

Ablösung des elektronischen Zugangssystems an der TUC

Das URZ und andere Struktureinheiten betreiben seit 1994 ein kommerzielles elektronisches Tür-Zugangs-Kontrollsystem der Firma "effeff". Mit diesem System werden UNI-weit insgesamt 55 Türen mittels Magnetkartenleser vor unbefugten Zutritt geschützt.

Das Zugangssystem besteht aus einer Vielzahl von Hardware- und Software-Komponenten. Mehrere PC-Systeme (Master), auf denen eine MS-DOS Applikation läuft, steuern über einen Feldbus (RS485) bis zu 32 Tür-Controller (siehe Bild1). Diese Controller sind so konstruiert, dass sie auch ohne Verbindung zum Master oder nach einem Stromausfall auf Grund der aktuell gespeicherten Zugangsinformationen funktionstüchtig sind. Das bedeutet, dass alle relevanten Zugangs- und Magnetkarteninformationen auf jedem einzelnen Tür-Controller vorgehalten werden müssen.

Die MS-DOS Steuerapplikation für das Zugangssystem wurde vom URZ mittels trickreicher Mechanismen in die damals vorhandene Nutzer-Verwaltungs-Infrastruktur eingebunden. Weiterhin wurden im Jahr 2000 mit der Einführung der eigenentwickelten Managementsoftware MoUSe (Management of User and Services) die von den einzelnen Struktureinheiten separat betriebenen Teilsysteme zusammengefasst, um so eine einheitliche "Fernbedienung" des vorhandenen Zugangssystems zu realisieren.

Grenzen des alten Zugangssystems

Die damals angeschaffte Version des Zugangssystems konnte maximal 9999 verschiedene Magnetkarten unterscheiden. Dies wird im Wintersemester 2002 mit der neuen Immatrikulationswelle zu einem Problem, da derzeit schon 8422 Karten ausgegeben sind, und mit 2000 Neuimmatrikulationen gerechnet wird. Weiterhin ist die alte Lösung nicht offen und auf DOS-PC's als Steuerrechner fixiert und somit nur mit viel Aufwand integrierbar und erweiterbar. Aus diesen Gründen wurde im Jahr 2000 entschieden, das System durch ein innovatives Produkt abzulösen. Es wurden Angebote für Weiterentwicklungen und neue Systeme eingeholt.

Vorgaben an das neue System waren unter anderen:

- Alle ausgegebenen Karten müssen weiter funktionstüchtig sein.
- Eine Integration in vorhandene Infrastruktur muss möglich sein (vor allem die

Anbindung an die Nutzerverwaltung des URZ).

- Bis zu 20000 Nutzer muss das System verkraften.
- An zentraler Stelle durchgeführte Modifikationen von Zugangsbefugnissen müssen sofort an allen Türen wirksam werden.

Es hat sich jedoch herausgestellt, dass die verfügbaren kommerziellen Produkte die meisten unserer Forderungen nicht erfüllen. Am schwerwiegendsten jedoch wäre die enorme finanzielle Belastung bei der Einführung eines neuen kommerziellen Systems.

Eigenentwicklung

Aus oben genannten Gründen hat sich das URZ dazu entschlossen, ein eigenes Zugangssystem sowohl software- als auch hardwareseitig unter dem Namen **DACS (Distributed Access Control System)** zu entwickeln. Die Entwicklungsleistung wurde ausschließlich durch eine studentische Hilfskraft, im Rahmen einer Studienarbeit und eines Praktikums erbracht.

Das entwickelte Zugangssystem wird derzeit an 4 Türen in der Universität getestet (Computerpool 066, Sun-Pool in der Informatik, Raabestraße Hintereingang und Computerpool Raabestraße).

Für das Zugangssystem wurden auch eigene Tür-Steuer-Controller entwickelt, welche demnächst für die Universität produziert werden.

Vorteile

Neben der wichtigsten Neuerung, über 9999 verschiedene Personen identifizieren zu können, gibt es weitere Vorteile unseres eigenen Zugangssystems. Im Vergleich zum alten Zugangssystem, bei dem der Updatezyklus neuer Berechtigungsinformationen ein halber Tag war, dauert die Propagierung neuer Zugangsinformationen beim neuen System nur noch wenige Sekunden. Die Integration in die vorhandene Infrastruktur ist sehr gut möglich, da das ganze Projekt als OpenSource entwickelt worden ist. Weiterhin verhält sich das verteilte Zugangssystem als ein einheitlich arbeitendes System. Bei der Entwicklung wurde auch darauf geachtet, dass das System skalierbar bleibt. Es ist nun möglich, ohne viel Aufwand beliebig viele Türen oder andere Objekte durch DACS zu schützen.

Eine weitere Vorgabe war, dass alle ausgegebenen Karten weiter funktionieren müssen. Auch dieses Ziel wurde im Gegensatz zu anderen Produkten erreicht. Neben den alten Cronoskarten, den TUC-Karten und zukünftig neu ausgegebenen Karten ist es darüber hinaus möglich, später andere Authentifizierungsverfahren, wie z.B. den berührungslosen Chip auf der TUC-Card, zu nutzen.

Technik Details

Wie schon erwähnt besteht das Zugangssystem aus Hardwarekomponenten, welche an jeder Tür installiert sind und aus Softwarekomponenten, welche die Tür-Controller steuern.

In den Türcontrollern arbeitet ein embedded Board mit einem embedded AMD 133 Mhz Prozessor, 32 Mbyte Ram und 16 Mbyte Flash (DiscOnChip2000). Auf dem Flash-Speicher ist ein eigenentwickeltes Linux für embedded PC's installiert. Gleichzeitig hält dieser Speicher alle relevanten Zugangsinformationen vor. Das System ist nach einem Stromausfall sofort wieder einsatzbereit.

Softwareseitig wurde ein verteiltes Dienstesystem entwickelt, mit dem es sehr einfach möglich ist, eine Vielzahl von Diensten und Controllern zu verwalten. Somit ist das Beherrschen von vielen Knoten in einem Gesamtsystem sehr einfach geworden.

Um die Funktionalität des Zugangssystems zu realisieren, wurden eine Vielzahl von selbstständigen DACS-Diensten entwickelt. Diese Dienste kümmern sich um das Aktualisieren der Controller, um die Systemüberwachung, um das Einsammeln von Statusinformationen. Auf dem Controller selbst arbeiten wiederum auch selbstständige Dienste, welche z.B. Personen anhand von Magnetkarten identifizieren, die Tür-Magnetöffner steuern oder Zugangsinformationen verwalten.

Weiterhin wurde ein Linux-Kernel-Netzwerktreiber für die Kommunikation über einen Feldbus (RS485) entwickelt, um das vorhandene Bussystem weiter zu nutzen. Somit ist es möglich, die neuen Tür-Controller ohne bauliche Veränderungen zu installieren.



*Bild 1: Zugangskontrollgerät
des
alten Zugangssystems*



*Bild 2: Eigenentwickelter
DACS-Tür-Controller*

Umstellung

Derzeitig sind bereits 4 von 55 Türen auf das neue System umgerüstet und das Hintergrundsystem ist in die vorhandene Managementinfrastruktur eingebunden. Die restlichen Systeme werden sukzessive in den nächsten Jahren durch neue Geräte ersetzt. Eine gleichzeitige Umrüstung aller Türen ist auf Grund der aktuellen Haushaltslage nicht möglich. Somit wird das alte und das neue System in den nächsten Jahren parallel betrieben. Für das neue System stellt dieses Vorgehen kein Problem dar, da hier die Identifikationskennung auf den Karten (Magnetstreifen der TUC-Card) frei wählbar ist. Alte und neue Identifikationskennungen können unterschieden werden. Erweiterte (neu) Kennungen werden jedoch von dem alten Zugangssystem abgewiesen. Dies bedeutet, dass an noch nicht erneuerten Tür-Controller-Karten mit erweiterter Kennung nicht funktionieren.

Zuerst werden die Controller an jenen Türen getauscht zu denen ein großer Personenkreis Zugang hat (zentrale Pools). Die Umstellung an Türen zu Speziallaboren und Fakultätspools muss aus dem o.g. Grund später erfolgen. Nutzer, die dafür Zutritt benötigen, können bis zur Umstellung keine Karten mit erweiterter Kennung erhalten. Mit Hilfe von MoUSE wird abgesichert, dass Karten mit erweiterter Kennung zunächst nur an neue Studenten aus der Philosophischen und der Naturwissenschaftlichen Fakultät ausgegeben werden, da diese potenziell nur zugangesicherte Türen vom URZ nutzen (diese Fakultäten haben keine Türen, die durch das Zugangssystem des URZ geschützt sind). Alle anderen Nutzer erhalten bis zur endgültigen Umstellung eine Identifikationskennung auf ihrer Karte, die an allen Türen funktioniert. Durch diese organisatorische Massnahme wird die Umstellung für nahezu alle Benutzer unbemerkt erfolgen.

Sollte dennoch der Fall eintreten, dass ein Nutzer, welcher eine erweiterte Kennung auf seinem Ausweis hat, zu einer nicht umgerüsteten Tür Zugang erlangen möchte, so kann dieser sich im Nutzerservice seine TUC-Card auf das alte Format umschreiben lassen. Somit ist der Zugang zu beiden Systemen wieder möglich.



Bild 3: Magnetkartenleser an

Fazit

Durch die Eigenentwicklung DACS als Ablösung für das elektronische Tür-Zugangs-System fallen bei der Umstellung und in Zukunft pro Tür über die Hälfte weniger Kosten für die benötigten Tür-Controller an. Software- und Lizenzkosten (bei kommerziellen Produkten im 5-stelligen Bereich) entfallen vollständig. Dadurch konnte ein beachtlicher Betrag eingespart werden, welcher der gesamten Universität zugute kommt.

Es wurde ein verteiltes Zugangskontrollsystem geschaffen, welches nicht nur an der TU Chemnitz, sondern potenziell auch für den Einsatz an anderen Hochschulen geeignet ist. Darüber hinaus ist es flexibler und erweiterungsfähiger als kommerzielle Systeme und basiert ausschließlich auf OpenSource.

Literatur:

- Ronald Schmidt: [Verteilte Zugangssteuerung](#), Studienarbeit 2002

[Ronald Schmidt](#), Juli 2002