifizierung von Benutzern, Analyse verwendbarer Authentifizierungsverfahren, Konzeptentwicklung
3. prototypische Umsetzung

Ergebnisse der Arbeit

Entwurf des Authentifizierungsverfahrens
Um vorhandene Schwachstellen in bereits verfügbaren Verfahren zu vermeiden, wurde vom Autor der Versuch der Konzeption eines eigenen Authentifizierungsprotokolles unternommen. In der Diplomarbeit wird unter Anwendung gängiger Analysemethoden gezeigt, daß das resultierende Verfahren eine einseitige Benutzerauthentifizierung basierend auf asymmetrischem Schlüsselmaterial erlaubt. Darüber hinaus wird gezeigt, daß Benutzer bei der Verwendung des neuen Verfahrens niemals von ihnen nicht beeinflußbaren Daten signieren oder verschlüsseln muß. Es werden standardisierter Datenformate verwendet.

Entwurf des Kommunikationsprotokolles
In Anlehnung an existierende Kommunikationsprotokolle wurde vom Autor ein nachrichtenorrientiertes, zustandsabhängiges Protokoll für CIDAS entworfen. Es ermöglicht die Nutzung der folgenden von CIDAS gebotenen Funktionalität:

- Identifizierung, Authentifizierung
- Behandlung und Austausch von Autorisierungsinformationen
- Änderungen an den Datenbeständen
- Nutzung zusätzlicher Funktionalität des Servers

Die prototypische Umsetzung
Die konzipierten Protokolle und Verfahren wurden als „Proof of Concept“ größtenteils umgesetzt. Unter Mithilfe von Herrn Markus Dahms entstanden Prototypen für einen CIDAS-Server und -Client, der Quellcode ist auf Anfrage unter den Bedingungen der GNU GPL verfügbar.