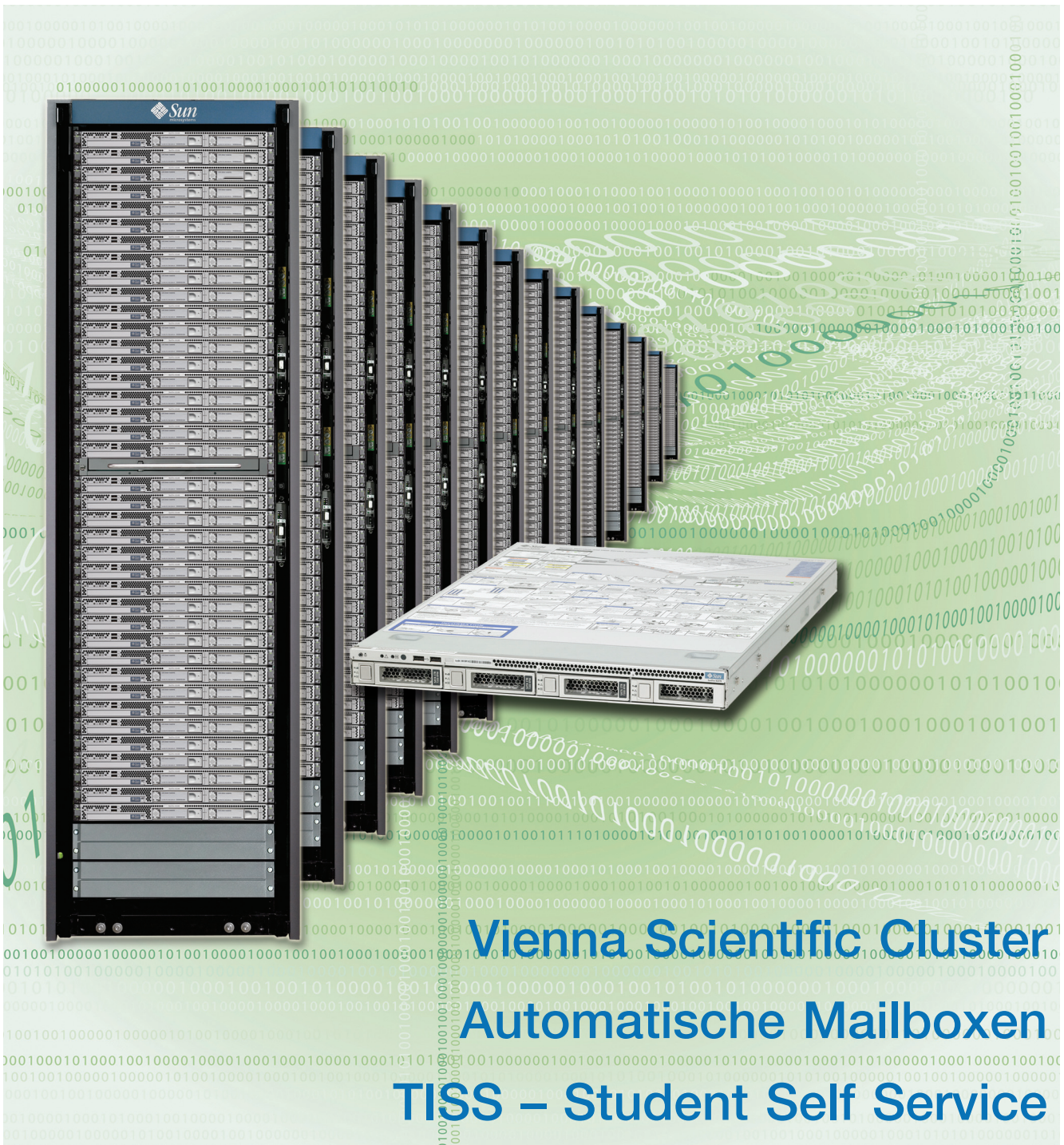


ZiD *line*

ZEITSCHRIFT DES ZENTRALEN INFORMATIKDIENSTES DER TU WIEN



Vienna Scientific Cluster
Automatische Mailboxen
TISS – Student Self Service

Inhalt

Vienna Scientific Cluster	3
TISS – Neue Workflows für Studienabschlüsse und den Zeugnisdruck	7
Geoblocking des MS XP Professional Produktschlüssels	11
Automatische Mailboxen und eindeutige generische E-Mail-Adressen.	12
Externer Zugang zu den Lizenzservern	14
Windows Server 2008 – nicht nur Verbesserungen	15
Feuerwände für das TUNET	18
Mobiles Gebäudesicherheitsmanagement Ein TISS Projekt.	20
NI Multisim 10.0 Elektronikdesign und -test mit virtuellen Instrumenten in der studentischen Ausbildung.	23
TISS is digging deep – Software Reengineering supported by Database Reverse Engineering	25
IT-Handbücher des RRZN	30
Auskünfte, Störungsmeldungen: Service Center.	31

Impressum / Offenlegung gemäß § 25 Mediengesetz:

*Herausgeber, Medieninhaber:
Zentraler Informatikdienst
der Technischen Universität Wien
ISSN 1605-475X*

*Grundlegende Richtung: Mitteilungen des Zentralen
Informatikdienstes der Technischen Universität Wien*

Redaktion: Irmgard Husinsky

*Adresse: Technische Universität Wien,
Wiedner Hauptstraße 8-10, 1040 Wien
Tel.: (01) 58801-42014, 42002
Fax: (01) 58801-42099
E-Mail: zidline@zid.tuwien.ac.at
WWW: <http://www.zid.tuwien.ac.at/zidline/>*

*Erstellt mit Corel Ventura
Druck: HTU Wirtschaftsbetriebe GmbH,
1040 Wien, Tel.: (01) 5863316*

Editorial

Die Entscheidung für den Vienna Scientific Cluster, den gemeinsamen Hochleistungsrechner von Universität Wien, Universität für Bodenkultur und TU Wien, ist gefallen. Im Sommer wird er in Betrieb gehen.

Aus dem hausinternen Entwicklungsprojekt für Informations-Systeme und Services – TISS – ist zu berichten, dass unter Einsatz neuer Technologien ein mobiles Gebäudesicherheitsmanagement implementiert wurde. Ein Prototyp für die Abwicklung bei Studienabschlüssen ist in allen Dekanaten der TU im Einsatz. Im so genannten Student Self Service können Einzel- und Sammelzeugnisse bereits selbst ausgedruckt werden. Zur Dokumentation der technischen Aspekte hinter dem TISS-System veröffentlichen wir eine Zusammenfassung aus einer Diplomarbeit, die in englischer Sprache verfasst ist und Database Reengineering zum Thema hat.

Über das TUpPhone-Projekt – Ersatz der bestehenden Telekommunikationsanlage durch eine moderne VoIP-Anlage – kann im Moment nichts Neues berichtet werden. Das Ausschreibungsverfahren läuft noch.

Für die TU-interne dienstliche Erreichbarkeit erhalten alle Personen im Personalstand der TU Wien automatisch eine Mailbox vom ZID. Außerdem werden eindeutige und intuitive generische E-Mail-Adressen für alle eingerichtet.

Weitere Themen in dieser Ausgabe der ZIDline sind: Geoblocking des Microsoft XP Professional Produktschlüssels, Windows Server 2008, Firewalls, Lizenzserver sowie Campus Software Multisim in der Anwendung.

Ich bedanke mich sehr herzlich bei allen Autoren – ZID-Mitarbeiter und externe – für ihre Kooperationsbereitschaft und ihre interessanten Beiträge.

Am 13. Oktober 2009 werden wir wieder einen so genannten **ZID-Day** veranstalten. Bitte merken Sie sich den Termin vor, besuchen Sie uns im Freihaus und informieren Sie sich über unsere Services und über interessante neue Projekte.

Irmgard Husinsky

www.zid.tuwien.ac.at/zidline/

Vienna Scientific Cluster

Der gemeinsame Hochleistungsrechner von Universität Wien, Universität für Bodenkultur und TU Wien

Peter Berger

Herbert Störi, Institut für Allgemeine Physik

Wie bereits in der letzten ZIDline [1] berichtet, bemühen sich die drei Universitäten, gemeinsam einen Hochleistungsrechner zu beschaffen. Nach einem intensiven Workshop mit potentiellen Anwendern und nach Abschluss des Ausschreibungsverfahrens wird nun ein entsprechendes Clustersystem von Sun Microsystems im Sommer an der TU Wien aufgestellt werden. Die Finanzierung erfolgt aus dem Globalbudget der beteiligten Universitäten.

Computational Science and Engineering Workshop [2]

Die zukünftigen Anwendungen des Supercomputers wurden über Einladung von Frau Prof. Seidler (Vize-Rektorin für Forschung der TU Wien) bei einem gemeinsamen Workshop mit Anwendern aller drei beteiligten Universitäten diskutiert. Der Workshop fand am 8. und 9. Jänner im Seehotel Rust statt. Bei den Vorträgen und Diskussionen im Rahmen des Workshops zeigte sich, dass eine unerwartet große Zahl von relativ gut skalierenden parallelen Programmen existiert, andererseits aber die Parallelisierung mit MPI immer noch der Standard ist und viele Programme eine entsprechend leistungsfähige Kopplung zwischen den Rechnerknoten brauchen. Ein mehr oder weniger kompakter Rechner-Cluster, dessen Knoten mit einem Hochgeschwindigkeitsnetzwerk (etwa InfiniBand) gekoppelt sind, kann also nur in einzelnen Fällen durch lose gekoppelte Rechner (Grid Computing) ersetzt werden.

Neue Konzepte der parallelen Verarbeitung und neue Entwicklungstools sind für die Zukunft sicher ein wesentlicher Punkt. Die Hoffnung ruht hier einerseits auf der Tatsache, dass mit der zunehmenden Verbreitung von multi-core Prozessoren die Parallelisierung zu einem Element der main-stream Softwareentwicklung wird, und andererseits auf der konkreten Beteiligung der Informatik am gegenständlichen Projekt. Eine projektierte Kooperation zwischen Prof. Dustdar (TU, verteilte Systeme) und Prof. Kreil (BOKU, Bioinformatik) ist hier ein erster konkreter Ansatz.

Es wurde auch klar, dass im Moment Prozessoren mit Intel-artiger Architektur und das Betriebssystem Linux den gemeinsamen Standard darstellen. Einige verwendete Programme sind für andere Architekturen nicht verfügbar. In Zukunft könnte aber auch eine speziell für Hochleistungsrechner adaptierte Version von Windows auch hier eine zunehmende Rolle spielen.

Steering Committee

Fragen in Zusammenhang mit dem Vienna Scientific Cluster (VSC) werden auf oberster Ebene von einem gemeinsam besetzten „Steering Committee“, bestehend aus den Vizerektoren für Forschung, den Leitern der zentralen Informatikdienste (ZID) und Vertretern der Nutzer entschieden. Bisherige Aufgaben waren die Freigabe der Ausschreibung, die Zuschlagsentscheidung und Diskussionen über die Regelung des Zugangs zum VSC für Wissenschaftler.

Ausschreibung

Bei der ersten Sitzung des Steering Committees am 20. Jänner wurde der Ausschreibungstext genehmigt und das System in den folgenden Tagen europaweit ausgeschrieben. Verlangt wurde ein Cluster, dessen Knoten über Prozessoren mit x86-Architektur, 64 bit, und über mindestens 2 GByte Hauptspeicher je Prozessor-Kern (core) verfügen und untereinander mindestens mit InfiniBand 4xDDR (20 GBit/s full duplex, netto 16 GBit/s) vernetzt sind. Aus Kostengründen war allerdings eine Reduktion der Bandbreite im Backbone-Bereich erlaubt. Teilt man den Cluster von n Knoten gedanklich in 2 Teile zu $n/2$ Knoten, dann müsste die gesamte Bandbreite der Netzwerkleitungen, die die Teilungslinie überqueren, eigentlich $n/2 \cdot 16$ GBit/s je Richtung betragen. Diese Forderung wurde auf die Hälfte reduziert, d. h. ein Blockierungsfaktor von max. 2 wurde zugelassen.

Der maximal zulässige Preis inklusive Cluster-Kühlsysteme und Mehrwertsteuer war 1,6 Millionen €. Zur Beurteilung der Leistungsfähigkeit wurden den Anbietern eine Anzahl von Benchmark-Programmen übergeben, welche hauptsächlich aus Programmen zukünftiger Anwender bestehen. Die Bewertung erfolgte auf Basis eines Punktesystems, das hauptsächlich auf den Gesamtdurchsatz des Systems abstellte. Ende der Ausschreibungsfrist war der 31. März 2009.

Insgesamt wurden von 10 Anbietern 13 Angebote eingereicht. Alle Angebote enthielten Knoten mit je 2 Quad-Core Prozessoren (insgesamt 8 Prozessor-Kerne) und je 16, 18 oder 24 GByte Hauptspeicher. Die angebotenen Prozessoren waren entweder Intel Nehalems (X55x0) oder AMD Opterons mit 2,26 bis 2,93 GHz. Das Rennen war in der Spitzengruppe eher spannend; es gab 4 weitere Angebote, welche weniger als 10% hinter dem Bestbieter lagen.

Zuschlag

Bei der Steering Committee Sitzung am 21. April wurde entschieden, dem laut Punktesystem bestbewerteten Angebot den Zuschlag zu erteilen. Dabei handelt es sich um ein System von Sun Microsystems, welches von der Wiener Firma IPS angeboten wurde. Das angebotene System besteht aus 424 Knoten mit je 2 Intel X5550 Nehalem Prozessoren mit 2,66 GHz und je 24 GByte 1,333 GHz DDR3 RAM als Hauptspeicher und je einer 500 GByte SATA Platte. Die Kopplung erfolgt über InfiniBand [5] mit gemischter DDR und QDR (40 Gbit/s full duplex, netto 32 GBit/s) Geschwindigkeit (siehe Abbildung „InfiniBand-Netzwerkstruktur“). Ein zusätzliches GBit-Ethernet sorgt für den Zugriff auf die Fileserver. Zusätzlich hat das System 5 Zugangsknoten. Alle Knoten und Netzwerk-Komponenten werden in 14 konventionelle 19-Zoll Rack-Schränke eingebaut.

Die theoretische Spitzenleistung des Systems beträgt $R_{peak}=36,1$ TFlops, die tatsächliche Leistung R_{max} dürfte

bei ca. 30 TFlops liegen [4]. Der gesamte Hauptspeicher beträgt etwa 10 TByte.

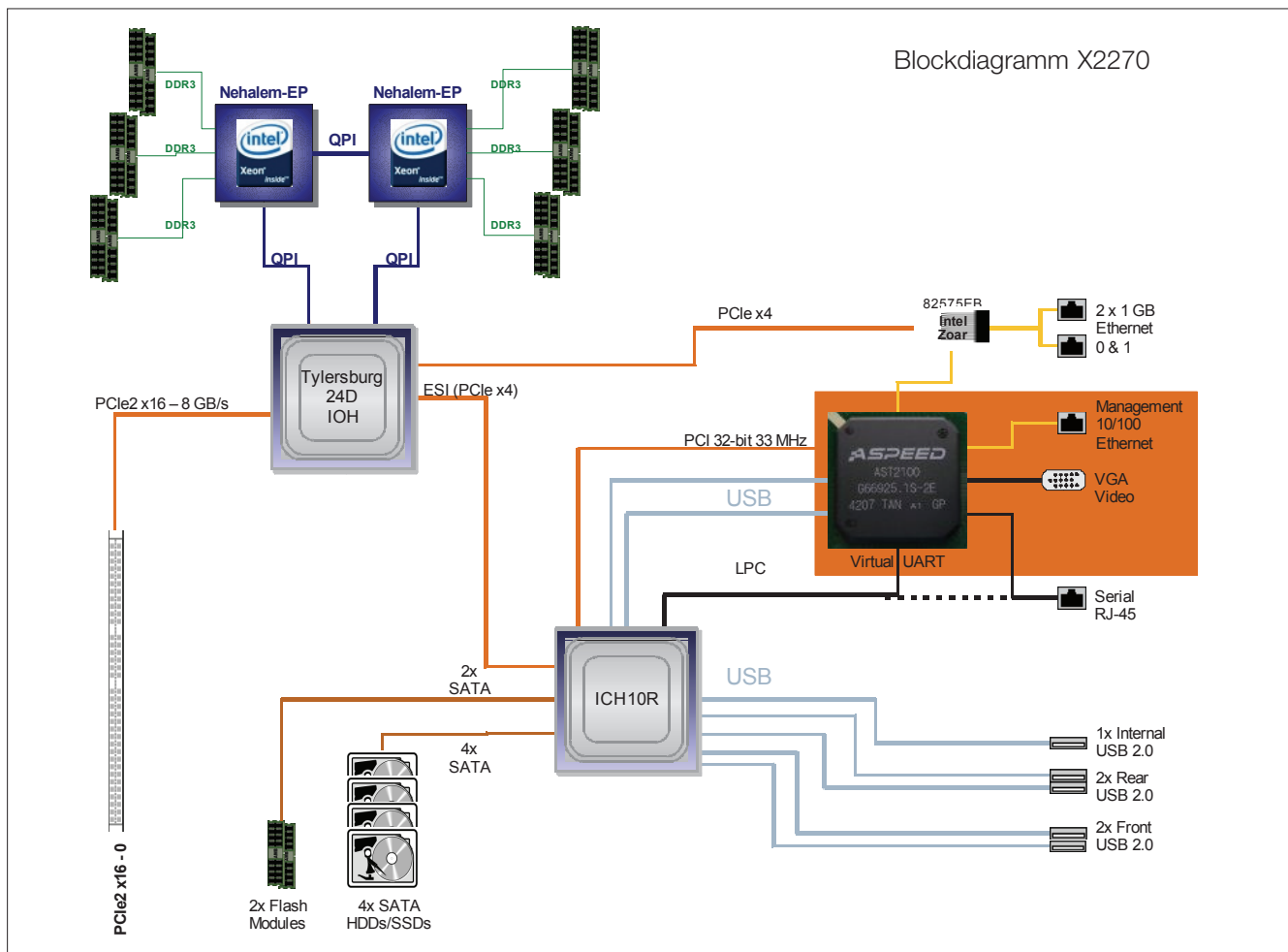
Das System wird eine Anschlussleistung von ca. 150 kW haben. Die Knoten und Netzwerk-Komponenten sind luftgekühlt und blasen die warme Abluft in einen geschlossenen Gang, aus dem sie von Kühlgeräten abgesaugt und wieder auf Raumtemperatur gekühlt wird (Warmgangeinhausung).

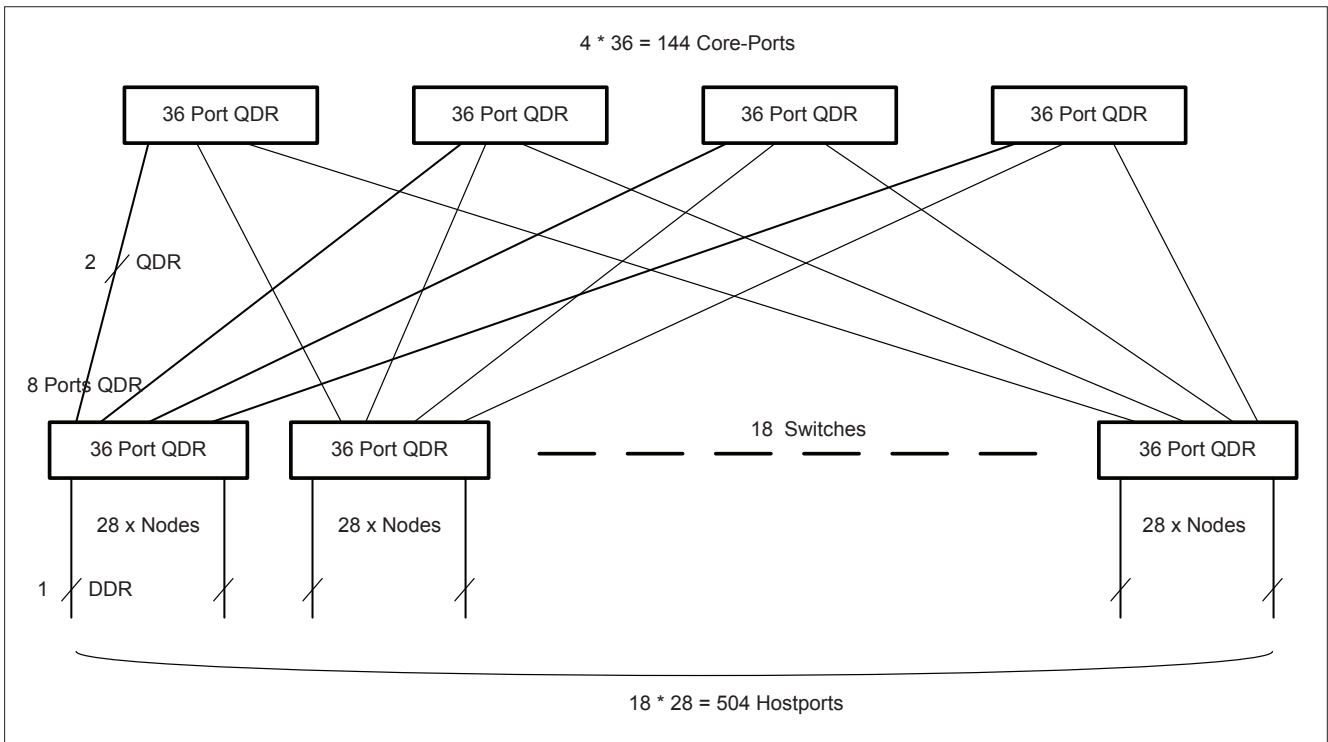
Die angebotenen Systemkomponenten im Detail

Compute Nodes

Als Compute Nodes werden 1U Rackmountserver (Sun Fire X2270) zum Einsatz kommen, die mit den neuesten Intel Nehalem CPUs ausgestattet sind.

CPU:	2x Intel Xeon X5550 4-Kern Prozessor Nehalem 8 MB L3 Cache, 2.66 GHz, 6,4 GT/s QPI, 95 Watt
Hauptspeicher:	24GB (6x 4 GB DDR3-1333 Registered ECC Memory)
Festplatten:	1x 500 GB SATA Festplatte, 3,5 Zoll, 7.200rpm
Powersupply:	1x Stromversorgung
Netzwerk:	2x 10/100/1000 Ethernet Anschluss on Board
Chipset:	Intel Tylersburg 24D
Management:	ILOM Service Prozessor Module





InfiniBand Netzwerkstruktur

InfiniBand Netzwerk

Für die Kopplung der Clusterknoten für die Parallelisierung wird ein schneller Cluster Interconnect über InfiniBand zur Verfügung gestellt. Die IB Fabric wird in QDR Technologie aufgebaut (*Quad Data Rate*, 40 Gbit/s full duplex, 8B/10B Codierung – 32 Gbit/s netto), wobei jedoch DDR HCAs (*Double Data Rate Host Channel Adapter*) in den Servern verwendet werden. Als Switches kommen 36 Port Switches zum Einsatz. Dabei werden 4 Spine- und 18 Edge-Switches verwendet. Zwischen den Spine und Edge Switches werden 8 Uplinks verwendet. Daher stehen $18 \cdot 28 = 504$ Ports für Compute Nodes, Zugangsknoten und externe Systeme zur Verfügung.

Core Switches:	2x Qlogic Truescale 12300 (36ports QDR), managed 2x Qlogic Truescale 12200 (36ports QDR), unmanaged
Edge Switches:	18x Qlogic Truescale 12200 (36ports QDR), unmanaged
HCA:	QLE7240 Truescale/Infinipath HCAs (Single Port 4x DDR)
IB Kabel:	QSFP-CX4 Cables for Host connection QSFP-QSFP Optical Cables core-edge connection

Gbit-Netzwerk

Das Gbit-Netzwerk dient vor allem für das Fileservice (NFS) und zum Booten der Compute-Nodes. Die Fileserver sind mit je 10 Gbit/s Ethernet angeschlossen, die Zu-

gangsknoten haben je 2 Anschlüsse in das jeweilige Netzwerk der Universitäten.

Es ist in naher Zukunft geplant, das Fileservice ebenfalls über InfiniBand zu realisieren.

Management Netzwerk

Sun verwendet für die Verwaltung und Steuerung der X86-Server ein ILOM (*Integrated Lights out Manager*) System. Dieses System ist eine Kombination der ILOM Service Prozessor (SP) Hardware und der ILOM Software Suite.

Mit ILOM ist das Monitoring und die Verwaltung der Systeme *remote* möglich. Der Service-Prozessor arbeitet unabhängig vom restlichen System und besitzt ein eigenes Management LAN Interface. ILOM beinhaltet ein eigenes Web-Interface (https), ein CLI (ssh oder seriell), ein SNMP Interface (v1,v2c,v3) und ein IPMI v2.0 Interface.

Zugangsknoten und Fileserver

Als Master- und Zugangsknoten kommen 5 Stück Sun-Fire X4245 (2 Sockel Intel Nehalem E5540) mit je 4x 300 GB SAS-Platten zum Einsatz.

Kühlung

Die Clusterkühlung wird mit Schrankkühlssystemen der Firma Knürr durchgeführt, 6 CoolLoops werden zwischen den Schränken installiert. Eine Cluster-Einhausung (geschlossene Decke, Schiebetüren) verhindern eine zu intensive Durchmischung der heißen Abluft mit der Raumluft.

Batch-System und Software

Betriebssystem

Als Betriebssystem wird Linux CentOS zum Einsatz kommen.

Sun HPC Software

Angeboten wurde die Sun HPC Software, Linux Edition 1.2. Dies ist ein umfassender Software Stack unter Linux, der es erlaubt, hochskalierbare Applikationen zu entwickeln, ablaufen zu lassen und den Cluster effizient zu managen. Abgedeckt werden hier unter anderem: Linux Distribution (CentOS, basierend auf Red Hat Enterprise Linux), Netzwerktreiber, Filesysteme und Werkzeuge für Provisionierung und Management.

Sun Studio Entwicklungstools für Linux

- C, C++ und Fortran 90/95 Compiler
- Debugger und Performance-Analyser für parallele Applikationen
- Shared Memory OpenMP
- Performance Library
- Open MPI Stack
- Intel C++ und Fortran Compiler 11 Professional Edition für Linux

Batch-System

Als Batch-System steht die „Sun Open Source Grid Engine“ zur Verfügung, es wird zurzeit der Einsatz eines kommerziellen Batch-Systems evaluiert.

Installation

Das System wird im Rechenraum im 2. Stock des Freihaus-Gebäudes der TU Wien installiert. Die Vorbereitung des Aufstellungsortes ist abgeschlossen. Dort musste vor allem der 20 Jahre alte Doppelboden saniert und verstärkt werden, da das System 7-8 Tonnen wiegen wird. Alte Glykol-Kühlleitungen des früher dort installierten CDC CYBER Mainframes wurden entfernt.



Hier wird das gekapselte Zuhause des Clusters entstehen

An einer neuen Kaltwasserzuleitung mit 150 mm Nennweite von der Kältezentrale im 11. Stock bis in den Rechenraum wird derzeit gearbeitet. Diese Arbeit gestaltet sich schwierig, da die Rohre neben einer Vielzahl von Kabeln in den Installationsschächten geschweißt werden müssen. Zusätzliche Stromzuleitungen sind bereits fertig gestellt.

Für die Installationsarbeiten am System selbst sind etwa 14 Tage anberaumt. Diese werden nach jetziger Planung in der ersten Hälfte des Monats Juli erfolgen. Anschließend erfolgt der Abnahmetest, bei dem die Benchmark-Leistung verifiziert wird, sowie ein 2-wöchiger Dauertest. Nicht unwichtig ist die Durchführung des so genannten LINPACK-Benchmarks, welcher für die Position in der Top500 Liste [3] der weltweit leistungsfähigsten Computer entscheidend ist. Wenn alles nach Plan läuft, startet der Benutzerbetrieb Anfang September.

Zugang und Betrieb

Die genauen Modalitäten der Account-Vergabe sind derzeit in Ausarbeitung. Jedenfalls soll der Zugang abgesehen von Test-Accounts auf wissenschaftlich begutachtete Projekte beschränkt werden. Bereits begutachtete, etwa von FWF oder EU finanzierte Projekte, werden dabei nicht nochmals begutachtet. In Ausnahmefällen ist auch eine Benutzung gegen Kostenerstatz möglich. Grundsätzlich werden Ressourcen für Projekte an einen Projektleiter vergeben, der dann die Möglichkeit haben wird, persönliche Accounts für Mitarbeiter auf einfache Weise anzulegen.

Ein professionelles Queueing-System wird eine entsprechend saubere Zuteilung von Ressourcen bei guter Gesamtauslastung ermöglichen. Für zeitkritische Arbeiten können je nach Bedarf und Genehmigung auch Reservierungen im Voraus verwaltet werden.

Die Fileserver dienen grundsätzlich dem Handling der bearbeiteten Jobs. Die Anwender werden für die Sicherung und Archivierung der Datenbestände selbst verantwortlich sein. Ein entsprechendes Massenspeicher- und Sicherungssystem hätte den finanziellen Rahmen deutlich gesprengt.

Links

- [1] Das HPC-Cluster Projekt. ZIDline 19, Dezember 2008: http://www.zid.tuwien.ac.at/zidline/z119/das_hpc_cluster_projekt/
- [2] Computational Science and Engineering Workshop (CSE 2009): 8. - 9. 1. 2009, Seehotel Rust: <http://www.infosys.tuwien.ac.at/autocompwiki/index.php/CSE09>
- [3] TOP 5000 Liste: <http://www.top500.org/lists>
- [4] LINPACK Benchmarks: <http://www.netlib.org/benchmark/hpl/>
- [5] InfiniBand: <http://www.infinibandta.org/home>
- [6] Vienna Scientific Cluster: <http://www.zid.tuwien.ac.at/vsc/>

TISS – Neue Workflows für Studienabschlüsse und den Zeugnisdruck

Andreas Böhacker, Ronald Steininger

Andreas Knarek, Monika Suppersberger, Wolfgang Kleinert

Nicht nur die Integration der bestehenden Services und Systeme der TU Wien zu einer einheitlichen Daten- und Servicebasis sondern auch die Konzeption und Entwicklung neuer Funktionen ist Teil des Projekts TISS. Auf dem Weg zur Gesamtlösung begegnet TISS immer wieder veralteten Abläufen, die nun mit Hilfe moderner Software effizienter gestaltet werden.

Neben der Entwicklung des neuen TU Adressbuchs, über das in der letzten Ausgabe der ZIDline bereits ausführlich berichtet wurde, der Implementierung zusätzlicher Features sowie der laufenden Erarbeitung neuer Konzepte zur Erweiterung der Funktionalität bis zur vollständigen Ablöse der White Pages hat sich TISS in den vergangenen Monaten auch mit der Entwicklung neuer Systeme befasst. Mit veralteten Abläufen und langjährigen Problemen wird aufgeräumt und so eine deutliche Arbeitserleichterung für Mitarbeiter erreicht. Eines der TISS-Projekte, durch das die TU Wien mit dem Einsatz neuer Technologien wieder einmal eine Vorreiterrolle einnimmt, beschäftigt sich mit mobilem Gebäudesicherheitsmanagement und wird ausführlich in einem gesonderten Artikel auf Seite 20 dieser Ausgabe dargestellt. Zwei weitere Teilsysteme, die vor allem für Mitarbeiter eine erhebliche Arbeitserleichterung mit sich bringen, aber auch für Studierende mehr Komfort und Flexibilität bieten, sollen in diesem Artikel vorgestellt werden.

Studienabschlüsse – TISS STAB

Mit dem Ziel, die Abwicklung von Studienabschlüssen zu verbessern und zu automatisieren, wurde im Sommer 2006 vom damaligen Vize-Studiendekan Dr. Heinrich Pangratz ein Projekt zur Entwicklung einer entsprechenden Softwarelösung für das Dekanat der Fakultät für Elektrotechnik und Informationstechnik ins Leben gerufen. Nach der Analyse aller Studienpläne und der zugehörigen Abläufe zur Abwicklung der Abschlüsse, konnte in enger Zusammenarbeit mit DI Edmund Dvorak, dem Leiter der ADV-Abteilung des ZID, ein passendes Datenmodell entwickelt werden. Beginnend mit einem ersten Prototypen

für das Dekanat wurden in mehreren iterativen Schritten neue Funktionen hinzugefügt, die Benutzbarkeit der Software optimiert und die Abschlussdokumente aktualisiert. Die in einem weiteren großen Schritt geschaffene Web-Applikation für die Studierenden erlaubt eine Voranmeldung zu Studienabschlüssen inklusive einer initialen Zuordnung der absolvierten Lehrveranstaltungen zum Studienplan und ersetzt somit die Anmeldebögen aus Papier.

Im Sommer 2008 fiel dann die Entscheidung, die für die Fakultät für Elektrotechnik und Informationstechnik entwickelte Software im Rahmen des TISS auch den anderen Fakultäten der TU zugänglich zu machen und für deren spezifische Bedürfnisse bei der Abwicklung der Studienabschlüsse zu erweitern bzw. anzupassen. In Besprechungen mit den Dekanen, Studiendekanen und Mitarbeitern der Dekanate hat sich gezeigt, dass trotz der oftmals gravierenden Unterschiede bei den verwalteten Studienplänen die Abläufe in den einzelnen Dekanaten doch sehr ähnlich sind: Die Anmeldung beginnt mit dem Ausfüllen eines Papierformulars durch die Studierenden, welches zumindest die persönlichen Daten, die absolvierten Lehrveranstaltungen entsprechend dem Studienplan und, falls notwendig, auch die Daten der Abschlussarbeit enthält. Die Studierenden bringen das Papierformular und die notwendigen Zeugnisse ins Dekanat, wo alle Daten und Zuordnungen durch die Mitarbeiter manuell überprüft werden müssen. Abhängig vom Studienplan werden die Studierenden zu Abschlussterminen zusammengefasst und für kommissionelle Prüfungen eingeteilt. Listen mit den gebildeten Kommissionen sind für die Studierenden, Prüferinnen und Prüfer sowie die Vorsitzenden zu erstellen und zu veröffentlichen bzw. zu versenden. Nachdem alle Prüfungen absolviert wurden, müssen die entsprechenden

Notenmittelwerte der einzelnen Prüfungsfächer oder Module berechnet, die Gesamtbeurteilung ermittelt und zusammen mit den persönlichen Daten der Studierenden in die Abschlussdokumente eingefügt werden. Letztendlich werden die Studienabschlüsse mittels Prüfungsbeleg an die Studien- und Prüfungsabteilung übermittelt und Kopien aller Abschlussdokumente im Dekanat abgelegt.

Basierend auf diesen einheitlichen Abläufen und den in den Gesprächen identifizierten Bedürfnissen der einzelnen Dekanate und Studienpläne, wurde mit der Erstellung eines ersten Prototypen von TISS STAB (STUDIENABSCHLÜSSE), der in allen Dekanaten der TU eingesetzt werden kann, begonnen. Wie wir in der letzten ZIDline (Dezember 2008) berichtet haben, konnte bereits im Wintersemester 2008/09 mit dem Testbetrieb in ausgewählten Dekanaten begonnen werden.

Mittlerweile ist die erste Version der Software zur Abwicklung der Studienabschlüsse in allen Dekanaten der TU im Einsatz, teilweise noch im Testbetrieb, in einigen Dekanaten aber auch schon im Produktivbetrieb. Natürlich sind die Anpassung der Abläufe und der Einsatz einer neuen Software mit Zeit- und Lernaufwand für die Mitarbeiter der Dekanate verbunden. Der produktive Einsatz in den einzelnen Dekanaten erfolgt daher erst dann, wenn die Mitarbeiterinnen und Mitarbeiter mit den veränderten Abläufen und Mechanismen ausreichend vertraut sind. Doch der Einarbeitungsaufwand wird durch einige praktische neue Funktionen schnell relativiert:

- Die Überprüfung aller an der TU ausgestellten Zeugnisse kann entfallen. Die Berechnung der Notenmittelwerte der einzelnen Prüfungsfächer und die Ermittlung der Gesamtbeurteilung erfolgen automatisch.
- TISS STAB unterstützt die Mitarbeiter der Dekanate bei der Bildung von Prüfungssenaten und der Abwicklung der kommissionellen Abschlussprüfungen. Die Benachrichtigung der Studierenden, der Prüferinnen und Prüfer und der Vorsitzenden sowie die Verteilung der Unterlagen können auf Wunsch per E-Mail erfolgen.
- Der Abschluss eines Studiums muss nicht mehr mit einem Prüfungsbeleg erfasst werden, sondern wird per Knopfdruck an die Studien- und Prüfungsabteilung übermittelt.
- Alle für die internen Abläufe benötigten Dokumente (z. B. Absolventenlisten, Diplomarbeitslisten, Prüfungseinteilungen etc.) und die an die Studierenden auszuhändigenden Dokumente (z. B. Abschlusszeugnisse, Bescheide, Diplome etc.) werden automatisch erstellt, ausgedruckt und gleichzeitig zentral archiviert. Letzteres soll u. a. zu einer deutlichen Reduzierung der Papierarchive in den Dekanaten führen.
- Für die Abwicklung von Abschlussfeiern (Sponsionen) können die notwendigen Diplome und Urkunden der teilnehmenden Studierenden und verschiedene Listen zur Durchführung der Feiern erstellt werden.
- Zahlreiche Statistikfunktionen erlauben u. a. die Erstellung von Tabellen mit den Daten der Absolventen oder das Ranking der Studierenden basierend auf deren Abschlussnoten.

Das Continuing Education Center der TU zählt mittlerweile auch zu den Benutzern von TISS STAB. Durch den engagierten Einsatz von Prof. Bob Martens und seinem Team ist es in kürzester Zeit gelungen, die Software für die Studien und Lehrgänge des CEC zu erweitern. Dank der einfachen und klar strukturierten Studienpläne kann das Weiterbildungszentrum besonders gut von den Automatismen der neuen TISS-Software profitieren.

In Zusammenarbeit mit dem Vizerektor für Lehre, den Studiendekanaten, der Rechtsabteilung und den Mitarbeitern der Dekanate ist es gelungen, einheitliche Bescheide und Abschlusszeugnisse für alle Fakultäten zu erstellen. Zusätzlich wird gegenwärtig an neuen Entwürfen für die Diplome gearbeitet, um diesen repräsentativen Dokumenten ein moderneres und an das Corporate Design der TU angepasstes Layout zu geben. Außerdem werden in Kürze allen Studierenden beim Abschluss auch Diploma Supplements direkt in den Dekanaten ausgestellt.


Das TISS-Team erhält durch die intensive Beschäftigung mit den derzeit gültigen Studienplänen und den zugehörigen Abläufen in den verschiedenen Dekanaten sowie durch die Gespräche mit den verantwortlichen Mitarbeiterinnen und Mitarbeitern wertvolle Informationen und Vorschläge für die Entwicklung eines neuen Studienplanmodells. Dieses neue Modell soll alle bisherigen Studienpläne abbilden können, aber auch gleichzeitig ein Framework für die Erstellung neuer Studienpläne bieten. In den letzten Jahren hat sich gezeigt, dass Anpassungen an bestehenden Studienplänen und die Einführung neuer Studienpläne in immer kürzeren Abständen erfolgen. Daher sind eine Optimierung der Abläufe und die Entwicklung von Software zur Unterstützung dieser Abläufe dringend notwendig, um die schnelle und effiziente Einbindung neuer Studienpläne in den Studienbetrieb zu ermöglichen. Eine verbesserte Darstellung der Studienpläne und eine Verknüpfung mit den Prüfungsdaten sollen sicherstellen, dass die Studienpläne leichter verständlich sind und die Studienfortschritte sowohl für die einzelnen Studierenden als auch für die Mitarbeiter in den Dekanaten jederzeit leicht ersichtlich sind.

Student Self Service

Neben der vereinfachten Abwicklung von Abschlussprüfung sorgen noch weitere, neue Services für die Entlastung der Mitarbeiter und für mehr Komfort und Flexibilität für Studierende. Dem Ziel, die Abläufe in der Studienabteilung für Mitarbeiter und Studierende zu verbessern, ist TISS mit der Entwicklung der ersten Student Self Services einen großen Schritt näher gekommen. Diese Services bieten derzeit den Selbsta Ausdruck von Einzel- und Sammelzeugnissen sowie auch z. B. der Bestätigung laut Familienlastenausgleichsgesetz (FLAG) an. Studierende können auf diese Dokumente nun bequem von zu Hause oder von jedem beliebigen Zugang aus zugreifen, als PDF herunterladen und bei Bedarf ausdrucken. Für die Mitarbeiter der Studienabteilung bedeutet dies, mehrere Zehntausend Bestätigungen und bis zu 150.000 Zeugnisse pro Jahr weniger ausdrucken und kuvertieren zu müssen. Für Studierende entfällt der Weg in die Studienabteilung, das

Warten auf die Post, aber auch die Gebühren für das Ausstellen eines Duplikats in dem Fall, dass ein Zeugnis verloren geht oder versehentlich im Altpapier landet. Sämtliche Dokumente, egal ob Bestätigungen oder Zeugnisse, werden zentral gespeichert und sind jederzeit abrufbar. Der Zugriff erfolgt über einen Link in TUWIS++, der auf die entsprechende Seite des Services in TISS führt. Um den Anwendern einen zusätzlichen Anmeldevorgang zu ersparen, wurde nun auch TUWIS++ an das TU Portal angebunden, das mittels SingleSignOn den Zugang zu mehreren Anwendungen nach einmaligem Login ermöglicht.

Da mit diesem Service nun alle Zeugnisse und Bestätigungen über das Web verfügbar sind, wird natürlich auch sichergestellt, dass kein unbefugter Zugriff auf diese Dokumente erfolgen kann. Da die bisherigen Echtheitsmerkmale, Stempel, Unterschrift und im Falle von Einzelzeugnissen auch ein spezielles Papier, durch den Selbstausdruck entfallen, muss es aber vor allem für Behörden wie beispielsweise das Finanzamt die Möglichkeit geben, die Echtheit des Dokuments zu prüfen. Um beiden Anforderungen gerecht zu werden, wird für jedes Dokument ein 25-stelliger Hashcode, zusammengesetzt aus Ziffern, Groß- und Kleinbuchstaben, generiert, der zur eindeutigen Identifizierung verwendet und als Teil einer URL auf das Dokument gedruckt wird. Über diese URL ist der Zugriff auf das Originalfile ohne vorherige Authentifizierung möglich. Ein Beispiel für ein Einzelzeugnis (die URL des Musterzeugnisses ist ungültig) ist in Abbildung 1 zu sehen, ein Musterexemplar eines Sammelzeugnisses in Abbildung 2.



TECHNISCHE
UNIVERSITÄT
WIEN
VIENNA
UNIVERSITY OF
TECHNOLOGY

DVR: 0001234

Kennzeichnung des Dokuments: Matrikelnummer:

Bestätigung des Studienerfolges


Summen MUSTERMANN MAX HAUPTSTR. 1 A - 1234 WIEN		SV-Nr.: 1234010180 Geburtsdatum: 01.01.1980 Staatsbürgerschaft: Österreich Geschlecht: Männlich Allg. Univ./Fache: 08/2000 Schulform: Gymnasium Heimatadresse: Hauptstr. 1 A - 1234 Wien Beitragstatus: Inländer
Studium Bachelorstudium Technische Chemie		

LV-Num.	Typ	Titel der Lehrveranstaltung	SS	ECTS	Datum	Beurteilung
187250	VO	Zwischen Karriere und Barriere	2.0	3.0	1.1.2000	(2) Gut
185322	VO	Praxisorientierte BWL	2.0	3.0	1.1.2000	(2) Gut
184158	VU	Internet-Applikationen	2.0	3.0	1.1.2000	(2) Gut
188427	VU	E-Commerce	2.0	3.0	1.1.2000	(2) Gut
185307	SE	Seminar aus Programmiersprachen	2.0	3.0	1.1.2000	(2) Gut
185208	VL	Programmiersprachen	2.0	3.0	1.1.2000	(2) Gut
185211	VL	Fortgeschrittene objektorientierte Programmierung	2.0	3.0	1.1.2000	(2) Gut
184207	VL	Component Based Software Development	2.0	3.0	1.1.2000	(2) Gut
184154	VL	Computer Networks	3.0	4.5	1.1.2000	(2) Gut
184260	VL	Technologien für Verteilte Systeme	4.0	6.0	1.1.2000	(2) Gut
183235	VU	Internet Security	2.0	3.0	1.1.2000	(2) Gut
183166	VU	Management von Software Projekten	2.0	3.0	1.1.2000	(2) Gut
184153	VU	Entwurfsmethoden für verteilte Systeme	2.0	3.0	1.1.2000	(2) Gut

Gesamtanzahl der Prüfungen: 0
 Gesamtanzahl der positiven Prüfungen: 13.0
 Gesamtanzahl der negativen Prüfungen: 0.0
 Gesamtanzahl der ECTS-Credits: 43.5
 Gesamtanzahl der Semesterstunden: 29.0
 Gesamtanzahl der positiven Semesterstunden: 29.0

Dieses Zeugnis kann über den unten angegebenen Link bzw. über den rechts aufgedruckten QR-Barcode (codierter Link) validiert werden.

<https://tiss.tuwien.ac.at/sss/ez/>



Seite 1/1

Abbildung 2:

Musterexemplar eines Sammelzeugnisses für den Selbstausdruck

Ein kleines Rechenbeispiel soll veranschaulichen, weshalb es beinahe unmöglich ist, durch Zufall (gewollt oder ungewollt) einen vergebenen Code zu erraten und damit unbefugten Zugriff auf ein Zeugnis oder eine Bestätigung zu bekommen (alle Zahlen sind Annahmen, die teilweise sehr großzügig aufgerundet wurden): Auf Grund der Zusammensetzung des Codes ergeben sich ca. $6,453 \cdot 10^{44}$ mögliche Kombinationen $((10+26+26)^{25})$ der Ziffern, Groß- und Kleinbuchstaben. Geht man davon aus, dass pro Jahr etwa 5.000 neue Studierende an der Universität zugelassen werden, für die im Laufe ihres Studiums ca. 2000 solcher Dokumente ausgestellt werden, ergibt das eine Anzahl von 10.000.000 Dokumenten pro Jahr. Wird nun ein fiktiver Beobachtungszeitraum von 1.000 Jahren angenommen, so kommt man auf eine Zahl von 10.000.000.000 Dokumenten – also $1,0 \cdot 10^{10}$. Selbst über diesen langen Zeitraum betrachtet, würde nur jeder $6,453 \cdot 10^{34}$ -te Code ein gültiges Dokument adressieren. Nimmt man nun an, dass ein Angreifer auf das System 1.000.000 Codes pro Sekunde ausprobieren könnte, würde er statistisch gesehen über $2,046 \cdot 10^{21}$ Jahre benötigen, um einen einzigen gültigen Code zu erhalten. Selbst wenn der Angreifer aus irgendeinem Grund rund die Hälfte der 25 Stellen eines gültigen Codes wüsste, würde es statistisch betrachtet mit der obigen Abfragegeschwindigkeit $1,023 \cdot 10^8$ Jahre andauern, bis durch das Ausprobieren von allen möglichen Kombinationen das entsprechende Dokument gefunden werden würde.



TECHNISCHE
UNIVERSITÄT
WIEN
VIENNA
UNIVERSITY OF
TECHNOLOGY

DVR: 0001234

Kennzeichnung des Dokuments: Matrikelnummer:

Lehrveranstaltungszeugnis

akademische Grade, Familienname, Vorname(n) MUSTERMANN MAXIMILIAN		Geburtsdatum 01.01.1980
Studium Bachelorstudium Technische Chemie		
Prüfungsfach		
Nummer, Typ und Titel der Lehrveranstaltung 300123 (VU) Einführung in die Chemie		
Semester 2009W	Semesterstunden WS: 2.0 SS: 0.0	ECTS-Credits 3.0
Beurteilung (3) Befriedigend		
Datum 01.12.2009	Prüfer Univ.Prof. Dr.rer.soc.oec. Maria MUSTERFRAU	

Prüfungsfach: Bezeichnung des Diplom-, Vor- oder Abschlussprüfungsfaches oder Rigorosenfaches, dem die Lehrveranstaltung laut Studienplan zuzuordnen ist. Die Angabe kann entfallen, wenn der Erfolg der Teilnahme an einer Lehrveranstaltung beurteilt wird. Bei Kolloquien ist "Kolloquium" einzutragen.

Beurteilung: Sehr gut (1), gut (2), befriedigend (3), genügend (4), nicht genügend (5)
 Mit Erfolg teilgenommen, ohne Erfolg teilgenommen (bei Praktika)

Dieses Zeugnis wurde maschinell erstellt und ist ohne Unterschrift und Siegel gültig.

Dieses Zeugnis kann über den unten angegebenen Link bzw. über den rechts aufgedruckten QR-Barcode (codierter Link) validiert werden.

<https://tiss.tuwien.ac.at/sss/ez/>



Abbildung 1:

Musterexemplar eines Einzelzeugnisses für den Selbstausdruck

Man kann daher sagen, dass schon alleine die enorm hohe Anzahl von möglichen Codes das System bereits sehr sicher macht. Zusätzlich wird aber natürlich auch verhindert, dass jemand überhaupt in die Lage kommt, viele verschiedene Codes auszuprobieren. Dazu wird ein Mechanismus implementiert, der ab einer gewissen Anzahl von abgefragten ungültigen Codes den Zugang für die IP-Adresse des Angreifers für eine gewisse Zeit sperrt.

Da man aber auch die Möglichkeit in Betracht ziehen muss, dass ein Zeugnis auf Grund unglücklicher Umstände in falsche Hände gerät und das Originaldokument durch Veröffentlichung des Codes von jeder beliebigen Person abgerufen werden könnte, wurden zusätzliche Sicherheitsvorkehrungen getroffen, um unbefugte Zugriffe zu verhindern. Die Anzahl der tatsächlich erfolgten Aufrufe – und damit ein Indikator für einen möglichen Missbrauch – ist für den Studierenden jederzeit ersichtlich. Der Student hat unabhängig von der Anzahl der Zugriffe die Möglichkeit, die Online-Validierung eines Dokuments über die URL gänzlich zu deaktivieren und auch wieder zu aktivieren. Weiters kann bei Bedarf ein neuer Hashcode generiert werden, wodurch das ursprüngliche Dokument zwar weiterhin gespeichert, aber von außen nicht mehr zugänglich ist. Zu bedenken ist dabei aber, dass jeder Studierende insbesondere bei einer Bestätigung des Studienerfolgs für eine öffentliche Behörde wie das Finanzamt sicherstellen sollte, dass eine Online-Validierung für den in Frage kommenden Zeitraum möglich ist.

Der 25-stellige Code ist für die Eingabe in die Adressleiste eines Browsers allerdings ziemlich umständlich. Aus diesem Grund wird auf jedem Dokument zusätzlich zu der URL auch ein zweidimensionaler Barcode angezeigt, der die URL codiert. Der Barcode richtet sich nach dem QR-Code Standard (QR steht für *quick response*, schnelle Antwort) aus dem Jahre 1994. Für die Auswertung des Codes gibt es mittlerweile sehr viel Software, sowohl für Mobilfunkgeräte mit integrierter Kamera als auch für PCs und Notebooks mit Web-Cams. Ein einfacher Klick am Handy oder PDA kann damit ausreichen, um für eine Überprüfung der Daten das Originaldokument vom TISS-Server abzurufen.

Noch im Sommersemester 2009 sollen neben den Einzel- und Sammelzeugnissen sämtliche Bestätigungen, wie das Studienblatt, die FLAG-, die Studienerfolgs-, die Studienzeit-, die Studien- und die Fremdenstudien-Bestätigung online über TISS zum Selbstaussdruck für Studierende zur Verfügung stehen.

Ausblick

In den kommenden Monaten werden schrittweise weitere Teile von TISS sichtbar werden, wobei vor allem Fachabteilungen der TU Wien von neuen Systemen, Services und integrierten Lösungen profitieren werden. Iterative Entwicklung von Prototypen unter regelmäßiger Abstimmung und Prüfung durch die betreffenden Mitarbeiter werden zur Ergänzung und Erweiterung des Fachkonzepts und vor allem auch zu maßgeschneiderten Lösungen führen. Der Schwerpunkt wird dabei auf der Ablöse von Altsystemen liegen, aber gleichzeitig werden auch weiterhin kleinere, neue Teilsysteme entwickelt, die als moderne Hilfsmittel zur Entlastung der Mitarbeiter beitragen werden.

Aber auch für Studierende werden schon bald weitere Services in TISS aufgehen. Mit der Integration der Diplomarbeitbörse, die bisher vom TU Career Center gehostet wurde, erhalten Studierende weiterhin einen schnellen Überblick über angebotene Diplomarbeiten. Von der Überarbeitung, Neugestaltung und schrittweisen Erweiterung der bisherigen Funktionen werden nicht zuletzt auch Mitarbeiter profitieren.

In der kommenden Ausgabe der ZIDline wird TISS wieder über aktuelle Entwicklungen und Ergebnisse berichten. Bis dahin werden auch Zwischenberichte über den Projektfortschritt für Informationen aus erster Hand sorgen.

Für Feedback, Anregungen oder Verbesserungsvorschläge steht das TISS-Team natürlich weiterhin per E-Mail an feedback@tiss.tuwien.ac.at oder über das Kontaktformular (http://www.zid.tuwien.ac.at/ueber_tiss/kontakt/) zur Verfügung.

Geoblocking des MS XP Professional Produktschlüssels

Martin Holzinger

Mit Anfang Juni 2009 wird die WGA-Gültigkeitsprüfung für Rechner mit IP-Adressen, die seitens Microsoft als nicht aus Österreich stammend klassifiziert werden, fehlschlagen. Für den Betrieb von Rechnern mit der Campus- bzw. der Studentenversion von Windows XP innerhalb Österreichs (bzw. speziell innerhalb des TUNET) ergeben sich daraus keine Konsequenzen.

Vorgeschichte

Seit der erstmaligen Bereitstellung von MS Windows XP Professional im Oktober 2001 an der TU Wien sind nun fast 8 Jahre vergangen und mittlerweile wurde bereits das dritte Service Pack ausgerollt. Das Betriebssystem erfreut sich noch immer großer Beliebtheit, ca. 80% aller am Campus laufenden Microsoft-Systeme werden mit XP betrieben.

Im Unterschied zu den im Handel erhältlichen Retail-Versionen erhalten Unternehmen mit entsprechenden Lizenzverträgen so genannte Volumen-Lizenzschlüssel (*Volume Licensing Keys*, VLKs). Solche Schlüssel eignen sich unbegrenzt zur Aktivierung mittels zugehöriger Installationsmedien aufgesetzter Betriebssysteme und sollten daher entsprechend vertraulich behandelt werden. Nach eingehenden Untersuchungen hinsichtlich technischer Machbarkeit wurde der VLK seinerzeit so versteckt wie möglich in eine so genannte unbeaufsichtigte Installation (*unattended installation*) eingearbeitet, sodass dieser beim Installationsprozess nicht abgefragt wird.

Ein Key geht um die Welt ...

Mittlerweile existieren jedoch etliche Tools, die bequem per grafischer Oberfläche ein Auslesen solcher Schlüssel aus einer Distribution ermöglichen. Im Übrigen ist die Anwendbarkeit dieser Programme weder auf Keys von Windows XP noch auf Microsoft-Produkte allein beschränkt, sodass eine (illegale) Weiterverbreitung von Produktschlüsseln im Normalfall nur eine Frage der Zeit darstellt.

Speziell liefert eine gezielte Internet-Suche nach dem der TU Wien zuordenbaren XP-VLK an die 150 Webseiten mehr oder weniger konstruktiven Charakters, die von einfachem Anführen / Posten des Strings bis hin zur Download-

Möglichkeit ganzer Distributionen über Filesharing-Tools reichen. Da der VLK – aus welchen Gründen auch immer – nicht an eine spezielle Sprachversion gebunden ist, scheint er sich laut Microsoft auch im Reich der Mitte einer zunehmend größeren Beliebtheit zu erfreuen.

... und wie wir und Microsoft darauf reagieren

Wir haben daher mit Microsoft die Implementierung eines so genannten „Geoblockings“ vereinbart. Dieser Mechanismus soll mit Anfang Juni 2009 aktiv werden.

Betroffen von der Maßnahme werden alle jene Rechner sein, die mit einer IP-Adresse „außerhalb Österreichs“ durch die manuelle Update-Funktion (Windows Update oder Microsoft Update) oder WGA-Prüfung (manuell oder nach Erstinstallation) auf die Validierungsserver von Microsoft zugreifen. In diesem Fall ist mit einer Meldung zu rechnen, es handle sich möglicherweise um eine nicht legale Windows-Version, vgl.

http://de.wikipedia.org/wiki/Windows_Genuine_Advantage

Die „Funktionalität“ des Betriebssystems selbst bleibt davon unbeeinträchtigt. Auch ist eine solche Meldung in dem Sinne nicht persistent, als dass ein Rechner durch Verwendung einer „gültigen“ IP-Adresse (etwa durch VPN-Zugang) eine dann durchzuführende Gültigkeitsprüfung wieder besteht. Solche Fälle sind etwa für zu Tagungszwecken ins Ausland verbrachte Notebooks denkbar.

Für im Sinne des Punktes 8) der Allgemeinen Lizenzbedingungen – vgl. http://www.zid.tuwien.ac.at/fileadmin/files_sts/pdf/Lizenzbedingungen.pdf – begründbare Ausnahmefälle besteht zudem nach Rücksprache die Möglichkeit eines Austauschs des geblockten Keys.

Für weitere Informationen oder Fragen steht Ihnen das Service Center des ZID unter der Nummer 42002 bzw. unter office@zid.tuwien.ac.at gerne zur Verfügung.

Automatische Mailboxen und eindeutige generische E-Mail-Adressen

Georg Gollmann, Johann Klasek, Fritz Mayer

Für alle Personen im Personalstand der TU Wien stellt der ZID eine Mailbox für die TU-interne dienstliche Erreichbarkeit zur Verfügung.

Vorgeschichte

Bisher nahmen nicht alle Mitarbeiterinnen und Mitarbeiter der TU Wien die E-Mail-Dienste des ZID oder institutseigener Mailserver in Anspruch. Auch die Zuordnung der generischen Adresse zu einer Zustelladresse war nicht immer gegeben. Etwa ein Viertel des Personals der TU Wien hatte keine Zustelladresse und war daher nicht über eine generische E-Mail-Adresse erreichbar.

Durch die Einführung des SAP Moduls ESS – Employee Self Service – für das Reisemanagement (weitere Applikationen wie Urlaubs- und Krankenstandmeldung sollen folgen) wurde es notwendig, dass alle Mitarbeiterinnen und Mitarbeiter hausintern per E-Mail verständigt werden können.

Automatische Mailboxen

Im April 2009 wurde für alle Mitarbeiterinnen und Mitarbeiter im Personalstand der TU Wien, die keine E-Mail Zustelladresse hatten, vom ZID eine Mailbox vorbereitet.

Seither erhalten auch alle neu im Personalstand aufgenommenen Personen automatisch eine Mailbox vom ZID, sofern sie im Adressbuch [1] nicht schon eine Zustelladresse eingetragen haben. Insbesondere haben Tutoren meist schon eine Mailbox über ihren Studenten-Account.

Diese Mailbox muss durch Setzen eines Passwortes aktiviert werden [2]. Da dafür das TU-Passwort [3] benötigt wird, werden die Adressmanager des jeweiligen Institutes bei Bedarf per E-Mail gebeten, dem neuen Mitarbeiter ein TU-Passwort anzulegen.

Die Mailbox ist – zur Vermeidung von SPAM – vorerst nur innerhalb der TU Wien erreichbar. Über „E-Mail Einstellungen“ [4] im Adressbucheintrag kann diese jederzeit in eine weltweit erreichbare Mailbox umgewandelt werden. Dies geschieht, indem man die Spalte „SPAM-Level ignorieren“ für die entsprechende Zustelladresse leer lässt oder einen entsprechenden Wert > 0 (mindestens 6 empfohlen) einträgt.

Der Account für die Mailbox wird im Account Management System geführt [5] und ist bis 2 Monate nach dem Ausscheiden aus dem Personalstand gültig.

Mail Alias, generische E-Mail-Adressen

Für alle Mitarbeiterinnen und Mitarbeiter der TU Wien sind eindeutige generische E-Mail-Adressen der Form

Vorname.[Mittelteil.]Nachname@tuwien.ac.at

eingrichtet. Derartige E-Mail-Adressen [6] gibt es schon seit einiger Zeit für Studierende und Alumni (@student.tuwien.ac.at bzw. @alumni.tuwien.ac.at). Während die Adresse für Mitarbeiter automatisch vergeben wird, ist sie für Studenten und Alumni wie bisher optional.

Bei Namensgleichheit wird als Mittelteil standardmäßig der zweite Vorname oder das Kurzzeichen der Organisationseinheit eingetragen. Über „Mail Alias“ [7] im Authentifizierungsportal [8] kann der Mittelteil geändert bzw. hinzugefügt werden. Der Mittelteil ist für alle Rollen einer Person – Mitarbeiter, Student, Alumni – einheitlich.

Die bisherigen generischen E-Mail-Adressen der Form Vorname.[Vorname2.]Nachname+Abteilung@tuwien.ac.at für Personen im Personalstand vor der Einführung der automatischen Mailboxen bleiben weiterhin bestehen.

Anders als bei diesen Adressen ändert sich die neue generische E-Mail-Adresse bei einem Namenswechsel, etwa durch Verheiratung, nicht automatisch, damit publizierte Mail-Adressen weiterhin gültig bleiben. Jedoch kann im Fall eines Namenswechsels über „Mail Alias“ [7] im Authentifizierungsportal die Änderung in die generische E-Mail-Adresse übernommen werden.

Generische Adressen bleiben bis ein Jahr nach dem Ausscheiden aus dem Personalstand gültig und werden danach 6 Monate gesperrt, bevor sie an eine andere Person vergeben werden. Alumni Aliase werden gelöscht, wenn keine Zustelladresse mehr vorhanden ist, Studenten- und Mitarbeiter-Aliase nach dem Ausscheiden.

Als Zustelladresse für die generische Adresse von Mitarbeitern wird vorzugsweise die bei der Zustellorganisation im Adressbuch eingetragene Adresse genommen. Fehlt diese, wird auf allfällige bei anderen Instituten eingetragene Zustelladressen zurückgegriffen. Gibt es auch die nicht, wird nach einem gültigen Mail-Account am ZID gesucht, etwa die oben beschriebene automatisch eingerichtete Mailbox. Sollte auch die fehlen, wäre, so vorhanden, die Studenten-Mailadresse die letzte Option.

Für Studenten- und Alumni-Aliase wird wie bisher die im Adressbuch bei der Studentenrolle eingetragene Zustelladresse herangezogen.

Abruf und Versenden von E-Mails

Allen automatisch eingerichteten Mailboxen wird eine Zustelladresse der Form *username@mail.tuwien.ac.at* zugeordnet. *username* wird nach einem bestimmten Algorithmus aus Vor- und Nachname generiert und ist zugleich Benutzername für den E-Mail-Abruf. Der Abruf kann wahlweise über das POP3- oder IMAP-Protokoll erfolgen, muss aber verschlüsselt (SSL/TLS) sein. Als Posteingangs-Server als auch als Postausgangs-Server (SMTP) ist „mail.zserv.tuwien.ac.at“ anzugeben. Die SMTP-Funktion

steht auch von außerhalb des TUNET zur Verfügung, muss dann aber ebenfalls über Authentifizierung mit Benutzernamen, Verschlüsselung (TLS) und Port 587 erfolgen. Für den Fall, dass kein eigener E-Mail-Client verwendet werden kann, wird auch ein Webmail-Interface [9] angeboten. Jedem Mail-Account stehen 2 GB an Speicherplatz zur Verfügung [10].

Die Einrichtung von Weiter- und Umleitungen, Filtern und Abwesenheitsnotizen kann ebenfalls über ein Web-Interface vorgenommen werden [11].

Wichtige Links

- [1] TU Adressbuch:
<http://tiss.tuwien.ac.at/adressbuch/adressbuch/>
- [2] Passwort-Änderung:
<https://www.zid.tuwien.ac.at/passwort/>
- [3] TU-Passwort: http://www.zid.tuwien.ac.at/tu_passwort/
- [4] E-Mail Optionen für Mailboxen:
<https://iu.zid.tuwien.ac.at/ZID-DB.mailOptions>
- [5] Online Account Management:
<http://www.zid.tuwien.ac.at/zidaccounts/>
- [6] Mail-Adressierung: http://www.zid.tuwien.ac.at/kom/services/mail/konzept/mail_adressierung/
- [7] Mail Alias, generische E-Mail-Adresse ändern:
<https://iu.zid.tuwien.ac.at/ZID-DB.mailAlias>
- [8] Authentifizierungsportal:
<https://iu.zid.tuwien.ac.at/AuthServ.portal>
- [9] Webmail: <https://webmail.tuwien.ac.at/>
- [10] Mailbox-Service des ZID:
<http://www.zid.tuwien.ac.at/zserv/mail/>
- [11] Mail-Filter und Auto Reply:
<https://mail.tuwien.ac.at/filter/>

Neu als Campussoftware:

Bricscad

Bricscad – auf IntelliCAD basierend – ist eine 2D und 3D CAD Software, die das DWG Format liest und schreibt und somit die Kompatibilität zu AutoCAD bietet.

SolidWorks

3D-CAD Software für den Maschinenbau

Zwei Konstruktionsanalysewerkzeuge werden mit dieser Software angeboten:

COSMOSWorks – FEA: Finite-Elemente-Analyse

COSMOSFloWorks – CFD: numerische Strömungsmechanik (CFD) und thermische Analyse

www.zid.tuwien.ac.at/sts/arbeitsplatz_software/

Externer Zugang zu den Lizenzservern

Andreas Klauda

Durch die immer größer werdende Verbreitung mobiler Geräte und die Möglichkeit, das Internet auch unterwegs zu nutzen, ist auch der Wunsch nach einer Lösung entstanden, Software, welche einen Lizenzserver benötigt, auch außerhalb des TUNET zu verwenden.

Die angestrebte Lösung sollte ohne VPN oder zusätzliche Software auskommen, daher wurde eine web-basierte Möglichkeit geschaffen, um den Zugang zum Lizenzserver auch außerhalb des TUNET zu ermöglichen. Diese sieht wie folgt aus:

Die beiden Lizenzserver `acadls.tuwien.ac.at` und `acadls2.tuwien.ac.at` können für beliebige IP-Adressen für einen gewissen Zeitraum (im Augenblick sind es 480 Minuten) frei geschaltet werden.

Dazu – sobald man mit der gewünschten IP-Adresse online ist – folgende Webseite aufrufen <https://iu.zid.tuwien.ac.at/Products.licenceActivation> und mit TU-Usernamen und Passwort authentifizieren.

Nach der Authentifizierung wird die IP-Adresse frei geschaltet, man erhält dann folgende Meldung:

Voraussetzung ist, dass die entsprechende Software (welche einen Lizenzserver verwendet) auch auf den eigenen Namen registriert ist.

Danach sind die beiden Lizenzserver temporär frei geschaltet und die Software kann verwendet werden.

Alternativ dazu kann man auch weiterhin eine VPN-Verbindung verwenden, hier ist dann keine manuelle Freischaltung notwendig, aber auch dazu sind gewisse Voraussetzungen notwendig:

- Die Software, die verwendet wird, muss auf den eigenen Namen lizenziert sein.
- Der TU VPN-Zugang muss auf denselben Namen registriert sein (fixe IP-Adresse).
- Im TU-WLAN muss WLANIPSEC verwendet werden, welches ebenfalls auf denselben Namen registriert sein muss (fixe IP-Adresse).

Dieser Lizenzserver-Zugang ist für folgende Campussoftware-Produkte realisiert:

Acronis True Image Workstation 9.1
AMOS
Archdesktop, Mechdesktop
Autocad
Autocad Inventor
Autocad Map
LabView
Mathcad
Origin Pro
QuarkXpress
Scientific WorkPlace
Solidworks
SPSS

Windows Server 2008 – nicht nur Verbesserungen

Rudolf Sedlaczek

Dieser Artikel soll und kann keinen vollständigen Überblick über alle Neuigkeiten und Änderungen in Windows Server 2008 geben (dazu gibt es zu viele), sondern einige grundlegende Themen beleuchten und TU-spezifische Informationen vermitteln.

Windows Server 2008 kommt mit weniger verschiedenen Distributionen als frühere Server-Versionen. An der TU sind die Bits als DVD-Images für 32 Bit x86, 64 Bit x64 und IA64 Itanium verfügbar, alle auf Englisch und Deutsch.

Die Auswahl der gewünschten Server-Variante, ob Standard, Enterprise oder Datacenter, erfolgt erst bei der Installation. Dabei wird auch gefragt, ob man eine volle Installation (mit GUI) oder nur den Server Core (ohne GUI) installieren will. Der Server Core ist eine neue Installationsvariante und braucht weniger Plattenplatz, kann aber lokal nur mit Shell-Kommandos administriert werden und erinnert damit sehr an frühere UNIX-Systeme ohne grafische Oberfläche.

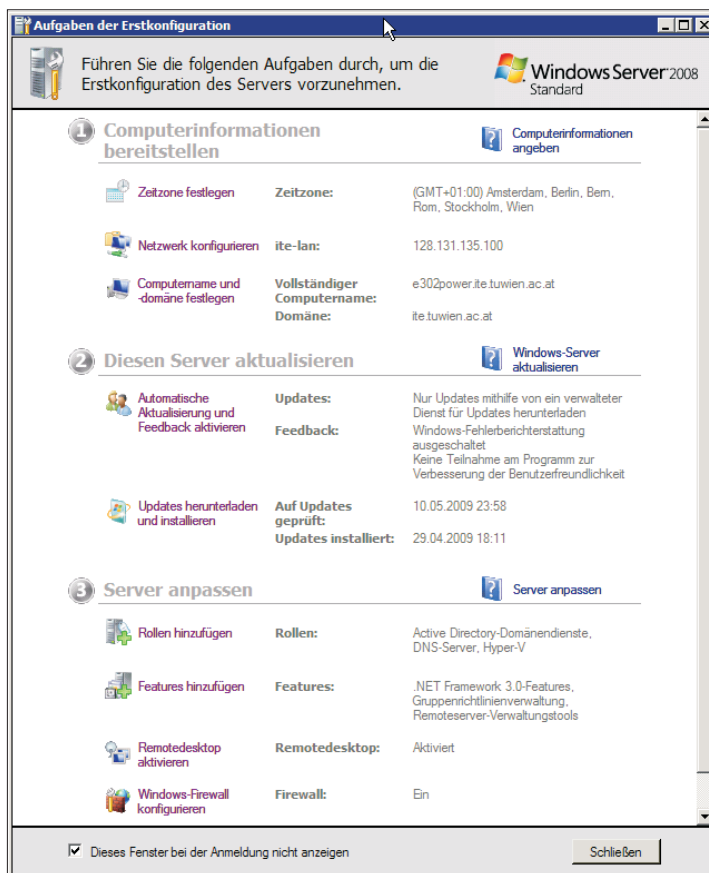
Nur am Anfang der Installation sind diese und wenige andere Einstellungen festzulegen, dann läuft die Prozedur ohne weitere Intervention ab. Das ist ein Vorteil gegenüber früheren Server-Versionen, wo auch während der Installation Fragen beantwortet werden mussten.

Aktivierung

Nach Installation muss der Server innerhalb von 60 Tagen über den Aktivierungs-Server der TU Wien aktiviert werden, sonst läuft das System nur mehr mit eingeschränkter Funktionalität weiter. Jede Aktivierung ist zeitlich beschränkt und gilt maximal 180 Tage. Die Aktivierung erfolgt über ein Script, das den Installationsmedien hinzugefügt wurde. Nach der Installation steht der Befehl „TU-Aktivierung“ am Desktop zur Verfügung. Im Gegensatz zur Aktivierung von Windows Vista muss der Systemadministrator nur eine einmalige Aktion zur permanenten Aktivierung des Servers durchführen. Durch das Ausführen des Aktivierungs-Scripts wird der Server in regelmäßigen Abständen automatisch reaktiviert.

Voraussetzungen für erstmalige Aktivierung und Verlängerung:

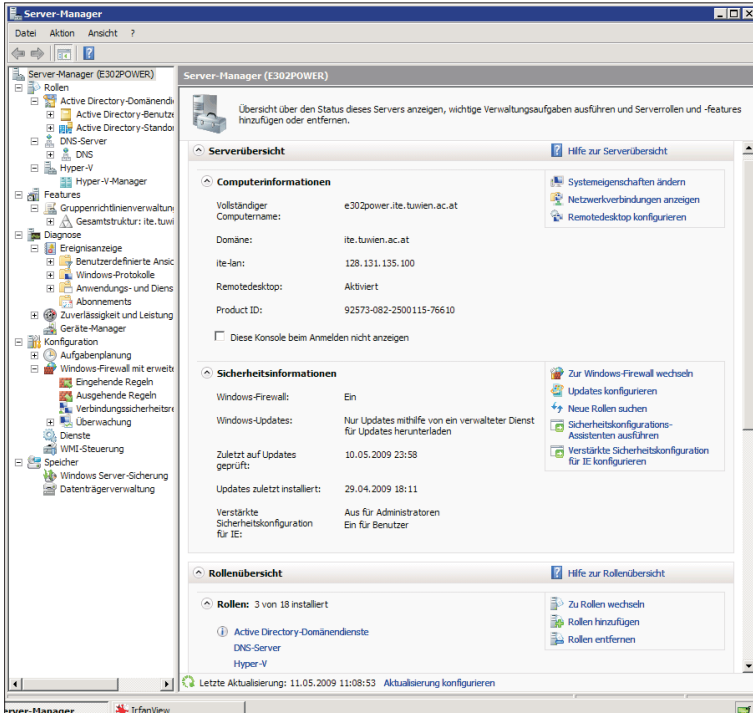
- Internetzugang des Rechners, ggf. Instituts-Firewall für Port TCP 1688 ausgehend öffnen.
- Rechner muss als Server angemeldet sein und über einen DNS-Eintrag verfügen.



Der *Erste Schritte Assistent* führt durch die Grundkonfiguration

Assistenten

Eine wesentliche Vereinfachung und bessere Übersicht bringen neue Assistenten und das Verwaltungsprogramm Server Manager. Der Server Manager ist eine erweiterte Microsoft Management Console (MMC), die es ermöglicht, praktisch alle Informationen über den Server zu erhalten und alle Werkzeuge zum Verwalten unter einer Anwendung anbietet. Mit den Rollen- und Features-Assistenten können alle zur Verfügung stehenden Funktionen installiert werden.



Server Manager

Backup

Die neue Server-Version hat aber nicht nur Erweiterungen erfahren, sondern auch Funktionseinschränkungen. So ist kein Backup mit ntbacup mehr möglich, die neue Server-Sicherung unterstützt keine Sicherung auf Bänder, nur auf Festplatten und optische Laufwerke (CD, DVD). Es arbeitet nicht mehr dateibasierend, sondern erzeugt mittels Snapshot-Verfahren Sicherungen in Form von VHD-Dateien. Während das für die Sicherung von Servern gravierende Vorteile bietet (eine ähnliche Sicherung ist ja zum Beispiel in Windows Vista schon integriert), ist für Exchange-Server die Sicherung komplizierter geworden. Windows Server Backup unterstützt keine Online-Sicherung von Exchange-Datenbanken mehr. Es kann alte Sicherungsdateien lesen und von diesen auch Daten wieder herstellen – es kann jedoch nicht neue Sicherungen nach dem alten Verfahren erzeugen.

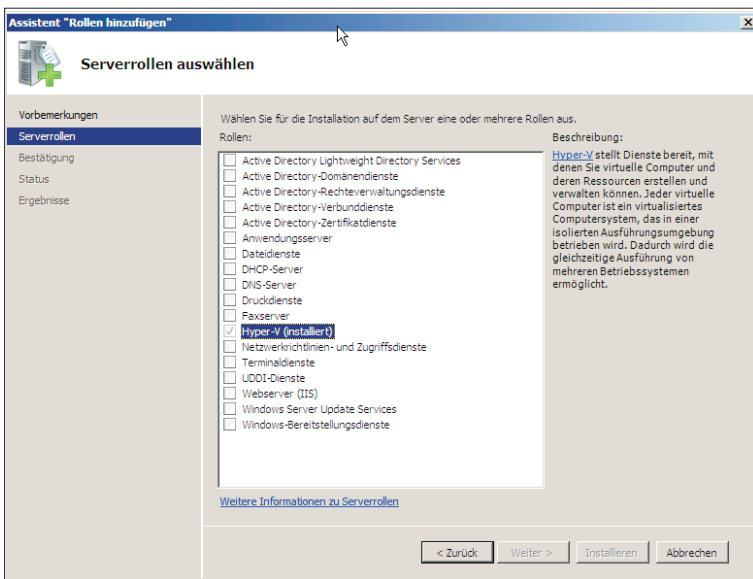
Man kann allerdings eine verkrüppelte Version von ntbacup herunterladen, mit der man aber die Daten von alten Bändern nur lesen kann. Dass Microsoft ein lange funktionierendes einfaches Programm aktiv unbrauchbar macht und damit vorhandene Bandlaufwerke und Backup-Prozeduren unbenutzbar macht, hat viele Anwender verärgert. Es mag stimmen, dass ntbacup für große Datenmengen kein wirklich professionelles Werkzeug war, da die notwendigen Verwaltungsfunktionen gefehlt haben. Für kleinere Server und zum Sichern des Exchange-Datenspeichers war es allerdings ausreichend.

Welche Alternativen gibt es nun, um weiter seine Exchange-Daten sichern zu können oder vorhandene Bandlaufwerke weiter verwenden zu können? Zunächst einmal Third Party Software: Symantec Backup Exec funktioniert einwandfrei, schnell, ist komfortabel einzurichten und ist als Campus Software erhältlich (das angebotene Bundle ist allerdings nicht gerade billig).

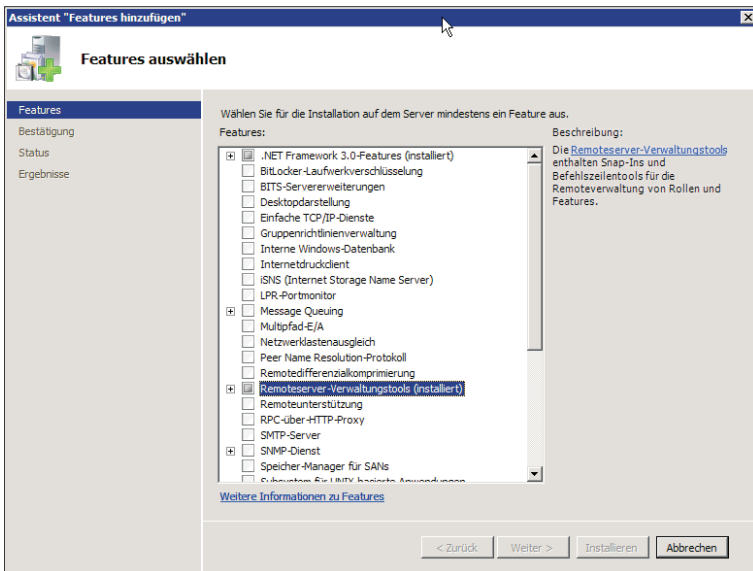
Ein nicht unterstützter, aber funktionierender Work-around ist die Verwendung von ntbacup von Windows 2003: Dazu müssen die Dateien ntbacup.exe, ntmapi.dll und vssapi.dll von einem Windows 2003 System in einen Ordner am Windows 2008 kopiert werden, dann funktioniert zumindest das Exchange Backup wieder so wie unter Windows 2003.

Was bietet Microsoft selber an, um Exchange-, Sharepoint- und SQL-Datenbanken online zu sichern?

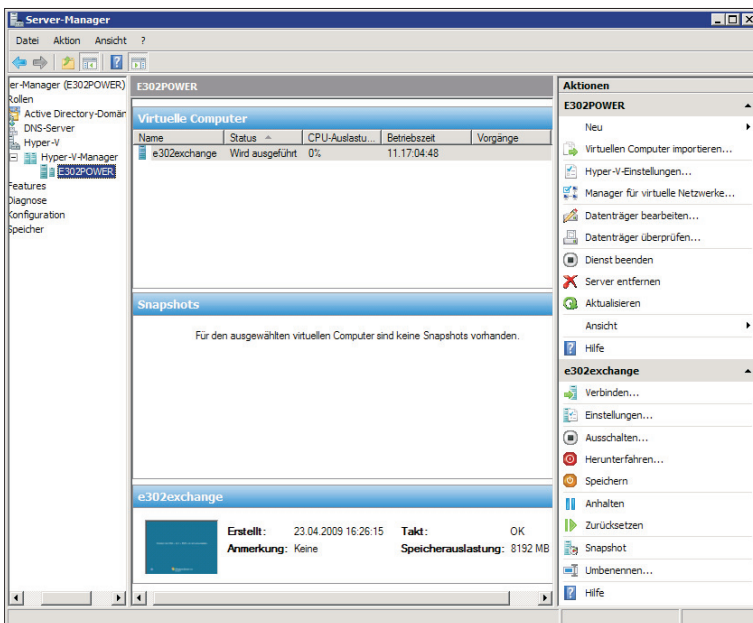
Den Microsoft System Center **Data Protection Manager 2007 (DPM)**, der die erforderlichen VSS-Writer (Volume Shadow Copy Service, Volumenschattenkopie-Dienst) für Exchange 2007 unterstützt. Damit können Sicherungen auf Disks und Bandlaufwerke durchgeführt werden. Der DPM wird als eigenes Campus-Software Produkt an der TU zur Verfügung stehen.



Rollen-Assistent



Features-Assistent



Hyper-V

Allerdings kann man den DPM nicht so einfach als Anwendung auf einem Applikations- oder Exchange-Server installieren wie Symantec Backup Exec. DPM muss ein eigener dedizierter single-purpose Server sein, der keinerlei andere Rollen oder Funktionen ausführen darf!

Dabei drängt sich gleich die Frage auf: Noch eine weitere Server-Kiste? Es ist ja schon so, dass ein Domain-Controller nicht auch ein Exchange-Server sein darf, wenn die Konfiguration von Microsoft unterstützt werden soll.

Virtualisierung

Um die erforderliche Flut an einzelnen Boxen einzudämmen, bleibt nur die Virtualisierung der Server. Schon seit Jahren war dies unter VMware möglich, allerdings weigerte sich Microsoft dann oft, Probleme auf virtuali-

sierten Servern näher zu untersuchen, mit dem Hinweis, dass der Server oder die Applikation unter VMware nicht voll unterstützt wären. Man möge doch die ganze Konfiguration auf einzelnen physischen Geräten installieren und sehen, ob der Fehler da auch auftritt! Welch weltfremdes Ansinnen von Microsoft! Zur Ehrenrettung von Microsoft muss allerdings eingestanden werden, dass einige aufgetretene Probleme wirklich erst durch die Virtualisierung entstanden sind, entweder durch Bugs in der VMware oder durch fehlerhafte Verwendung der virtuellen Instanzen (z. B. dieselbe Instanz gleichzeitig auf zwei Hosts laufen zu lassen, führt zu seltsamen Effekten...)

Mitte 2008 wurde schließlich Microsofts Virtualisierungslösung freigegeben: **Hyper-V**

Damit können wie unter VMware Windows und Linux Server mit 32 und 64 Bit parallel betrieben werden, wobei auch virtuelle Multiprozessorsysteme möglich sind. Hyper-V ist nur unter der x64 Version von Windows Server 2008 verfügbar und benötigt Hardware, die die Virtualisierung unterstützt (Intel VT bzw. AMD-V) und Hardware Data Execution Protection (DEP) ermöglicht. Das Snapshot-Feature erlaubt, den Status einer laufenden virtuellen Maschine zu sichern.

Da die Fähigkeiten von Hyper-V noch nicht an die von VMware heranreichen, bringt Microsoft einige Lizenzierungszuckerln, die VMware natürlich nicht bieten kann: Bei jedem Standard Server ist eine zusätzliche virtuelle Windows-Server-Instanz kostenlos inkludiert, beim Enterprise Server sind es vier Instanzen. Sind diese Instanzen ebenfalls Windows 2008 Server, müssen sie natürlich ebenfalls aktiviert werden und erfordern deshalb auch einen DNS-Eintrag und eine spezielle Server-Lizenz bei der Server-Software Anmeldung: „Windows 2008 Server virtuelle Hyper-V Instanz“.

Ein Argument für die Verwendung von Hyper-V ist auch der jetzt gewährleistete Support durch Microsoft für virtualisierte Anwendungen wie Exchange oder SQL.

Zusammenfassung

Wer wirklich alles wissen will, was sich mit Windows Server 2008 geändert hat, sei auf das 340 Seiten starke Dokument: „Changes in Functionality from Windows Server 2003 with SP1 to Windows Server 2008“, verwiesen, downloadbar unter:

www.microsoft.com/downloads/details.aspx?FamilyID=173e6e9b-4d3e-4fd4-a2cf-73684fa46b60&DisplayLang=en

Zusammenfassend kann man aber doch sagen, dass Windows Server 2008 ein stabiles und leistungsfähiges Betriebssystem geworden ist, das man schon uneingeschränkt für den Produktionsbetrieb empfehlen kann, wenn man sich mit der Backup-Problematik auseinandersetzt.

Feuerwände für das TUNET

Ein Service für die Computersicherheit

Fritz Schrogl

Mit zunehmender Bedeutung des Internets für unser alltägliches Leben steigt auch die Professionalität der Cyberkriminellen. Dieser Professionalisierung sollte man als verantwortungsvoller Benutzer nicht tatenlos zusehen, sondern entsprechende Schutzmaßnahmen ergreifen. Der ZID steht einem hierfür tatkräftig zur Seite.

Einleitung

Wer die Security-Meldungen der einschlägigen IT-Webseiten verfolgt wird schnell feststellen: Die Zeit der sogenannten Skriptkiddies ist vorbei. Die Cyberkriminellen von heute werden immer professioneller und organisieren sich immer besser. Einer der Gründe für diesen Wandel liegt vor allem in der zunehmenden kommerziellen Nutzung des Internets, wodurch immer größere Summen durch Cyberkriminalität lukriert werden können.

Ein Thema in diesem Kontext sind so genannte Bot-Netzwerke und die durch sie möglichen Denial-of-Service-Angriffe. Bei Bot-Netzwerken handelt es sich um einen losen Verbund von Rechnern, die mit entsprechender Schadsoftware infiziert wurden und anschließend unter der Kontrolle eines Command-and-Control-Servers stehen. Durch den C&C-Server können nun alle Rechner eines Bot-Netzwerkes angewiesen werden, zeitgleich wiederholte Male auf eine Webseite zuzugreifen. Durch diese schiere Masse an Anfragen kann die angegriffene Webseite zusammenbrechen und im Internet nicht mehr erreichbar sein. Da dies einen großen Geschäftsentgang für die Betreiber angegriffener Webseiten bedeuten kann, sind diese oftmals bereit, „Lösegeld“ an Cyberkriminelle zu zahlen, um von derartigen Angriffen verschont zu bleiben.

Was hat das alles mit mir zu tun?

Durch die Verbreitung von Breitband-Internet-Zugängen sind viele Computer 24 Stunden täglich mit dem Internet verbunden und verfügen zusätzlich über eine sehr leistungsfähige Anbindung an das weltweite Datennetz – dies

gilt insbesondere auch für die Rechner innerhalb eines Universitätsnetzwerks. Beides sind Merkmale, die einen Rechner sehr interessant für die Verwendung innerhalb eines Bot-Netzwerkes machen, und deshalb sollten die Besitzer derartiger Rechner auch entsprechende Schutzmaßnahmen treffen, um nicht unwissend „Mittäter“ bei den genannten Erpressungsversuchen zu werden.

Habe ich nicht schon eine Firewall auf meinem Rechner?

Oftmals sind Computernutzer der Meinung, dass ihre Rechner schon mit einer Firewall geschützt sind, da viele aktuelle Antiviren-Programme bereits eine derartige Funktionalität anbieten bzw. Windows ab XP Service Pack 2 bereits eine Firewall integriert hat. Dies ist prinzipiell richtig, nur kann eine Software-Firewall nicht den gleichen qualitativen Schutz bieten wie eine dedizierte Hardware-Lösung, da deren Konfiguration von Schadprogrammen nicht verändert werden kann. Somit bieten die vom ZID angebotenen Firewall-Lösungen einen Mehrwert gegenüber den reinen Software-Firewall-Lösungen am lokalen Computer.

Die Ausgangssituation an der TU

Ohne Zutun des Benutzers ist jeder Rechner innerhalb des TUNET durch den Grundschatz rudimentär gesichert. Beim TU-Grundschatz werden bestimmte „well known“-Ports gesperrt. Eine Liste der betroffenen Ports kann nachfolgender Tabelle entnommen werden:

Port	Protokoll	Port	Protokoll
-	Ping	177	xdmcp
7	echo	445	Microsoft-DS
9	discard	512	rexec
25	SMTP	513	rlogin
53	DNS	514	R-Kommandos / Syslog
67	bootps	515	lpd
68	bootpc	540	UUCP
69	TFTP	1080	Socks
111	Portmapper	1434	SSRS
123	ntpd	1900	SSDP
135	msrpc	2049	NFS
136	Profile Name Service	3128	Squid
137-139	Netbios	4045	lockd
161-162	snmp	5000	UPnP
		6000-6063	X11

Der Grundschutz ist nur als absolute Mindestmaßnahme anzusehen und sollte dringend durch eines der beiden folgenden Services ergänzt werden.

Die einfache Variante für mehr Schutz

Einen wirklichen Zugewinn an Sicherheit erhält man durch den Zugriffsschutz, welcher explizit vom EDV-Beauftragten des Instituts angefordert werden muss. Hier wird die zentrale TU-Firewall so konfiguriert, dass standardmäßig alle eingehenden, aufbauenden Verbindungen aus dem Internet zum Rechner blockiert werden. Obwohl dies sehr drastisch klingt, hat diese Maßnahme keinerlei negative Auswirkungen auf die normalen Surf-Aktivitäten des Benutzers, bringt jedoch ein deutliches Mehr an Sicherheit.

Für Server, die Dienste für das Internet anbieten, müssen die dafür benötigten Ports freigeschaltet werden. Aus administrativen Gründen können nur bestimmte Ports freigeschaltet werden, welche in so genannten Dienstgruppen zusammengefasst werden. Folgende Dienstgruppen werden derzeit angeboten:

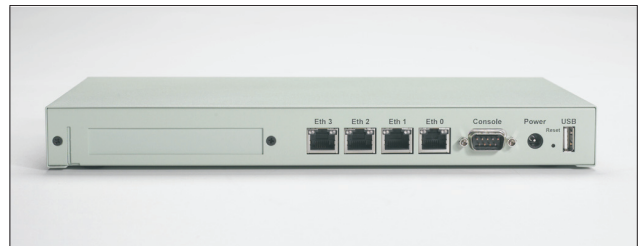
Dienstgruppe	Ports
WWW	HTTP(80) +HTTPS(443)
FTP	FTP(21)
SSH	SSH(22)
POPIMAP	POP3(110), SPOP3(995), IMAP(143), SIMAP(993), MSA(587)
REMOTE	VNC (TCP/5900-5910), pcAnywhere(TCP/5631, UDP/5632)

Die Aktivierung des Zugriffsschutzes kann durch eine formlose Mail an security@tuwien.ac.at und unter Angabe des zu sperrenden Subnetzes angefordert werden.

Die Variante für anspruchsvolle Nutzer

Sind dem Benutzer die Möglichkeiten des Zugriffsschutzes zu unflexibel, so bietet sich eine individuelle Hardware-Firewall-Lösung an, welche von der Abteilung Standardsoftware zur Verfügung gestellt wird. Diese Firewall bietet auch Schutz vor Angriffen innerhalb des TUNET.

Es handelt sich hierbei um ein Embedded-System der Firma Soekris, welches von Walter Selos adaptiert wurde und zwischen dem TUNET und dem Institutsnetzwerk installiert wird. Diese Firewall-Lösung kann vom Administrator ganz individuell konfiguriert werden und bietet somit die größte Flexibilität und Unabhängigkeit für den Benutzer.



Zur Installation dieser Firewall-Lösung muss entsprechende Hardware erworben werden, weshalb zukünftig dafür Kostenersatz geleistet werden muss. Zur Bestellung der Soekris-Firewall reicht ebenfalls eine formlose Mail an security@tuwien.ac.at.

Referenzen

Skriptkiddie: <http://de.wikipedia.org/wiki/Skriptkiddie>
 Botnetzwerke: <http://de.wikipedia.org/wiki/Botnetze>
 ZID IT-Security: <http://www.zid.tuwien.ac.at/sts/security/>
 ZID Firewalls: <http://www.zid.tuwien.ac.at/sts/security/firewall/>
 ZID Portsperrren: http://www.zid.tuwien.ac.at/de/sts/security/firewall/gesperrte_ports/
 ZID Zugriffsschutz: <http://www.zid.tuwien.ac.at/de/sts/security/firewall/zugriffsschutz/>
 Walter Selos: Firewall-Lösung für Institute. ZIDline 13, Dezember 2005: <http://www.zid.tuwien.ac.at/zidline/z113/soekris.html>

Mobiles Gebäudesicherheitsmanagement Ein TISS-Projekt

Philipp Kolmann

Helmut Ecker, Gebäude und Technik

Alfred Kaltenecker, Institut für Rechnergestützte Automation / INSO

An der TU Wien gibt es wie in vielen öffentlichen Gebäuden einen Sicherheitsdienst, der die personelle Basis der so genannten Sicherheitsinfrastruktur bildet. Während ihres Dienstes begeben sich die Mitarbeiter auf Sicherheitsrundgänge durch die Gebäude und leiten sämtliche besonderen Vorkommnisse weiter. Um diese Arbeit zu unterstützen, wurde an der TU Wien ein neues online System, unterstützt durch mobile Geräte und NFC-Technologie, eingeführt (TISS-MGSM), das die erforderlichen Abläufe erleichtert und beschleunigt.

Seit vielen Jahren gibt es an der TU Wien einen Sicherheitsdienst, der der Organisationseinheit Gebäude und Technik (GUT) zugeordnet ist und dessen Aufgabe es unter anderem ist, die Gebäude und deren Einrichtungen in regelmäßigen Rundgängen zu überprüfen und eventuelle Schäden und sämtliche Vorkommnisse weiterzuleiten. Die Rundgänge wurden hier schon länger mit Hilfe spezieller Geräte aufgezeichnet. Für den Sicherheitsmitarbeiter bewirkt dies zum Beispiel, dass der Mitarbeiter in der Portierloge jederzeit weiß, wo sich der Kollege, der seinen Rundgang allein durchführt, befindet. Die TU Wien erhält anhand der Aufzeichnungen die Bestätigung, dass der Rundgang durchgeführt wurde, man kann im Schadensfall belegen, wo sich die Mitarbeiter zu einem bestimmten Zeitpunkt aufgehalten haben oder wie sich ein Schadensfall zugetragen hat.

Geschichte

Rundgangs-Aufzeichnung

Das erste System zur Aufzeichnung der Rundgänge bestand aus tragbaren Uhren mit inkludierten Papierstreifen sowie aus Schlüsseln, die im Gebäude verteilt waren. Wenn der Mitarbeiter des Sicherheitsdienstes auf seinem Rundgang zu einem Schlüssel kam, musste er ihn in die Uhr einführen und drehen. Damit wurde das Schlüssel-symbol und die aktuelle Uhrzeit auf den Papierstreifen geprägt. Dieses System war bis 1994 im Einsatz.

Abgelöst wurde es vom Guard Control System (GCS). Mit Hilfe von Magnetstreifen, die im Gebäude verteilt angebracht wurden, und mit einem mobilen „Sammler“ wurden

Daten aufgezeichnet, über eine Ladestation an einen PC gesendet und dort ausgewertet.

Im Jahr 2001 wurde das Guard Control System durch das Blue Pointer System der Firma cdt ersetzt, welches bereits auf der Basis von so genannten RFID *Tags* arbeitet. Das sind Chipkarten, standardisiert für kontaktlose Kommunikation nach ISO14443A. Dieses System, das sich bis heute in Verwendung befindet, zeichnet sich vor allem durch geringe Anschaffungskosten und hohe Stabilität der Hardware, insbesondere des Datensammlers, aus.

Rundgangs-Auswertung

Während die Papierstreifen des initial verwendeten Aufzeichnungssystems noch händisch ausgewertet werden mussten, ging es beim zuletzt verwendeten System bereits automationsunterstützt ans Werk. Hier war eine Software einer externen Firma auf Basis von MS Access und Visual Basic im Einsatz. Durch diese Kombination war zwar eine automatische Auswertung der Daten möglich, von einem Mehrplattzugriff konnte jedoch noch keine Rede sein. Auch die Auswertungen waren nicht zur vollen Zufriedenheit möglich, da man nur die Anzahl der insgesamt gesannten *Tags* in der Auswertung fand. Welche *Tags* gesannt wurden, war jedoch nicht ersichtlich.

Gewünscht wurde hier ein System, das es ermöglicht, festzulegen, dass bestimmte *Tags* bei jedem Rundgang zu scannen sind (obligatorisch) und andere frei vom Mitarbeiter gewählt werden können. So können flexibel andere Routen frei festgelegt und auch gesetzte Schwerpunkte im System erfasst werden.

Dienstbuch

Ein weiterer Aspekt der Tätigkeiten des Sicherheitsdienstes war das Führen eines Dienstbuches, in dem besondere Meldungen festgehalten wurden. In früheren Jahren war dies ein gebundenes Buch, das vom Bereichskordinator in regelmäßigen Abständen durchgelesen und bearbeitet wurde. Mit Fortschritten in der EDV wurde auch dieses papierene Buch durch eine Software abgelöst.

Im Jahr 2001 wurde eine elektronische Variante des Dienstbuches gestaltet, welche ebenfalls auf MS Access und Visual Basic basierte. Diese Software wurde schließlich auf einem Windows 2003 Server gehostet, für jedes Gebäude gab es eine Instanz. Wollte man sich einen Überblick über die Gebäude machen, musste man sich so viele verschiedene Dienstbücher ansehen. Eine Korrelation von besonderen Vorkommnissen war auf diese Weise schwierig. Eine gewisse Mehrplatzfähigkeit wurde schließlich durch die Verwendung von Remote Desktop erreicht, eine wirklich optimale Lösung war aber auch das nicht.

Ein zusätzliches Problem war, dass Bug-Behebungen oder Änderungen meist recht lange dauerten.

GUT-Tracking

Im Sommer 2008 wurde Philipp Kolmann mit einer Analyse des Ist-Zustandes der EDV-Situation beauftragt. Im Laufe der Analyse zeigte sich, dass das Aufzeichnungssystem des Sicherheitsdienstes einer dringenden Überarbeitung bedarf, um ein modernes System zu schaffen, das einerseits sämtliche technischen Anforderungen erfüllt und andererseits benutzerfreundlich und flexibel in der Anwendung ist.

Inspiziert durch ein ähnliches Projekt an der FH Hagenberg entstand die Idee, eine neue, nicht-proprietäre, web-basierte Lösung auf Basis von NFC-Handys als Prototyp zu entwickeln. Die Forschungsgruppe INSO der TU Wien steuert hier ihr Know-how im Bereich mobiler Systeme, Over-the-air-Lösungen und NFC-Technologien bei. Als mobiler Client für die Rundgänge kam das zum damaligen Zeitpunkt am Markt verfügbare Handy Nokia 6131 NFC zum Einsatz. (Das Nachfolgeprodukt wurde zwar schon im April 2008 vorgestellt, offiziell erwerben konnte man es jedoch erst im April 2009.)

Die primären Ziele des neuen Systems waren eine zeitnahe Übertragung der Vor-Ort-Daten während des Rundgangs und eine einfache Mehrplatzfähigkeit, sowohl für den Sicherheitsdienst als auch für Mitarbeiter der Organisationseinheit Gebäude und Technik. Durch ein Webportal konnten die Anforderungen sehr einfach und rasch realisiert werden.

Mobiler Client

Der mobile Client wurde von Alfred Kaltenecker realisiert. Der Datenaustausch zwischen Server und Client erfolgt über eine Web-Schnittstelle und die Kommunikation

läuft über einen sicheren Kanal, um so die Integrität und die Vertraulichkeit der Daten zu gewährleisten.

Der Client wurde mittels der Java 2 Micro Edition (J2ME) implementiert, eine für mobile Endgeräte optimierte Version der Java Platform 2 Standard Edition (J2SE). Zusätzlich zu den zur Verfügung gestellten Basisklassen (MIDP 2.0, CLDC 1.1) wird für die gewünschte Anforderung ein Mobiltelefon mit *Near Field Communication* (NFC) benötigt.

NFC ist eine Technologie, die es ermöglicht, Daten auf sehr kurze Distanz (max. 10 cm) mit bis zu 424 kbps zu übertragen. Mobiltelefone mit NFC können in 3 verschiedenen Modi verwendet werden. Das Gerät kann passiv, aktiv oder im peer-to-peer (P2P) Modus betrieben werden. Im passiven Modus agiert das Mobiltelefon wie eine kontaktlose Chipkarte, im aktiven Modus können beispielsweise RFID-Tags ausgelesen werden und im P2P Modus tauschen Geräte Daten aus.

Im Fall des mobilen Clients agiert das Mobiltelefon im aktiven Modus und liest die auf den Tags gespeicherten Informationen aus. NFC wird beispielsweise auch von der Mobilkom in Kooperation mit der ÖBB, den Wiener Linien und Selecta Automaten eingesetzt. Ob sich diese Technologie durchsetzen wird, bleibt abzuwarten, die TU Wien zeigt jedoch wieder einmal ihre Vorreiterrolle bei neuen Technologien.

Neben der benötigten Hardware für das Mobiltelefon wird für den Einsatz mit J2ME softwareseitig eine Erweiterung der Basisklassen benötigt. Diese Erweiterung (JSR-257 *Contactless Communication API*) ermöglicht es dem Nutzer, empfangene Daten mittels J2ME auszulesen und zu verarbeiten. Diese Daten werden auf Tags gespeichert und vom entsprechenden Mobiltelefon ausgelesen.

Ein typischer Anwendungsfall sieht so aus, dass der Sicherheitsdienstmitarbeiter das Mobiltelefon an einen Tag hält, das mobile Endgerät die Daten (im Normalfall die Raumnummer) ausliest und an den Server weiterleitet. Darüber hinaus können Texte (Schadensmeldung, Hinweise, ...) zusätzlich zu den am Tag gespeicherten Daten übermittelt werden.



Webportal

Im Webportal werden die Daten von den Mobile-Clients in die Datenbank gespeichert und alle administrativen Tätigkeiten durchgeführt. Weiters können alle Daten in einer aufbereiteten Form für die involvierten Mitarbeiter der GUT und für den Sicherheitsdienst eingesehen werden.

Dienstbuch der letzten 24 Stunden

Name	Haus	Zeit	Text	action
	Gusshausstr. 27-29	2009-04-27 08:56:04	E128/1 bringt alle 4 ausgeliehenen Plakatständer zurück	normal
	Treittlstr. 3	2009-04-27 08:26:29	3 Obdachlose aus dem 1. UG in der Treittlstrasse des Hauses verwiesen.	wichtig
	Stadionallee 2 (ATI)	2009-04-27 08:10:45	Folgender Brandmelder wurde Abgeschaltet:39	Brandschutz
	Gusshausstr. 27-29	2009-04-27 08:10:41	07:00 Uhr, Internetraum aufgesperrt und Kontrolle der Hörsäle, i.O.	normal
	Wiedner Hauptstr. 8-10 (Freihaus)	2009-04-27 07:51:49	Rundgang von 06:00 bis 07:52; Aussenrunde und WC Kontrolle KBV	normal

Zusätzlich zur Umsetzung der technischen Anforderungen wurde bei der Entwicklung des neuen System auch darauf geachtet, den Umschulungsbedarf des Sicherheitspersonals so gering wie möglich zu halten. Aus diesem Grund hat man sich hinsichtlich der Bedienung stark am bisherigen System orientiert und erreichte dadurch eine sofortige Akzeptanz von Seiten der Benutzer.

GuT-tracker - Rundgang Detail

Rundgang: -47559020091
 MitarbeiterIn: TU Wien Einschulung / TU Wien
 Haus: Argentinierstr. 8
 Beginn: 2009-04-26 20:19:18
 Ende: 2009-04-26 20:30:16

Raum	Zeitpunkt
EAEG03A (BMZ)	2009-04-26 20:19:48
EAEG09 (Lift)	2009-04-26 20:21:14
EALIFT (Lift)	2009-04-26 20:21:57
EA0538 (Dachboden)	2009-04-26 20:22:17
EA0509 (Lift)	2009-04-26 20:22:39
EA0502 (Dachboden)	2009-04-26 20:23:11
EA0409 (Lift)	2009-04-26 20:24:03
EA0309 (Lift)	2009-04-26 20:24:53
EA0209 (Lift)	2009-04-26 20:26:02
EA0109 (Lift)	2009-04-26 20:26:52
EAU109 (Lift)	2009-04-26 20:28:35
EAU120A (EDV-Labor)	2009-04-26 20:29:19
EAEG10 (Seminarraum)	2009-04-26 20:30:06

Besonderer Wert wird auch auf eine intuitive Benutzung der mobilen Applikation gelegt. Im Falle eines Schadens oder Mangels im kontrollierten Raum kann schnell und ohne Umstände die zuständige Stelle benachrichtigt werden. Ein mühsames Notieren und Benachrichtigen nach Ende des Rundganges ist somit nicht mehr nötig.

Ausblick und weitere Schritte

In der ersten Phase des Probetriebs wurden die *Tags* mittels NDEF – ein für NFC entwickeltes Protokoll – beschrieben und ausgelesen. Da die Erkennung von NDEF-*Tags* mit Standardschlüsseln arbeitet und somit jeder mit einem NFC-fähigen Gerät die *Tags* neu beschreiben kann, musste eine Absicherung der Daten erfolgen. Bei NDEF können die *Tags* zwar auf Read-Only gesetzt werden, jedoch ist diese Absicherung nicht mehr umkehrbar. Um eine Wiederverwendbarkeit der *Tags* zu gewährleisten, da diese Daten für verschiedene Applikationen beinhalten können, wurde auf das Protokoll für RFID-*Tags* umgestellt. Die Daten können somit jederzeit mit einem entsprechenden privaten Schlüssel auf die entsprechende Chipkarte übertragen werden.

Kurzfristig ist geplant, alle Gebäude mit dem *Tag*-System auszustatten. Die ersten Evaluationen des neuen Nokia-Handys haben jedoch aufgezeigt, dass die derzeit eingesetzten *Tags* nicht mehr ausgelesen werden können, wenn sie auf Metall befestigt wurden. Für die alte Handy-Generation war dies kein Problem, doch durch das Antennen-Redesign hat sich diese Situation leider verschlechtert. Aus diesem Grund werden nun neue Versuche mit größeren *Tags* gestartet.

Mittelfristig ist geplant, das System auf alle Räume der TU Wien zu erweitern und das Reinigungspersonal ebenso mit NFC-/RFID-fähigen Handys auszustatten, um auch über die Reinigungszyklen besseres Management zu haben.

Nicht zuletzt auf Grund der guten Zusammenarbeit zwischen dem ZID, TU GUT und INSO lief das Projekt bisher äußerst positiv an und wir sind zuversichtlich für den Vollbetrieb des neuen Systems. Mittlerweile bekundeten mehrere Firmen Interesse an diesem System.

Folgende Bereiche sind derzeit implementiert:

- Sichtbar für alle Benutzer des Systems:
 - Dienstbuch (Eintragen und Übersicht der Meldungen zum eigenen Gebäude der letzten 24 Stunden)
 - Dienstan- und -abmeldung
 - Dienst- und Rundgangsübersicht der letzten 24 Stunden
 - Dienstbucharchiv (alle Häuser ohne Zeitbeschränkung)
- Sichtbar nur für GUT-Mitarbeiter:
 - Dienstarchiv
 - Dienstabrechnung (für externes Personal zum Vergleich mit den Rechnungen der Firmen)
- Sichtbar nur für Administratoren:
 - Benutzerverwaltung
 - Tagverwaltung
 - Rundgangsverwaltung

Derzeitiger Status

Derzeit hat die Software die alte Dienstbuchapplikation bereits flächendeckend an der TU Wien abgelöst. Bei den Rundgängen wurden zwei kleinere Häuser für zwei verschiedene Sicherheitsdienstgruppen auf die neue NFC-basierte Lösung umgestellt und es konnten bereits durchwegs positive Erfahrungen gesammelt werden.

NI Multisim 10.0¹

Elektronikdesign und -test mit virtuellen Instrumenten in der studentischen Ausbildung

Alois Lugstein, Jürgen Smoliner
Institut für Festkörperelektronik, TU Wien

Multisim ist neben PSPICE eines der bekanntesten Programme zum Erstellen von Schaltungssimulationen. Dabei handelt es sich um die neueste Version der interaktiven Software für die SPICE-Simulation und die Schaltungsanalyse, die verbreitet für die Schaltungserfassung, die interaktive Simulation, den Leiterplattenentwurf und interaktive Tests eingesetzt wird.

Das Institut für Festkörperelektronik verwendet die National Instruments Simulationssoftware Multisim für Schaltungssimulationen, vorwiegend im Rahmen der studentischen Ausbildung (Labor Technische Elektronik 362.080).

Mit der Umstellung des Bauelementelabors im Jahr 2007 wurde das Labor dadurch aufgewertet, dass einerseits die Hardwarekomponenten (Oszilloskope, Signalgeneratoren, Netzteile...) erneuert wurden und andererseits der Schwerpunkt vom Aufbau der Schaltungen auf dem Steckbrett hin auf die Schaltungssimulation und der automatischen Geräteansteuerung und Datenerfassung mit LabVIEW umgestellt wurde. Gleichzeitig mit dieser Einführung ergab sich die Notwendigkeit, dass für die Ausbildung ein entsprechendes Software-Paket für die Simulation zur Verfügung steht. Nachdem einige Jahre PSPICE zum Einsatz kam, hat das Institut für Festkörperelektronik daher im vergangenen Studienjahr beim Zentralen Informatikdienst angeregt, das Softwarepaket Multisim, das von der Firma National Instruments (<http://www.ni.com/>) vertrieben und weiter entwickelt wird, im Rahmen einer Campus-Lizenz zu erwerben. Für TU-Studenten gibt es eine Studentenlizenz. Mit LabVIEW werden leistungsstarke Technologien für den Vergleich von echten Prototypmessungen mit simulierten Daten hinzugefügt.

Charakteristika von Multisim

NI Multisim bildet den Grundstock der NI-Plattform für die Elektronikausbildung, zu der auch die Workstation für die Prototyperstellung NI ELVIS (*Educational Laboratory Virtual Instrumentation Suite*) sowie NI LabVIEW gehören.

Die Software Multisim von National Instruments kombiniert die intuitive Schaltungserfassung mit leistungsstarker Simulation zur schnellen, einfachen und effizienten Entwicklung und Validierung von Schaltungen.

Es wurde im Hinblick auf die Bedürfnisse von Lehrkräften entwickelt und unterstützt den Schaltungsentwurf durch Hilfsmittel wie eingebaute Tests, virtuelle Bauteile und Bauteile mit definierter Maximalbelastbarkeit. Mit NI Multisim können Schaltungen mit einer umfassenden Bauteilebibliothek zügig erstellt und das Schaltungsverhalten mit dem zum Industriestandard avancierten SPICE-Simulator analysiert werden.

Multisim 10.0 verfügt erstmals über zahlreiche neue, professionelle Designfunktionen. Im Mittelpunkt stehen dabei Werkzeuge für anspruchsvolle Analysen und eine verbesserte Bauteiledatenbank. Die Bauteiledatenbank umfasst über 1200 neue Komponenten und mehr als 500 neue SPICE Modelle von führenden Herstellern wie Analog

¹ Ein Simulationspaket für die Simulation elektrischer Schaltungen [1]

Devices, Linear Technology und Texas Instruments. Darüber hinaus sind über 100 neue Modelle aus dem Bereich Spannungsregler und -referenzen enthalten. Weitere Verbesserungen sind ein neues Stromsondeninstrument sowie aktualisierte statische Sonden für differenzielle Messungen.

Typisches Anwendungsbeispiel im Rahmen der Laborübung „Technische Elektronik“

Mit der Kombination der Schaltungssimulationssoftware Multisim 10.0 und der Messsoftware LabVIEW, beide von National Instruments, werden in der Laborübung simulierte und reale Daten einfacher elektronischer Schaltungen verglichen. Multisim unterstützt die Studierenden bei der Dimensionierung und Optimierung von elektronischen Schaltungen wie z. B. Verstärkerschaltungen oder Filter. Des Weiteren vermittelt es elektronische Konzepte unter Verwendung anspruchsvoller SPICE-Analysen und ermöglicht damit „Designexperimente“ vor der praktischen Umsetzung im Labor.

Eine anschauliche grafische Darstellung der Frequenzabhängigkeit eines Filters kann in Form eines Bode-Diagramms erfolgen. Dabei werden in zwei Teildarstellungen die Abhängigkeiten der Amplitude (Betrages des Übertragungsverhaltens) und der Phasenverschiebung zwischen dem Eingangs- und Ausgangssignal jeweils in Abhängigkeit von der Frequenz dargestellt. In Abbildung 1 ist ein einfaches Schaltungsbeispiel eines kaskadierten Bandpasses 2ter Ordnung [2] abgebildet, anhand dessen die Anwendungsmöglichkeiten von Multisim erlernt werden. Man sieht aber schon an dieser Stelle wie einfach es mit MULTISIM ist, ein virtuelles Messinstrument in die Schaltung zu integrieren.

Die in Multisim generierte Schaltungssimulation wird in weiterer Folge in einem praktischen Versuchsaufbau über ein LabVIEW-Programm automatisch aufgezeichnet.

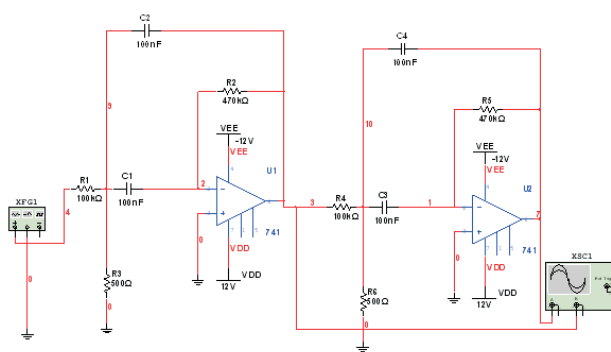


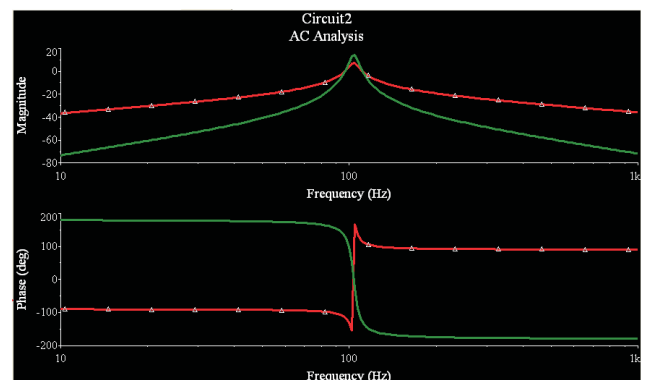
Abbildung 1: Kaskadierter Bandpass 2ter Ordnung mit virtuellen Messgeräten und zugehörigem Bodediagramm.

Erfahrungen mit NI Multisim

Die Erfahrungen mit NI Multisim, besonders für den Einsatz im Rahmen der studentischen Lehrveranstaltungen, sind durchwegs positiv. Die Studenten können sich rasch einarbeiten, da die Befehls- und Menüebenen sehr flach und gut strukturiert sind und damit sehr intuitives Arbeiten ermöglichen. Ein großer Vorteil ist die grafische, anschauliche Methode, aber vielleicht noch wichtiger, die dabei phantastisch einfache und direkte Art, mit verschiedensten Messgeräten und vorgefertigten Simulationsroutinen zurechtzukommen. Die Komplexität der SPICE-Simulation wird von Multisim abstrahiert, so dass der Anwender kein SPICE-Experte sein muss, um neue Designs schnell zu erfassen, zu simulieren und zu analysieren. Schon nach sehr kurzen Einarbeitungszeiten lassen sich in den Übungen schnelle Fortschritte erzielen. Der Vergleich mit anderen Softwareprodukten hat ergeben, dass NI Multisim für die Simulation der gängigen Schaltungen einen sehr guten Kompromiss aus Bedienungsfreundlichkeit und inhaltlicher Anwendbarkeit darstellt. Die einfache Bedienung und die gute inhaltliche Eignung für die Schaltungssimulation sowie der hervorragende Support waren im Endeffekt die Beweggründe, im Rahmen von studentischen Labors das Softwareprodukt NI Multisim einzusetzen.

Literatur

- [1] Jürgen Liepe, „Schaltungen der Elektrotechnik und Elektronik – verstehen und lösen mit Multisim“ Hanser Verlag, ISBN 978-3-446-41134-0.
- [2] Ulrich Tietze, Christoph Schenk: Halbleiter-Schaltungstechnik. 12.Auflage. Springer, 2002, ISBN 3-540-42849-6.



TISS is digging deep – Software Reengineering supported by Database Reverse Engineering

Stefan Strobl, Mario Bernhart
Institut für Rechnergestützte Automation / INSO

Ohne das tiefe Verständnis der Daten im Legacy System ist es schwer möglich, ein neues System zu schaffen. Die Migration von Funktionen eines Altsystems kann nicht bloß durch die Übersetzung des Source Codes einer Programmiersprache in eine andere erfolgen. Im Rahmen einer in englischer Sprache verfassten Diplomarbeit wurde ein Database Reverse Engineering Prozess adaptiert, um die Geschichte von vierzig Jahren Softwareentwicklung zu durchleuchten.

Introduction

One of the main goals of the project TISS (a detailed description of TISS can be found in [1]) is to reengineer and unify a large part of the information systems of the Vienna University of Technology (TUWIS). The legacy databases that have to be reverse engineered have a wide range of deficits making analysis and migration of the data structures and their contents difficult. In addition documentation for the database is scarce and consists mainly of comments for some tables and columns. Therefore a database reverse engineering process has been defined that aims at providing the necessary information about the legacy databases to successfully perform the data migration.

Problem Definition

TUWIS is a highly heterogeneous system. As almost every legacy system that has grown and evolved for forty years it has been modified and extended by numerous different developers with different technical skill levels and styles. To summarize briefly the legacy system to be reverse engineered actually consists of two subsystems which are tightly connected and highly interdependent. TUWIS, the older part, is written in COBOL and PL/SQL with a backend based on an Oracle DBMS. The newer part, TUWIS++, is a web built on the Zope application server, with a separate Oracle database. The two subsystems are mostly synchronized via their databases, which run on the same database server and duplicate large parts of the business data. Both systems interface in a wide variety of ways with neighboring systems. These neighboring systems range from information systems of government agencies, two SAP systems to multiple smaller specialized systems and tools.

Understanding the environment in which the database to be reverse engineered operates is essential. Often it is the only way to truly understand the structure of the database, if you analyze the data contained in it as well as the dataflow.

The identified deficits of the legacy databases the project team has to deal with are described in the following sections.

Missing Documentation

Original Cobol Legacy System (TUWIS)

Missing documentation is one of the key issues, a problem encountered in virtually all reengineering projects [2]. The original TUWIS user documentation consists of approximately 100 Microsoft Word files. Although primarily aimed at the users of TUWIS it contains valuable information about the database tables. This includes the table name as well as a table listing all columns, their data type and a short per column description. It does not, however, include more specific information like whether a certain column can be left empty or not. Basically this documentation is very similar to Oracle's table documentation that can be retrieved as HTML provided that the column comments have been entered into the database. Unfortunately the column comments have not been fully entered into the database, leaving the two documentation locations largely out of sync.

Another problem with the old TUWIS documentation is that the development of TUWIS++ has not been reflected. It does not reflect any changes made to the old schema during and after the development.

Web-based Extension (TUWIS++)

Technical documentation for the newer, web based part of TUWIS is even scarcer. Unfortunately attempts to document the system in detail have not been successful. There is a collection of information specific to project management issues. This includes mostly out of date information about the general direction and goals of the project (developing and maintaining TUWIS++). An incomplete Wiki proved to be useful for the architecture overview, its relevance for the project TISS is limited at best. Besides, the data also seems to be fairly out of date.

But there is a part of the TUWIS++ documentation that is most relevant for TISS. It provides additional information about the data of seven database tables. Compared to the total number of tables, this seems to be rather limited, but the tables documented are absolutely vital to the system. It provides a per column description of the data contents, which is an almost exact duplicate of the column comments provided directly in the database. Additionally it contains quite detailed information about the purpose of the table and its use. For the tables that can be found both in the TUWIS and TUWIS++ schema, it also provides information on how the data is synchronized and it is also the most recent, with the last modifications not dating back more than a year.

Database Comments (Data Dictionary)

The Oracle DBMS, like many other RDBMS products, provides the possibility to store a comment on each table and column directly in the database. This information is stored along with some information automatically gathered by the RDBMS system directly in the system. It is usually referred to as a data dictionary. This mechanism has been used by the developers on both schemas, but to different extents. In the TUWIS database schema not even a fifth of the tables have a comment associated with them (see Table 1).

In the second schema (TUWIS++) the commenting feature has been used a bit more extensively. A little more than a quarter of all tables in this schema have comments. Looking at the overall picture of the combined schemas, a little less than a quarter of all tables have comments associated with them.

Tables			
	Zope (TUWIS++)	Oracle (TUWIS)	Total
Commented	57	24	81
Uncommented	154	110	264
Total	211	134	345

Table 1: Amount of comments on tables in the legacy database

When it comes to comments on table columns the situation does not look that different (see Table 2). In fact the commenting feature has been hardly used at all for the old TUWIS schema. The new schema has been documented significantly better. About a third of all columns have been commented. Nonetheless, looking at the complete picture of the combined schemas gives a rather sobering view, as the high degree of documentation of the TUWIS++ schema is outweighed by the fact that the old TUWIS schema has significantly more (uncommented) columns.

Columns			
	Zope (TUWIS++)	Oracle (TUWIS)	Total
Commented	774	109	883
Uncommented	1644	3089	4733
Total	2418	3198	5616

Table 2: Amount of comments on columns in the legacy database

Oracle provides procedures to generate up to date documentation out of the information stored in the database. This way it is easy to provide a comprehensive document, like a collection of HTML files that correctly describe the content of a schema. As the comment information is transparently stored directly in the database in regular database tables it is also easy to generate or export the documentation information in a custom format.

Missing Normalization

In 1970 Codd [3] devised a set of normal forms that database designers should adhere to. The main goal of normalizing a database schema is to avoid inconsistent data in the database. The Boyce Codd Normal Form (BCNF) [4], although not the strictest variant of normal forms, is a de facto industry standard today. The normal forms define a set of rules that are intended to guide the designer of a data model towards a model that will prohibit database constructs that allow the storing of inconsistent data. Following this model will ensure that the data collected over the years will be consistent and complete enough to be useable later on. Generally not conforming to the normal forms can also be seen as a feature, mainly to achieve greater performance as described in [5]. Denormalization, as the process of intentionally introducing some violations to the normal forms for performance reasons is called, always starts with a completely normalized data model though. This is a risky approach that requires careful planning, documentation and evaluation whether the benefits outweighs the risks. In addition it imposes a certain responsibility on the developers of the application to enforce the constraints that have not been explicitly declared in the database schema in the higher layers of the application.

In the TUWIS and TUWIS++ data models virtually all of these rules have been violated. Yet this cannot be seen as the fault of the database designer. The design is a result of the migration of the legacy COBOL data storage to a relational database. A good example of a violation of normal forms is the way personal data is stored in the two systems. There are two tables representing personal data (e.g. name, date of birth, address, etc.), one for employees and one for students. Now the problem is that the two groups of persons are not disjoint. A student can be employed by the university and all the same a university employee might register as a student. As soon as a person is student and employee, two records partly containing the same data have to be maintained and kept consistent. The integrity of the data therefore cannot be enforced by the DBMS as it lacks the necessary information. Another violation of the First Normal Form (1NF) can be found in the employee table. A standardized email address is stored for each employee. In addition an employee can enter an additional email address via a university-wide address book application. All email addresses are stored in two fields, EMAIL1 and EMAIL2 of the same table. As the 1NF prohibits the use of "repeating groups" [6], this is a clear violation.

Data Model Deprecation

This section discusses the problem of obsolete database objects cluttering an overall view of the database. At first this seems like a rather easy problem to come by – identify unnecessary tables and document the findings so developers later know that these tables can be ignored (or removed from the production database, depending on the exact goal of the analysis).

Exactly therein the most difficult part can be found. Missing documentation makes solving this problem much harder than it needs to be. Actually, the two problems pretty much go hand in hand. While it would be fairly easy to remove old unused tables in a well documented environment it is a rather tough task if no reliable information is provided.

The basic problem is, as with missing documentation, the fact that a common policy or process for changes is not implemented or, if implemented, not followed by the developers. Many of the deprecated tables look like temporary tables, either created as a backup before running a certain script or simply used for some complex one time evaluations of the business data that needed a temporary storage. Some simple measures would have avoided the problem.

First of all, it is a best practice policy that temporary tables do not go into the same schema as the business data.

It would be rather easy for the developer to add a short note as a comment on the table indicating that this table does not contain business data.

Third, another way to mark tables as temporary would have been some common naming convention. Prefixing all temporary table names with something like “TMP_” or the like would have probably been enough too.

None of these measures have been implemented by the team developing and maintaining TUWIS(++). This leaves the new development team with the problem that it will have to tediously reverse engineer this information with the help of a set of fairly unreliable heuristics.

Data – Application Responsibility

This section will cover the problem of data responsibility. Data responsibility is a clear definition of which system is responsible for a certain (subset) of the business data in an environment where many systems share some common data. A good example of such data is the information that is stored about each person or employee. This data will be needed by several systems and it is likely that more than one system will be able to modify the data. This exposes this data to the risk of concurrent modifications.

Usually this problem is solved on the database level. This will only work though, if all data related to a specific business domain is stored in a single database schema. As soon as the data is distributed across several database schemas, conflicting changes can easily be stored by both systems and have to be merged later on. This task of merging conflicting changes (e.g. one person has different

home addresses in two different systems) often has to be done manually which is both expensive and inherently error prone. (How should somebody in the human resources department know which home address is correct?)

In TUWIS(++) data responsibility is often not clearly defined. Data gets imported from several different neighboring systems requiring manual intervention for conflicts in multiple cases. The logic behind the data synchronization is frequently hard coded in multiple places including import scripts and database triggers. Usually, this would not affect the reverse engineering of the database itself, but rather the overall task of migrating the whole application. Unfortunately, as the logic defining the data responsibility is partly implemented as database objects, it is necessary to also pay attention to this matter, especially during the migration phase.

Close Coupling

TUWIS is only part of a whole environment of systems that provide and process information. While these systems mainly operate independently from each other and are operated by different parts of the organization they also have to share information.

Since no common method of data exchange is employed, usually each interface between two systems is a separate solution often built on different methods of data exchange using a wide variety of different technologies. As TUWIS is an integral part of the overall system, it has a large amount of these interfaces – a total of approximately 25. Many of these interfaces operate on a similar dataset. So when migrating a set of tables that are used by some of these interfaces from TUWIS to TISS, all of them have to be modified in order to work with the new system. In many cases the migration will result in a complete rewriting of the interface. In some cases modifying or rewriting the interface will not be enough either, as the old interfaces are often highly specific. So in these cases modifications to the neighboring systems on the other end of these interfaces might be necessary.

All of the issues described above, especially the analysis of the old interfaces, necessary for modifying them accordingly, will require detailed information about the underlying database.

Solution

Migrating the data from the legacy database to the newly designed schema can be tedious without any documentation. In order to document the database properly, it is necessary to thoroughly analyze its structure, the use of the specific construct and its contents. The goal therefore is to detect most inconsistencies in the database during the documentation effort. This will greatly facilitate the migration process as the developer can use the documentation as a reliable resource pointing out the inconsistencies that he will later have to take into consideration during the migration phase.

The following process depicted in Figure 1 has been elaborate to reveal the required information on the legacy database. The process is structured into four parts, three of which are designed to be executed sequentially. None the less care has been taken to allow an iterative revisiting of each process step at later times. The fourth part is actually a cross section that is executed in parallel. It is also possible to define this part as a task that is common to all of the three primary parts.

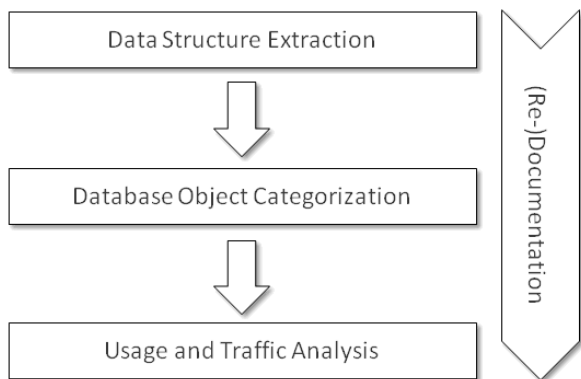


Figure 1: The reverse engineering process

Data Structure Extraction

Initially neither the extent nor the complexity of the legacy databases was known. Therefore it was necessary to create a comprehensive overview of the current structure. This step of the process was supported by off the shelf CASE (Computer Aided Software Engineering) tools. These tools, Fabforce DBDesigner41 and a documentation tool provided by the database vendor, were of great help for extracting the meta data (or source physical schema in [7]) describing the database structure. Nevertheless the (meta)data that has been automatically retrieved must be manually checked and, if necessary, completed. Furthermore a lot of more specific database object types will not be captured by any generic tool. Good examples are triggers, which are database objects that execute a procedure if a certain operation is executed on a data row, and synonyms, which are aliases to access a database object under a different name.

In the end the structural information about 346 tables with a total of around 5600 columns was extracted. Furthermore the comments stored directly in the database system were also transferred to a human readable and distributable format.

Database Object Categorization

The next step was to fully categorize the database assets discovered by the previous analysis. Therefore three main categories were defined:

- Relevant business data: all data that has to be migrated to the new system as otherwise a loss of business value would be unavoidable.
- System and implementation specific data: all data that is only needed for the legacy system to operate properly, but will not be migrated.

- Deprecated database assets: all aspects of the legacy databases that do not represent any semantical or operational value to either the legacy or the reengineered system.

The distinction between operational data and deprecated assets is relevant, as the operational aspects of the database still have to be regarded during the reengineering phase. It might not be possible to fully understand existing functionality, which has to be reengineered to the new system, without understanding the respective database areas.

The results of the categorization effort can be seen in Table 3.

Category	Oracle (TUWIS)	Zope (TUWIS++)
<i>DEPRECATED</i>	29	92
<i>Lookup</i>	3	16
<i>SAP</i>	22	19
<i>Studium</i>	23	12
<i>Pruefung</i>	9	11
<i>Raum</i>	2	0
<i>Personal Monatsjob</i>	6	0
<i>System</i>	7	6
<i>Personal</i>	20	7
<i>Batchsystem</i>	3	0
<i>Kanzleinformation</i>	4	0
<i>Lehrveranstaltungen</i>	7	16
<i>External applications</i>	0	9
<i>TUWIS++</i>	0	22
Total	135	210

Table 3: Categorization of the database in both schemas

Usage and Traffic Analysis

In this step of the analysis process the goal is to get a better impression of how intensively the legacy system is used and therefore get a first idea of how much of a strain will be on the reengineered system. The analysis of the legacy system will give some idea as to which parts should be most carefully designed with respect to performance.

Generally speaking the goal is to gather as much information about the usage of the database as possible. This starts with collecting read and write statistics. Ideally the database system provides means to count the number of reads, writes, updates and deletes on each table. It is essential that this data is gathered over the longest period of time possible. Depending on the legacy system and the business processes it implements, a lot of patterns will only become apparent over an extended period of time. To observe as many usage patterns as possible gathering the statistics for two or three months is essentially the absolute minimum.

The production database was configured to collect the appropriate data and produce a daily report. The data gathered in this way was then collected over more than six months and evaluated on a regular basis.

(Re-)Documentation

As mentioned earlier, unlike the other steps of the process, this task can be executed during or after each step. The presentation of results was deliberately separated from the remaining tasks, as it is frequently elaborated by a different group of developers on the reverse engineering team. In addition, this separation allows for a flexible “just-in-time” delivery of artifacts for concrete purposes.

During the application of this process the following artifacts were produced: One of the most valuable output of the process resulted from the results of the current state analysis and the categorization effort. The first step yielded a graphical representation of all tables of the legacy databases.

Due to the fact that all foreign keys were implicit the tables were more or less randomly distributed though. However, after performing the categorization step, some conclusions could be drawn as to which tables were related to each other. By including the categorization in the diagram from the previous step, the expressiveness of the presentation was significantly increased. By simply arranging the tables by category and at the same time color coding each of the categories, a universal diagram was created that visualized some of the key aspects of the migration effort. It demonstrated to nontechnical stakeholders the fact, that more than 40 percent of the legacy database assets would not be included in the migration.

A second and equally useful output was the web based redocumentation of the legacy database. On the basis of the results of the first two steps in the process a skeleton structure was generated in a wiki system. This skeleton consisted of one page for each table in the database as well as a series of indexes for easy access. The indexes were built representing the categorization. Additional indexes (e.g. sorted alphabetically) were also included. Each page describing a single table was already generated to include all the information available from the previous steps. During the execution of the data reverse engineering step the analysts then entered the newly retrieved information into these pages. After completing the third step of the process, the documentation was a fairly complete and up to date source of information for a wide array of developers, requirements analysts and of course the data migration experts.

Finally the usage and traffic analysis conducted in the last step also yielded results suitable for graphical presentation. A combined graph was developed that showed the number of read, write and delete in a bar chart in the bottom half and displayed the development of the total row count as a continuous line in the upper half. This chart was automatically generated for each database table.

Evaluation

Especially the categorization of the database tables including the elicitation of deprecated ones and the web based documentation has proven to be a vital part of the overall effort. On the other hand the usefulness of the effort put into producing a full usage analysis of the database has yet to fully surface. At this point it seems to make the most sense to again focus on the documentation effort to further improve this comprehensive source of information.

References

- [1] W. Kleinert, T. Grechenig, T. Költringer, M. Bernhart, A. Knarek, and F. Schönbauer. The making of TISS: Juni 2008. *ZIDline*, 18:3–8, June 2008.
- [2] Michael R. Blaha. Dimensions of database reverse engineering. In *WCRE '97: Proceedings of the Fourth Working Conference on Reverse Engineering (WCRE '97)*, page 176, Washington, DC, USA, 1997. IEEE Computer Society.
- [3] E. F. Codd. A relational model of data for large shared data banks. *Commun. ACM*, 13(6):377–387, 1970.
- [4] E. F. Codd. Recent investigations in relational database systems. In *ACM Pacific*, pages 15–20, 1975.
- [5] G. Sanders and S. Shin. Denormalization effects on performance of rdbms. In *HICSS '01: Proceedings of the 34th Annual Hawaii International Conference on System Sciences (HICSS-34)-Volume 3*, page 3013, Washington, DC, USA, 2001. IEEE Computer Society.
- [6] William Kent. A simple guide to five normal forms in relational database theory. pages 66–71, 1989.
- [7] J. Henrard, J.-M. Hick, P. Thiran, and J.-L. Hainaut, “Strategies for data reengineering,” in *Proceedings of the Ninth Working Conference on Reverse Engineering 2002*, (WCRE '02), 2002, pp. 211 – 220.

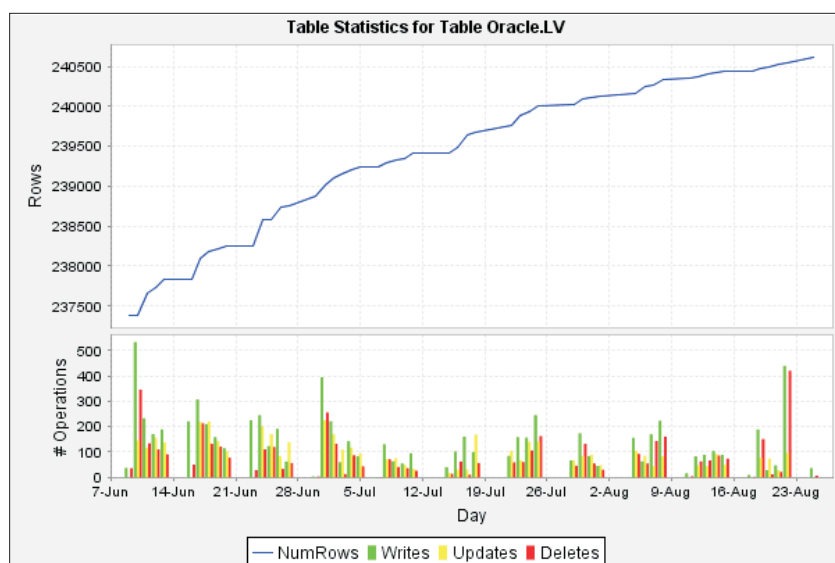


Figure 2: Example of the statistics visualization of a legacy database table

IT-Handbücher des RRZN

Die folgenden Handbücher des Regionalen Rechenzentrums Niedersachsen (RRZN) sind im Service Center des ZID für Studierende und TU-Mitarbeiter gegen Barzahlung erhältlich:

Titel	Preis
AutoCAD 2008 - Grundlagen	EUR 7,00
AutoCAD 2009 - Fortgeschrittene Techniken	EUR 7,00
C	EUR 4,00
C#	EUR 6,50
C++	EUR 4,00
CorelDRAW X3	EUR 6,00
CSS	EUR 6,00
Eclipse 3	EUR 6,50
Excel 2007	EUR 6,00
Excel 2007, Formeln und Funktionen	EUR 4,50
Excel 2007, Fortgeschrittene Techniken	EUR 6,00
Excel 2007, Automation und Programmierung	EUR 6,50
Flash CS3, Grundlagen	EUR 6,00
HTML 4	EUR 6,00
Java 2	EUR 7,00
Java und XML 2003	EUR 6,00
JavaScript	EUR 6,50
LaTeX	EUR 6,50
Mathematica - Eine Einführung	EUR 5,00
MySQL, Administration	EUR 6,50
Netzwerke, Grundlagen	EUR 6,00
Netzwerke, Sicherheit	EUR 6,50
Outlook 2007	EUR 6,50
Perl	EUR 4,50
PhotoShop CS3	EUR 6,50
PHP Grundlagen	EUR 5,50
PHP5	EUR 6,00
PowerPoint 2007	EUR 6,00
Programmierung, Grundlagen	EUR 6,00
Project 2007	EUR 6,50
SQL Grundlagen+Datenbankdesign	EUR 6,00
StarOffice 8 / OpenOffice 2 mit CD	EUR 5,00
Windows Vista - Grundlagen	EUR 6,00
Windows Vista, Systembetreuer	EUR 6,00
Word 2007	EUR 6,00
Word 2007, Fortgeschrittene Techniken	EUR 6,00

Aus organisatorischen Gründen kann der ZID nicht alle vom RRZN angebotenen Handbücher vertreiben. Wenn Sie Wünsche zur Beschaffung weiterer Handbücher haben (Angebot siehe <http://www.rrzn.uni-hannover.de/buecher.html>), senden Sie bitte eine E-Mail an office@zid.tuwien.ac.at.

Monatlicher Newsletter: <http://www.rrzn.uni-hannover.de/newsletter.html>

Zentraler Informatikdienst (ZID) der Technischen Universität Wien

Wiedner Hauptstraße 8-10 / E020
1040 Wien
Tel.: (01) 58801-42002
Fax: (01) 58801-42099
Web: www.zid.tuwien.ac.at

Leiter des Zentralen Informatikdienstes:
Dipl.-Ing. Dr. Wolfgang Kleinert

Auskünfte, Störungsmeldungen: Service Center

Bitte wenden Sie sich bei allen Fragen und Problemen,
die das Service-Angebot des ZID betreffen, zunächst an das Service Center.

Telefon: 58801- 42002
Adresse: 1040 Wien, Wiedner Hauptstraße 8-10, Freihaus, 2.OG, gelber Bereich
Montag bis Freitag, 8 bis 17 Uhr

Ticket System
Online-Anfragen: <https://service.zid.tuwien.ac.at/support/>

E-Mail-Adressen:
für Auskünfte und
Störungsmeldungen

office@zid.tuwien.ac.at
trouble@noc.tuwien.ac.at
hostmaster@noc.tuwien.ac.at
telekom@noc.tuwien.ac.at
security@tuwien.ac.at
pss@zid.tuwien.ac.at
css@zid.tuwien.ac.at
kurse@zid.tuwien.ac.at
operator@zid.tuwien.ac.at
mailhelp@zid.tuwien.ac.at
studhelp@zid.tuwien.ac.at
tuwis@zv.tuwien.ac.at

allgemeine Anfragen
TUNET Störungen
TUNET Rechneranmeldung
Telefonie
Netz- und Systemsicherheit
Systemunterstützung
Arbeitsplatz-Software
IT Online-Kurse
Operating zentrale Server
Mailbox-Service
Internet-Räume
TUWIS++



13. Oktober 2009

10:00 - 17:00

Geplante Themen:

Vienna Scientific Cluster
TUphone Projekt
u:book Informationsstand
TISS – Informationssysteme & Services
TUNET Infrastruktur
Services TU Bibliothek
Goodie Domain Service
SWD-Serverinfrastruktur
Dateninfrastruktur
Studentenservices
Service Center

Museum: „EDV an der TU Wien von 1965 bis heute“

Freihaus, 1. und 2. OG
Wiedner Hauptstraße 8-10

Wie schon im Jahr 2008 veranstaltet der ZID auch heuer einen „ZID-Day“.

Besuchen Sie uns am 13. Oktober im Gangbereich des Freihauses und informieren Sie sich über interessante neue Projekte.

www.zid.tuwien.ac.at/zid_day_09/