Zeitschrift: Visionen : Magazin des Vereins der Informatik Studierenden an der ETH Zürich

Herausgeber: Verein der Informatik Studierenden an der ETH Zürich

Band: - (1997)

Heft: 8-9

Heft

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Siehe Rechtliche Hinweise.

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. Voir Informations légales.

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. See Legal notice.

Download PDF: 16.05.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Visionen

8-9/97
August
September

Praktika in London und IT-Camp
Nebenfach Arbeitswissensch.
PGP Signing Party

VISKAS Bilder

Visionen Herausgegeben vom Verein der Informatikstudierenden an der ETH Zürich

Adressen

Präsident & Unterricht:
Michael Baumer mgb
Guggachstrasse 10, 8057 Zürich
e-mail: baumi@vis.inf.ethz.ch

Vize-Präsident & Quästor:
Katrin Rutishauser kr
Kampstrasse 18, 8952 Schlieren
e-mail: katrin@vis.inf.ethz.ch

Aktuarin: Silvia Geissberger sg
Etzelstrasse 24, 8200 Schaffhausen
e-mail: silvia@vis.inf.ethz.ch

Redaktion: Faby Honegger fh
Untere Halde 2, 5400 Baden
e-mail: faby@vis.inf.ethz.ch

Infrastruktur & Prüfungen:
Joachim Buechse jb
Leonhardstrshalde 19, 8001 Zürich
e-mail: jbuechse@iiic.ethz.ch

Verlag & Visinfo:
Michel Müller mm
Cristalinweg 4, 4310 Rheinfelden
e-mail: mimuelle@iiic.ethz.ch

Rechneradmin. & Exkursionen:
Caspar Schlegel cs
Schoental 5, 8126 Zumikon
e-mail: cschlege@iiic.ethz.ch

Feste: Andreas Tscharner at
Freiestrasse 38, 8032 Zürich
e-mail: andy@vis.inf.ethz.ch

WWW & Information:
Roland Brand rb
Gönhardweg 78b, 5000 Aarau
e-mail: roland@vis.inf.ethz.ch

Impressum

«Visionen»
Vereinsmagazin des
Verein der Informatikstudierenden an der ETH Zürich (VIS)

Erscheint 9x jährlich
Auflage: 1250

Bilder: Christian Fritz

Anschrift Verlag & Redaktion:
Verein der Informatikstudierenden (VIS)
ETH Zentrum, IFW B29
8092 Zürich

Tel.: 01/632 72 12 (zu Präsenzzeiten)
Fax: 01/632 11 72
Präsenzzeiten: Mo–Fr, 12.15–13.00

e-mail: vis@iiic.ethz.ch
http://www.vis.inf.ethz.ch/Visionen/
Postkonto: 80-32779-3

Jahresabonnement: CHF 25.–

Inserate:

1/1 Seite, schwarz/weiss	CHF 500.–
1/1 Seite, s/w + 1 Farbe	CHF 750.–
1/2 Seite, schwarz/weiss	CHF 250.–

Andere Formate auf Anfrage.

Druck:
Kaspar Schnelldruck AG
Birkenweg 2, 8304 Wallisellen

Die in den ***Visionen*** veröffentlichten Beiträge geben die Meinung des jeweiligen Autors wieder und müssen nicht mit der Meinung des VIS übereinstimmen. Für die Fehlerfreiheit solcher Beiträge kann keine Gewähr geboten werden. Offizielle Mitteilungen des VIS oder des Departements IIIC sind als solche gekennzeichnet.

Hoi zäme

Endlich haltet Ihr wieder ein Exemplar der Visionen in den Händen. Ein untrügliches Zeichen, dass es wieder aufs Semester zugeht. Die Studis erwachen aus dem Sommerschlaf? Nicht ganz, werden doch gerade jetzt noch einige ihre Zeit an irgendwelchen Prüfungen zubringen. Jedoch: rein vom gesellschaftlichen her stimmt das schon, beginnt mit dem Semester doch auch die Zeit der Feste, Cafeteria-Treffs und (was Professoren weniger gern hören) gesprächigen Vorlesungen wieder.

Damit sind wir bereits wieder bei den Aktivitäten des VIS angelangt. Beginnend mit dem Erstsemestrigentag, für den Tutoren gern gesehen sind (ab 9.00h in der IFW-Cafeteria) über die Erstsemestrigenfeste (von VIS und VSETH), den ACM-Programmierwettbewerb und eine PGP-Key-Signing-Party (siehe Artikel) zur Mitgliederversammlung des VIS.

NEXUS
Personal- & Unternehmensberatung AG

Die Informatik-Job-Börse
http://www.nexus.ch
Besuchen Sie uns!

Informatikstellen für ETH-Absolventen

Erstaunlich ist vielfach, wie wenig Zeit in eine Bewerbung investiert wird, nachdem man jahrelang für einen guten Abschluss gearbeitet hat. Machen Sie diesen Fehler nicht! Stellen Sie Ihre Weichen auf Zukunft. Wir helfen Ihnen dabei, sich professionell auf dem Informatikmarkt zu positionieren. Wir kennen den Insider-Stellenmarkt für ETH-Absolventen. Nutzen Sie unsere Beziehungsstärke zu innovativen Firmen. Die Beratung ist für Sie unverbindlich und kostenlos. Wir freuen uns auf Ihre Kontaktaufnahme und sichern Ihnen kompetente und neutrale Beratung zu.

NEXUS Personal- & Unternehmensberatung AG
Technopark, Pfingstweidstr. 30, 8005 Zürich, Telefon 01/445 20 21

Consultants für Hoch- und Fachschulabsolventen der Informatik

Und nun die grosse Überraschung: Wir suchen noch Mitglieder, die sich gerne betätigen würden. Der Möglichkeiten sind gar viele: Redaktor, Verleger, Feste-Mensch, Vertreter beim Departement und bei unserem Dachverband VSETH. Wer sich auch nur entfernt vorstellen kann etwas bei seinem Fachverein mitzuhelfen, soll sich eines der Vorstandsmitglieder schnappen und sich nach den offenen Posten erkundigen. Besonders fortschrittliche dürfen uns auch eine eMail senden.

Sofern wir dann einen neuen Festmenschen haben gibts dann auch wieder ein FIGUGEGL (Wenn Du diese Abkürzung nicht kennst: Wo lebst Du? :-)

Zum Schluss noch ein Nachtrag zu den letzten VISIONEN. Die drei Artikel ohne Autor (Bzgl. Prüfungsreglement) sind von mir. Die Unterschrft fehlte aufgrund eines Missverständnises. Allfällige Arztrechnungen wegen zu hohem Blutdruck übernimmt meine Krankenkasse.

Gruss „baumi" Michael

Blei im Kasten

Low-Level-Formatierung aus der Hüfte: Offensichtlich aus Ärger hat ein Mann in Issaquah im amerikanischen Bundesstaat Washington seinen Computer mit Blei vollgepumpt. Wie die Nachrichtenagentur AP berichtet, jagte der User vier Kugeln in die Festplatte und eine in den Monitor. „Wir wissen nicht, was los war, vielleicht wollte er nicht booten oder so", zitiert AP einen Polizisten. Die Polizei brachte die Nachbarn in Sicherheit, überredete den Mann am Telefon, herauszukommen und lieferte ihn in ein Krankenhaus ein. Dort soll er (EDV-gestützt?) auf seine seelische Gesundheit untersucht werden.

Aus der Meldung geht nicht hervor, welches Fabrikat und welches Betriebssystem den Amerikaner in die jähe Eruption sinnloser Gewalt trieben. (PC Magazin / mk)

Markus Dommann
mdommann@iiic.ethz.ch

PGP Key Signing Session

Die Sicherheit und Privatsphäre wird im Informatikbereich immer mehr thematisiert. Mit diesen Themen hat auch die Software PGP zu tun. Nachdem der VIS eine Kurzanleitung zu PGP in den Visionen 2-3/97 veröffentlicht hat, geht es jetzt weiter mit einer PGP Key Signing Session.

Was ist das?

An einer Key Signing Session geht es darum, dass die anwesenden Personen untereinander die Public Keys austauschen.

Und wozu?

Bei jedem Public Key Verfahren ist die Authentizität ("Echtheit") der Public Keys ein Problem. Ein kleines Beispiel: Ich erhalte von Germano Caronni eine elektronisch unterschriebene Mail. Um die Unterschrift zu prüfen, brauche ich seinen public key. Eine Mail an pgp-public-keys@keys.ch.pgp.net mit dem Subject GET caronni@tik liefert mir seinen public key. Aber ist das wirklich sein public key? Jemand (ein Betrüger) könnte einen Key mit dem Namen Germano Caronni erzeugt und auf dem Keyserver deponiert haben.

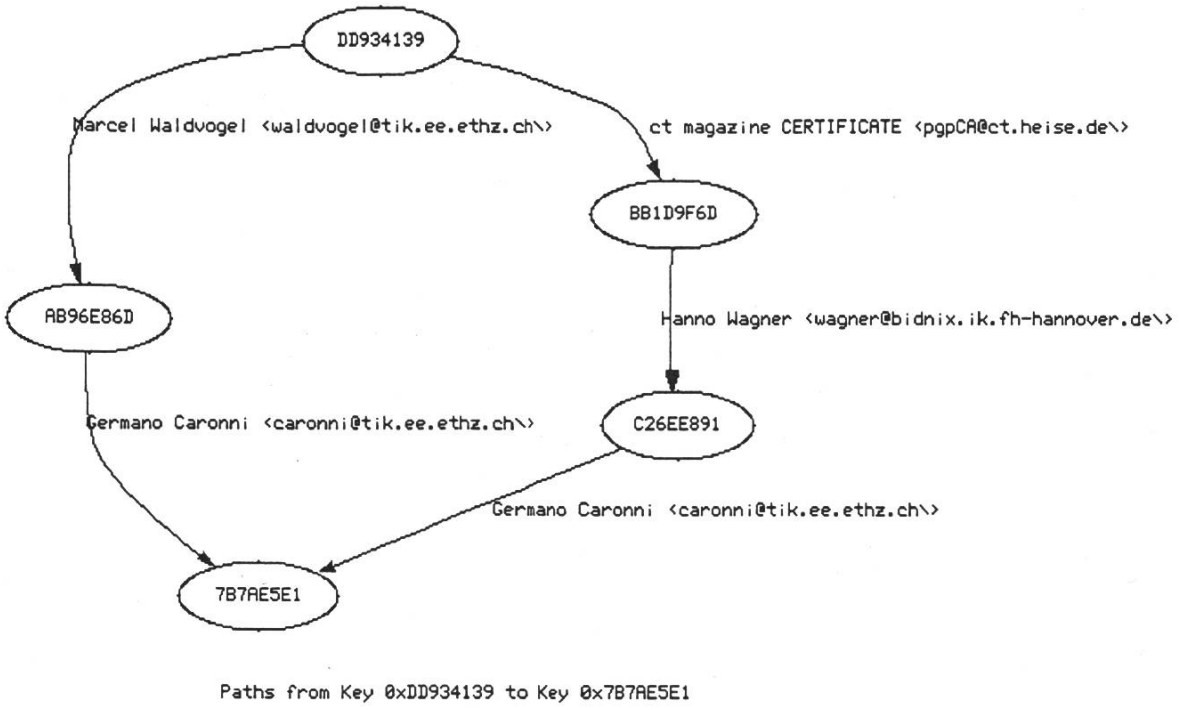
Ich muss nun die Echtheit dieses public keys überprüfen. Dazu habe ich verschiedene Möglichkeiten, zum Beispiel::

Ich suche im offiziellen Telefonbuch nach seiner Telefonnummer, rufe ihn an und lasse mir von ihm seine Schlüsseldaten (siehe Glossar) geben. Dazu muss ich ihn aber kennen (Stimmenidentifikation), denn es könnte sich ja eine andere Person als Germano Caronni ausgeben.

Ich gehe bei ihm vorbei, lasse mir seinen Ausweis zeigen und die Schlüsseldaten geben.

Ich schaue, ob jemand den ich kenne, seine Identität elektronisch bestätigt.

Die ersten beiden Möglichkeiten sind aufwendig und zum Teil undurchführbar (wenn der Key z.B. einer Person weit weg gehört). Die Dritte ist dagegen relativ einfach. Dazu gibt es sogar eine Hilfe, den AT&T PathServer, erreichbar unter `http://www.research.att.com/~reiter/PathServer/`. Dort kann ich die Schlüssel-ID meines public keys (`DD934139`) eingeben und die Schlüssel-ID des public keys von Germano (`7B7AE5E1`). Als Resultat erhalte ich folgendes Bild:



Paths from Key 0xDD934139 to Key 0x7B7AE5E1

Daraus ersehe ich: Marcel Waldvogel bestätigt, dass der Schlüssel `7B7AE5E1` Germano Caronni gehört (Marcel hat den Schlüssel von Germano unterschrieben). Ich wiederum habe den Schlüssel von Marcel Waldvogel unterschrieben und bestätige, dass der Schlüssel `AB96E86D` ihm gehört. Daneben gibt es noch einen weiteren Pfad über das ct'magazin und Hanno Wagner.

Damit solche Pfade existieren können (und möglichst kurz und disjunkt sind), müssen möglichst viele Schlüsselinhaber die Schlüssel anderer Schlüsselinhaber unterschreiben und diese Unterschriften auf den Keyservern (siehe Glossar) veröffentlichen, damit Dritte diese Bestätigungen auch nutzen können.

Das Ganze wird dann web of trust genannt.

Warum müssen die Pfade kurz und disjunkt sein? Die Pfade sind Ketten von Bestätigungen. Je länger der Pfad zwischen meinem Schlüssel und dem Schlüssel vom Germano ist, desto weniger sicher kann ich mir über die Echtheit des Schlüssel von Germano sein. Pfade, die keinen gemeinsamen Schlüssel zwischen dem Start- und Endschlüssel haben, sind disjunkt. Je mehr disjunkte Pfade existieren, desto geringer ist die Wahrscheinlichkeit, dass ein ‚schwarzes Schaf' durch eine falsch ausgestellte Unterschriften eine Bestätigungskette vortäuscht, die so gar nicht existiert. (Durch mehrere Schlüssel, die von derselben Person stammen, ist das dennoch möglich).

Was bringt Dir die Teilnahme?

Dein Schlüssel wird von vielen anderen Personen unterschrieben. Das erhöht die Wahrscheinlichkeit, dass Dritte die Echtheit Deiner Unterschrift nachvollziehen (überprüfen) können.
Du unterschreibst viele andere Schlüssel. Dadurch erhöht sich die Wahrscheinlichkeit, dass Du Schlüssel Dritter als echt akzeptieren kannst.

Brauche ich das denn?

"Nicht immer, aber immer öfter". Gefälschte Mails nehmen zu. Wenn Du all Deine Mail signierst fällt es auf, wenn eine Mail plötzlich nicht signiert ist. Wenn jemand ein Programm veröffentlicht und dieses digital unterschreibt, kannst Du überprüfen, ob es nicht gegen eine gefälschte Version (mit Viren oder sonstigen Geziefer) ausgetauscht wurde. (Ok, dem Autor musst Du trotzdem trauen. Aber alle mir bekannten Viren wurden von Dritten eingeschleust).
Immer mehr Dokumente werden elektronisch gespeichert und verteilt. Wer garantiert, dass diese Dokumente unverfälscht sind? (Man stelle sich vor, die Publikationen würden verfälscht: Wie peinlich, wenn darin plötzlich Sachen stehen, die an der fachlichen Kompetenz des Autors zweifeln lassen...)
Es ist heute selbstverständlich eine Mail unverschlüsselt zu versenden. Aber würdest Du die gleichen Texte auch per Postkarte versenden? Eine Postkarte ist erst noch nicht maschinell lesbar...
Oder Du brauchst für den Zugang zu einer Dienstleistung ein Passwort. Wäre doch schön, wenn der Dienstanbieter das rasch und unkompliziert per Mail zustellen könnte, oder?

Was kostet die Teilnahme?

Nur etwas Zeit.

Wer darf teilnehmen?

Alle, die mir Ihren public key zugesandt haben (siehe Wie nehme ich teil?). Explizit also Studierende aus allen Fachrichtungen, ETH-Angestellte aller Art (Dozierende, Assistierende, wissenschaftliche Mitarbeiter, sonstige Mitarbeiter...) und Externe.

Was bedeutet die Unterschrift eines Schlüssels?

Eine Unterschrift unter einen Schlüssel von XY heisst: Ich bestätige, dass der von mir unterschriebene Schlüssel zur Person XY gehört. Eine solche Unterschrift trägt aber keinerlei Informationen über die Rechtschaffenheit einer Person oder die persönliche Beziehung zu dieser Person.

Wie nehme ich teil?

Falls Du noch keinen PGP Schlüssel hast, musst Du Dir einen generieren. Siehe dazu den Text Installation von PG, Schlüssel generieren mit PGP und die Visionen 2-3/97.
Hole Dir die neuste Info über die Key Signing Session und PGP von http://www.vis.inf.ethz.ch/pgp/ . Dort findest Du weiterführende Infos zum Gebrauch von PGP. Z.B. wie PGP in verschiedene Mailprogramme integriert wird oder wie man mit den Schlüsseln umgehen soll und anderes mehr.
Überprüfe, ob Dein eigener Schlüssel von Dir unterschrieben ist (siehe Schlüssel generieren mit PGP).
Sende eine Mail mit Deinem PGP-Schlüssel an pafei@vis.inf.ethz.ch. Von Unix aus ist das möglich mit dem Befehl pgp –kxaf <userID> | Mail –s add pafei@vis. inf.ethz.ch. Damit kann ich alle public keys sammeln und zusammenstellen. (Siehe Was geschieht am 29. Oktober 1997.)

Reserviere Dir den 29. Oktober 1997 ab 15:15.

Kontrolliere ob von mir eine Bestätigung Deiner eMail kommt.
Was geschieht am 29. Oktober 1997? Der genaue Ablauf ist von der Anzahl Teilnehmer abhängig. Dies soll die Idee vermitteln:
Es wird ein Blatt mit allen Schlüsseldaten der mir zugesandten public keys verteilt.
Reihum liest jeder seine Schlüsseldaten (vom eigenen Key mit pgp –kvc erzeugt, ausgedruckt und mitgebracht) vor. Damit können die Übrigen kontrollieren, dass sie dieselben Schlüsseldaten auf ihrem Blatt haben.
Die Person, die vorgelesen hat, macht glaubhaft, dass sie auch die Person ist, die sie vorgibt zu sein. Falls die Person nicht wohlbekannt ist, durch einen Ausweis.
Jeder hat nun ein Blatt mit überprüften Schlüsseldaten. Nach dem Meeting holt jeder die bereitgestellte Datei mit allen öffentlichen Schlüssel und unterschreibt (zu Hause) die Schlüssel der überprüften Personen.
Ich sammle diese Unterschriften und lege sie zum Download bereit. Damit kann jeder in einem Durchgang alle diese Unterschriften zu seinem öffentlichen Schlüsselring hinzufügen. Ich sende die Unterschriften auch auf die Keyserver.

Weitere Infos?

Wer Fragen oder Anregungen hat: Ich freue mich über Mail an pafei@vis.inf.ethz.ch (verschlüsselt und signiert, wenn möglich). Sehr viel mehr findet sich auf http://www.vis.inf.ethz.ch/pgp/:
Kann ich denselben Schlüssel zu Hause und an der ETH benutzen?
Ich habe mehrere eMail-Adressen,

was nun?
Kann root meinen Schlüssel lesen?
Was muss ich im Umgang mit meinem Schlüssel beachten?
Wie funktioniert das web of trust?
Kann ich PGP konfigurieren?
Wie vereinfache ich die Anwendung von PGP?
Was ist bei der neuesten Version von PGP (Version 5.0) zu beachten?
Wie ist das mit Lizenzen und Exportrestriktionen?
...

Glossar

Schlüsseldaten: Fingerabdruck, Schlüssellänge und Schlüssel-ID. Kann mit pgp –kvc <userID> abgerufen werden.
Fingerabdruck (key fingerprint): Eine Art Kontrollsumme, die aus dem Schlüssel berechnet wird. Die Wahrscheinlichkeit, dass zwei Schlüssel dieselbe Kontrollsumme haben, ist vernachlässigbar klein. Es ist aber möglich, gezielt einen Schlüssel mit derselben Kontrollsumme zu erzeugen. Dann ist aber die Schlüssellänge unterschiedlich. Deshalb müssen alle Schlüsseldaten verglichen werden. (Üblicherweise kann ein Schlüssel mit gefälschtem Fingerabdruck nicht zur sicheren Kommunikation benutzt werden, da sie kein Produkt zweier Primzahlen mehr sind und einfach faktorisiert werden können. Es dürfte auch schwierig sein, den dazugehörigen secret key zu generieren. Der Schlüssel kann aber trotzdem auf dem Keyserver deponiert werden.)
Schlüssel-ID (key ID): Eine 8 Byte grosse Zahl in sedezimaler Schreibweise, die eindeutig einen Schlüssel identifizieren soll. Von diesen 8 Byte werden von PGP jeweils die 4 niederwertigsten angezeigt. Es wäre möglich, dass ein zweiter Schlüssel dieselbe Schlüssel-ID hat. Auf den Keyservern (mit im Moment ca. 50'000 Schlüsseln) ist bisher aber eine solche Kollision noch nicht passiert. Damit PGP zwischen einem Benutzernamen (UserID) und einer Schlüssel-ID unterscheiden kann, wird dem Schlüssel-ID ein `0x` vorangestellt, z.B. `0xDD 934139`.
Keyserver: Rechner, die eine Datenbank mit öffentlichen Schlüsseln und Unterschriften führen. Die Server (im Moment über 50) tauschen neue Schlüssel/Unterschriften untereinander aus. Dadurch kann für Abfragen ein beliebiger Server verwendet werden.
UserID: Der Benutzername, der zu einem Schlüssel gehört. Im Prinzip kann das ein beliebiger String sein, per Konvention ist das Format aber Name <eMail>, also z.B. Patrick Feisthammel <pafei@rubin.ch>. Ein Schlüssel kann mit mehreren UserID's versehen werden.

Installation von PGP

Allgemeine Infos

PGP legt zwei Schlüsselringe an. Einen für die öffentlichen Schlüssel (public keys) und einen für die privaten, geheimen (secret keys). Diese Schlüsselringe heissen pubring.pgp und secring.pgp. Zudem legt PGP noch eine Datei mit dem Namen randseed.bin an. Diese enthält Zufallswerte und ändert sich immer wieder, da bei jedem Gebrauch von PGP aus den Tastatureingaben neue Zufallswerte gewonnen werden.

Wer seine Schlüssel auf ein anderes System mitnehmen will, kann das durch Kopieren der Dateien pubring.pgp und secring.pgp. Um mit verschiedenen Schlüsseln und Unterschriften zu experimentieren, empfiehlt es sich vorher pubring.pgp und secring.pgp zu kopieren. Nach den Experimenten können diese einfach zurückkopiert werden und der alte Zustand ist wieder hergestellt.

Es gibt eine neue Version 5.0. Ich empfehle im Moment aber noch die Verwendung der Version 2.6.3ia, bis die Kinderkrankheiten der Version 5.0 ausgemerzt sind. Mehr dazu auf http://www.vis.inf.ethz.ch/pgp/.

Unter Unix

Wenn Du PGP auf den rifraf- oder slab-Rechnern verwendest, ist die Installation trivial:

Wechsle in Dein Home-Verzeichnis: cd ~

Erzeuge ein Verzeichnis mit dem Namen ‚.pgp': mkdir .pgp

Sollte pgp nicht in Deinem Pfad sein (einfach ‚pgp' aufrufen um das zu testen), musst Du Dein .zshrc oder .tcshrc (ev. auch eine andere Datei, je nach Shell und Installation) anpassen und /usr/local/bin zu der Variablen PATH hinzufügen.

Sollte PGP noch nicht installiert sein, oder traust Du der installierten Version nicht, dann musst Du PGP selber kompilieren und installieren. Die Sourcen sind erhältlich auf dem ftp-Server ftp://ftp.ch.pgp.net/pub/pgp/unix/pgp263is.tar.gz. Dieser FTP Server steht übrigens am TIK an der ETH.

Unter DOS, OS/2 und Windows

PGP selber kennt bis zur Version 2.6.3 keine graphische Oberfläche. PGP kann unter Windows und OS/2 in einem DOS-Fenster verwendet werden, oder aber über graphische Bedieneroberflächen, die dann im Hintergrund PGP in einem DOS-Fenster aufrufen.

Eine Quelle für PGP unter DOS ist ftp://ftp.ch.pgp.net/pub/pgp/dos/. Dort finden sich die Sourcen (pgp263is.zip, übrigens dieselben wie die im Unix-Verzeichnis, nur anderst gepackt), sowie eine bereits kompilierte Version von PGP in der Datei pgp263i.zip.

Eine Liste von graphischen Tools für Windows findet sich auf http://pgp/winutils. shtml.

"Win–Win!"

Das ist unsere Strategie–das Credo, nach dem der wahre Erfolg immer zwei Gewinner kennt. In unserem Business sind das

•der Mensch, den wir beraten, •und das Unternehmen, für das wir Menschen suchen und auswählen.

Wenn **Infor**matik oder Betriebswirtschaft Ihre Spezialität ist, Sie **da**s Ende Ihres Studiums vor Augen haben oder bereits **im** Beruf stehen, dann sollten Sie mit uns darüber sprech**en**. Wir bringen Sie zum Start bzw. Re–Start Ihrer **Karr**iere in Poleposition.

ATKINSON STUART & COMPANY

Consulting · Search · Selection

8023 Zürich · Löwenstrasse 2 · Postfach · Tel. 01/225 40 80 E-Mail: zuerich@atkinson.ch
5400 Baden · Badstrasse 15 · Tel. 056/221 81 00 E-Mail: baden@atkinson.ch
Internet: http://www.atkinson.ch

Die Installation:
Hole ftp://ftp.ch.pgp.net/pub/pgp/dos/pgp263i.zip
mkdir C:\PGP
Kopiere pgp263i.zip nach C:\PGP
pkunzip pgp263i. Diese Datei enthält pgp263ii.zip und eine dazugehörige elektronische Signatuer pgp263ii.asc. Wer eine ältere Version von pgp hat, kann die Signatur mit pgp pgp263ii.asc pgp263ii.zip überprüfen. (Z.B. auf slab: Zuerst unzip pgp263i.zip, dann Unterschrift mit dem auf den slab installierten pgp prüfen.)
pkunzip –d pgp263ii entpackt das Archiv mit Unterverzeichnissen.
Modifiziere AUTOEXEC.BAT:
SET PGPPATH=C:\PGP
SET PATH=C:\PGP;%PATH%
SET TZ=MET
TZ gibt die Zeitzone an, damit PGP die Zeit nach GMT umrechnen kann.
Wer MD5 hat, kann als kleine Sicherheit lässt die MD5 Summe (eine Kontrollsumme) von pgp263i.zip überprüfen: md5sum –b pgp263i.zip pgp263ii.zip muss ergeben: 4f ca f2 47 c2 6c 4c 15 a4 7d 3f d8 66 59 55 29 *pgp263i.zip ef 21 b8 15 5b 33 92 f0 95 ed 4e bb cd 16 82 c2 *pgp263ii.zip
Starte den Rechner neu, damit die Einträge in Autoexec.bat aktiv werden.
Damit ist die Installation beendet und Du kannst Deinen PGP Schlüssel generieren.

Unter Macintosh
Ich habe leider PGP noch nie auf einem Macintosh installiert. Es gibt aber eine eigene Homepage für die Macintosh-Version mit entsprechenden Informationen: http://www.math.ohio-state.edu/~fiedorow/PGP/.

PGP Schlüssel generieren

Achtung: Gib Passwörter (und speziell den pass phrase von PGP) nie über eine unverschlüsselte Leitung ein! Die Eingabe sollte immer auf dem Computer erfolgen, an dem Du arbeitest. (Um eine verschlüsselte Verbindung herzustellen, gibt es auf gut administrierten Rechnersystemen übrigens ssh als Ersatz von rsh und telnet.)
Bevor PGP eingesetzt werden kann, muss ein persönliches Schlüsselpaar erzeugt werden. Das geschieht mit pgp -kg. Für die Schlüsselgrösse sollte mindestens 1024 Bits gewählt werden. Eigentlich gibt es keinen Grund, nicht 2048 Bit zu wählen. Der einzige Nachteil ist die etwas längere Verarbeitungszeit. In den meisten Fällen stört dies jedoch nicht.
Als userID ist der eigene Namen und email-Adresse anzugeben, z.B.: Patrick Feisthammel <pafei@ rubin.ch>. Damit sonst niemand diesen Schlüssel verwenden kann, wird der geheime Schlüssel (secret key) mit einem pass phrase verschlüsselt. Das Wort phrase deutet darauf

hin, dass es länger sein sollte wie normale Passwörter (mind. 20 Zeichen werden empfohlen)! Durch den Rest - wie heisst es jeweils - führt das Programm. Danach befindet sich der öffentliche Schlüssel in einer Datei mit dem Namen pubring.pgp und der geheime Schlüssel (verschlüsselt mit dem pass phrase) in secring.pgp.
PGP 2.6.2 kann nur Schlüssel bis 2047 Bits erzeugen. Kein Grund zur Aufregung, wenn also trotz Eingabe von 2048 ‚nur' ein 2047 Bit Schlüssel erzeugt wird.

Den eigenen Schlüssel signieren

Ältere Versionen von PGP (2.6.2 und älter) unterzeichnen den erzeugten Schlüssel nicht selber. Das muss dann unbedingt manuell nachgeholt werden. Ohne die eigene Unterschrift könnte jemand die userID des Schlüssels verändern. Also unbedingt mit pgp –ks <userID> den Schlüssel unterzeichnen. Ob der Schlüssel unterzeichnet ist, kannst Du mit pgp –kvv <userID> kontrollieren. Hier der von mir selber unterschriebene Schlüssel (das sind zwei v nach dem k in pgp –kvv!):

```
Type Bits/KeyID  Date
pub  2020/DD934139 1996/02/14
Patrick Feisthammel <pafei@ rubin.
ch> sig DD934139 Patrick Feist-
hammel <pafei@rubin.ch>
```

Und hier ein Schlüssel ohne eigene Unterschrift:

```
Type Bits/KeyID  Date
pub  400/A6B06E6D 1997/08/27
Fritz Muster <nowhere@rubin.ch>
```

Key revocation Zertifikat

Jetzt ist auch der Moment um ein key revocation Zeritifikat zu machen. Mit diesem kann der Schlüssel als ungültig erklärt werden. Z.B. wenn man den pass phrase vergessen hat. Dieses Zertifikat sollte an einem sicheren Platz gespeichert werden. Da dieses Zertifikat erst in den Umlauf geraten darf, wenn der Schlüssel wirklich zurückgezogen werden soll, müssen die Originalschlüssel zuerst gerettet werden (die Befehle sind in Unix-Syntax angegeben):

cd <Verzeichnis mit pgp-Dateien>
mkdir backup
cp pubring.pgp pubring.ok
pgp –kd <userID>
pgp –kxa <userID> revoke
cp pubring.ok pubring.pgp

Mit dem Schritt 6 wird der ursprüngliche öffentliche Schlüsselbund wieder hergestellt. Das Rückrufzertifikat ist nun in der Datei revoke.asc. Wird diese Datei mit pgp eingelesen (oder auf die Keyserver gelegt), wird der Schlüssel unwiderruflich als ungültig erklärt.
Um zu kontrollieren, ob alles geklappt hat kann mit pgp –kv <userID> überprüft werden, dass kein key revocation Zertifikat mehr im eigenen Keyring ist.

Backup
Das key revocation Zertifikat und die Schlüssel sollte jetzt auf eine Diskette kopiert werden (DOS-Syntax):
copy *.pgp a:\
copy revoke.asc a:\
copy pgp.exe a:\
Diskette schreibschützen.
Diskette an einem sicheren Ort aufbewahren.
Die Diskette ermöglicht es später zur Kontrolle die original Schlüssel wieder zu holen. Das revoke.asc kann auf der Harddisk gelöscht werden um zu verhindern, dass es versehentlich auf einen Keyserver geschickt wird.

Eigene Schlüsseldaten
Damit andere Personen den Schlüssel unterzeichnen können, müssen die Schlüsseldaten überprüft werden können. Am Besten ist ein Papier-Ausdruck der eigenen Schlüsseldaten mit der eigenen handschriftlichen Unterschrift. Die Schlüsseldaten werden mit pgp –kvc <userID> ermittelt. Bei meinem Schlüssel sieht das so aus:
> pgp –kvc pafei@rubin
`Type Bits/KeyID Date`
pub 2020/DD934139 1996/02/14 Patrick Feisthammel <pafei@rubin.ch>
Key fingerprint = AD 23 A1 90 B1 2B AF BA 44 49 16 7E 3D A0 F3 C3
Wenn jemand Euren Schlüssel überprüfen will, muss er den Papierausdruck Eures Schlüssels mit seinem Programm-Output (von pgp –kvc <userID>) vergleichen. Dabei müssen alle drei Schlüsseldaten - die Schlüssellänge (Bits), die KeyID und der Key fingerprint - übereinstimmen. Zusätzlich muss natürlich auch die User ID stimmen.

Schlüssel an die Keyserver senden
Unter Unix geht das einfach mit pgp -kxaf <userID> | Mail -s add pgp-public-keys@keys.ch.pgp.net.
Allgemein lässt sich der Key zuerst extrahieren und dann per Mail an die Keyserver senden:
pgp –kxa <userID> mykey (erzeugt eine Datei mykey.asc mit dem öffentlichen Schlüssel)
Sende Mail an die Adresse pgp-public-keys@keys.ch.pgp.net mit dem Subject add und als eigentlicher Mailinhalt den Inhalt der Datei mykey.asc
Die Keyserver sind auch per WWW erreichbar. Der schweizerische Keyserver hat die Adresse http://www.ch.pgp.net/pgpnet/.

Patrick Feisthammel
pafei@rubin.ch

Danke
Ein spezieller Dank geht an Marcel Waldvogel, den Betreiber des CH-Keyservers für seine wertvollen Anmerkungen und Korrekturhinweise zu diesem Artikel.

PGP Key *Signing*

Session

Datum: 29. 10. 1997
Zeit: 15.15 Uhr
Ort und weitere Infos erhältlich unter
http://www.vis.inf.ethz.ch/pgp/

Praktikum im IT Camp des SBV

Im Wintersemester 1996/97 habe ich während fünf Monaten ein Praktikum im IT Camp des Schweizerischen Bankvereins in Basel absolviert. Dieses beschäftigt sich mit der Anwendung neuester IT-Technologien im Bankgeschäft. Dazu kooperiert es einerseits mit bankinternen Partnern, andererseits aber auch mit Hochschulen (z. B. ETH). Es besteht aus rund einem Dutzend Leuten, hauptsächlich (promovierten) Informatik- und Elektroingenieuren.

Ich arbeitete in der „Electronic Commerce"-Gruppe mit. Diese zeigt Ansätze auf, wie die Kommunikation zwischen Kunde und Bank unter Ausnutzung neuester Internet-Technologien gestaltet werden kann. Dazu werden Prototypen im Bereich Telebanking mit integrierter Kundenberatung, Homebanking mit objektorientierten User-Interfaces oder auch im Bereich elektronischer Zahlungssysteme und Kommunikationssicherheit erstellt. Beim Telebanking soll der Bankkunde ausser allgemeinen Bankinformationen auch ein speziell auf ihn zugeschnittenes Informationsangebot erhalten, welches dynamisch zusammengestellt wird und konfigurierbar sein soll. Bei Fragen soll er
die Möglichkeit haben, mit einem Kundenberater und bei Bedarf mit weiteren Spezialisten per Videokonferenz Kontakt aufzunehmen. Aus logistischen Gründen soll dafür keine separate, evtl proprietäre Videokonferenz-Anwendung verwendet werden, sondern ein in den Internet-Browser integriertes Tool, das auf Internet-Protokollen aufbaut. Meine Aufgabe war es nun, solch eine Videokonferenzmöglichkeit zur Verfügung zu stellen.

In einem ersten Schritt habe ich mir einen Überblick über schon vorhandene Anwendungen verschafft. Die erste Zeit meines Praktikums verbrachte ich somit primär mit Internet-Surfing und dem Ausprobieren verschiedener Videokonferenzapplikationen. Dabei zeigte sich, dass aus Bandbreitengründen kaum von Videokonferenz, sondern eher von Still Image-Konferenz gesprochen werden muss und die knappe Ressource primär dem Audioteil zuzuteilen ist. Die vorhandenen Tools hatten meist den Nachteil, dass es sich um Standalone-Applikationen handelte, die unabhängig vom Browser

funktionierten. Auch erlaubten nur wenige mehrere gleichzeitige Verbindungen. Browserbasierte Audio- und Video-Lösungen beschränkten sich meist auf den Empfang von „streaming data". Deshalb entschloss ich mich, selber ein den Erfordernissen entsprechendes Tool zu entwickeln.

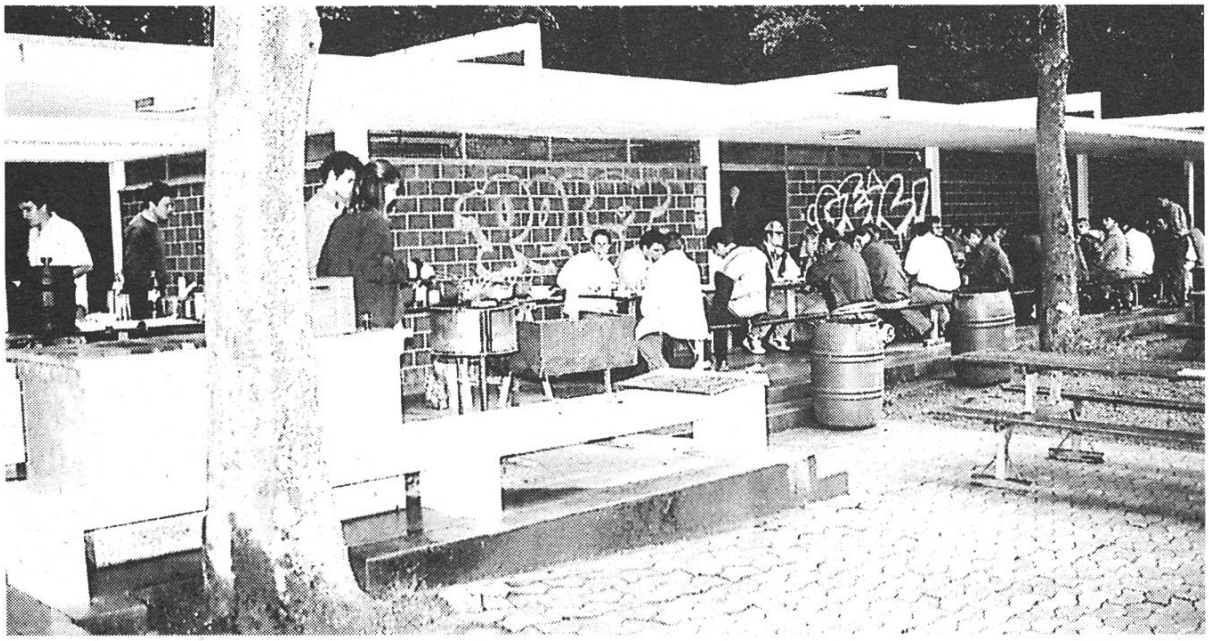
In einem zweiten Schritt nahm ich die dazu verwendbaren Technologien Java, ActiveX und Netscape-Plugin etwas genauer unter die Lupe. Die ersten beiden fielen aus Performanz- resp. Komplexitätsgründen rasch aus dem Rennen, und ich entschloss mich, ein Plugin für den Netscape Navigator zu implementieren.

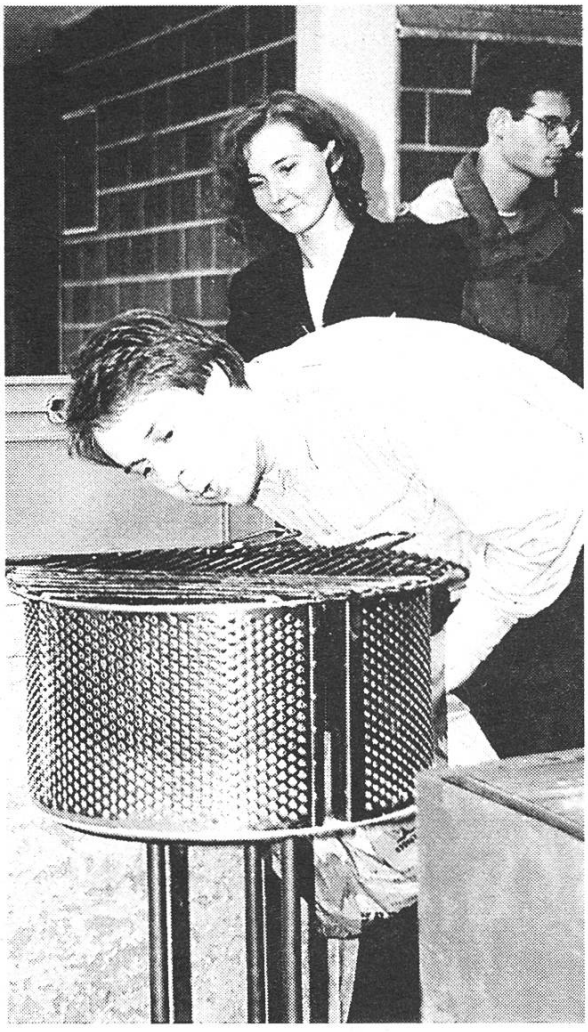
Um Entwicklungsaufwand zu sparen, hielt ich Ausschau nach einem Videokonferenz-Tool mit frei verfügbarem Sourcecode, das ich dann in ein Plugin umgewandelt hätte. Allerdings fand ich nur eine Internet-Telefonie-Applikation, die meinen Ansprüchen gerecht wurde. Das Video-Capturing und die Übertragung dieser Daten musste ich also selber entwickeln. Zu deren Komprimierung untersuchte ich verschiedene Standards wie MPEG und H.263.

In der Mitte des Praktikums fiel der Entwicklungsentscheid; die oben erwähnte Telefonie-Applikation sollte in ein Plugin umgewandelt und mit einer MPEG-codierten Videoübertragung ergänzt werden. Zur Ermöglichung mehrerer gleichzeitiger Sender und Empfänger sollte ein Reflektor verwendet werden. Dazu sollte der Sourcecode eines bestehenden Produktes lizensiert werden.

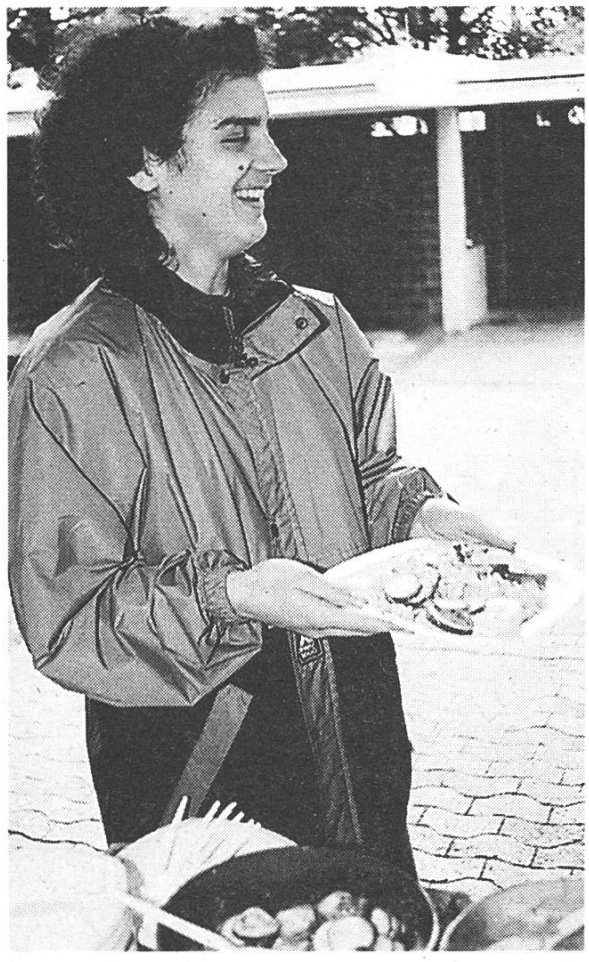
Die zweite Hälfte meines Praktikums diente der Implementierung des Plugins. Als Entwicklungsplattform verwendete ich MS Visual C++ 4.2 unter Windows NT 4.0 auf einem 90 MHz Pentium-Rechner. Die Entwicklung des Plugins verlief von ein paar (zeitraubenden) Windows-Macken abgesehen problemlos. Weil gegen Ende des Praktikums abzusehen war, dass der Reflektor-Sourcecode nicht rechtzeitig eintreffen würde, habe ich selber einen einfachen Reflektor implementiert.

Das Praktikum war für mich sehr interessant und lehrreich. Auf der Informatikseite erhielt ich die Gelegenheit, mich in ein mir vorher nahezu unbekanntes Gebiet einzuarbeiten. Des weiteren konnte ich das Aufkommen des Videoconferencing via Internet mit vielen neuen Tools (und noch mehr Ankündigungen...) mitverfolgen. Auf der Geschäftsseite gewann ich einen Eindruck vom strukturellen Umbau und der informatikmässigen Er-





VISKAS



neuerung einer Schweizer Grossbank.

Für einen Informatiker herrschen im IT Camp fast schon paradiesische Zustände, er muss sich nicht mit irgendwelchen Legacy-Anwendungen herumschlagen und kann sich mit neuen Technologien beschäftigen. Auch auf persönlicher Ebene sind meine Erfahrungen mit dem IT Camp durchwegs positiver Natur; ich war von Anfang an mit allen Mitarbeitern per Du, sie standen mir bei Problemen stets zur Seite, und ich wurde voll ins Camp integriert, d. h. ich nahm an allen Sitzungen und auch an einem Weiterbildungsseminar zu OLE, ActiveX & Co. teil.

Urs Hengartner
uhengart@iiic.ethz.ch

180 Semester zum Vernaschen.

180 SEMESTER STUDENTEN-KIOSK
Eine Non-Profit-Organisation der Studentinnen und Studenten der Universität Zürich

Informatik-Nebenfach Arbeitswissenschaften: Ein Erfahrungsbericht

Wohl die meisten haben sicher schon die traurige Erkenntnis gewonnen, dass es sehr deprimierend sein kann, wenn man auch nach einer halben Stunde den Videorecorder nicht programmieren oder ein Dokument auf dem Computer nicht ausdrucken konnte oder die Speicherfunktion des Telephons immer noch nicht so funktioniert, wie sie eigentlich sollte. Viele bereits bestehende Produkte besitzen grundlegende Designfehler, die darauf schliessen lassen, dass bei deren Entwicklung nicht genügend Augenmerk auf die physiologischen und psychologischen Merkmale des Menschen gelegt wurde. Ein Forschungsgebiet, welches sich mit diesem Thema auseinandersetzt, heisst Ergonomie (in Europa) oder Human Factors (in den USA). Schon die Namen deuten darauf hin, dass es dabei darum geht, die menschlichen Eigenschaften in die Entwicklung von Produkten verstärkt einfliessen zu lassen. Es wird nicht der Mensch an die Arbeit und Maschine angepasst, sondern die Arbeit gemäss den menschlichen physiologischen und psychologischen Merkmalen geplant und die Maschine an die menschlichen Masse und Fertigkeiten angepasst.

Interaktion mit Maschinen

Die Idee, bessere und intuitivere Schnittstellen zu schaffen, ist viel älter als der Computer. Jedes Werkzeug, das wir benutzen, hat eine menschliche Schnittstelle und die Art und Form dieser Schnittstelle hängt sowohl vom Können des Designers als auch von der Komplexität der Aufgabe, die das Werkzeug leisten soll, ab. So ist der Griff eines Hammers eine sehr einfache menschliche Schnittstelle, genauso wie der Hammer nur für eine einzige, einfache Aufgabe – eben das Hämmern – konstruiert ist. Aber wenn Sie schon einmal vor einem Fotokopierer mit fünfzig Knöpfen standen und sich gefragt habe, wie das Ding funktioniert, dann wissen Sie, was eine komplizierte Maschine mit einer schlecht gestalteten Schnittstelle ist. „Ich weiss, was ich will, aber wie kriege ich die Maschine dazu, es zu tun?" fragt sich der Benutzer.

Je komplexer das Werkzeug, desto schwieriger ist es, eine brauchbare Schnittstelle zu konstruieren. Und weil ein Computer tausendmal komplizierter als ein Fotokopierer und millionfach komplexer als ein Hammer ist, verwundert es nicht, dass viele Leute nichts mit Compu-

Exklusiv für Informatiker!

Ihr erster Karriereschritt

Lassen Sie sich unverbindlich beraten, ehe Sie eine so wichtige Entscheidung treffen. Sie finden bei uns umfassende Informationen über den aktuellen Arbeitsmarkt und ein breites Angebot an Informatik-Stellen. Eine Auswahl offener Positionen finden Sie jede Woche neu im Internet: Home Page http://www.cba.ch

Kennen Sie Ihren persönlichen Arbeitsstil?

Analysieren Sie Ihren Arbeits- und Leistungsstil anhand des Selbsteinschätzungsverfahrens «CAPTain». So erfahren Sie, wo Ihre Stärken liegen. Das Resultat: Sie kennen sich besser – Sie verkaufen sich besser.

Kostenlose Stellenvermittlung im Internet

Auf Wunsch publizieren wir Ihr anonymes Bewerbungsprofil in unserer Home Page. Dabei bürgen wir für absolute Diskretion und Qualität.

Mit uns finden Sie die richtige Stelle

Wir unterstützen Ihre Stellensuche mit unseren Vorlagen und Empfehlungen. Entscheidungsträger der Wirtschaft vertrauen uns.

Möchten Sie mehr über unsere Dienstleistungen erfahren? Rufen Sie uns an! Pia Brodmann gibt Ihnen gerne Auskunft.

Tel. 01/284 11 11, Fax 01/284 11 22. E-Mail admin@cba.ch

CBA

Computer Brainware Advisors
Unternehmensberatung und Stellenvermittlung
Beethovenstrasse 47, Postfach, 8039 Zürich
Internet Home Page: http://www.cba.ch

Basel Bern Genf Luzern Winterthur Zug Zürich

Mitglied VPS

tern zu tun haben wollen oder sich sogar vor ihnen fürchten. Aber das muss nicht so sein.

Schnittstellen zwischen Mensch und Maschine

Geben wir's doch zu: Mit Computern zu arbeiten, kann ganz schön schwierig sein. Zum einen sind sie unglaublich dumm: sie tun nur, was der Mensch ihnen sagt. Ausserdem verstehen sie lediglich merkwürdige, auf sie zugeschnittene Sprachen. Und schliesslich ist die Auswahl an Möglichkeiten, mit dem Computer zu kommunizieren, sehr klein.
Bei den frühen Computern war das noch viel mühseliger, weil die Information durch das Umlegen von Schaltern oder das Stanzen von Lochstreifen übermittelt werden musste. Dann verbesserte man die Schnittstelle, so dass der Rechner auf Texteingaben reagierte. Wenn der Computer also eine Berechnung ausführen sollte, tippte der Bediener eine Anleitung ein, die der Rechner verstehen und umsetzen konnte. War das Programm durchgelaufen, gab der Rechner seine Antwort.
Die Schwierigkeit mit dieser Text-Kommunikation ist, dass der Bediener meist eine Unmenge willkürlicher Verschlüsselungen und Abkürzungen parat haben muss. In den 70er Jahren entwickelte man daraufhin die grafische Benutzeroberfläche, um die Kommunikation zwischen Mensch und Maschine zu vereinfachen. Dank eines solchen Systems wie dem Apple Macintosh oder Microsoft Windows kann man auf dem Bildschirm bestimmte Zeichen mit der Maus anklicken oder hin und her schieben, um dem Rechner mitzuteilen, was man von ihm will. Der Rechner antwortet mit Bildern, Wörtern oder Tönen. So wird das Arbeiten nicht nur angenehmer, man kann sich auch leichter merken, wie man das Gerät benutzt.

Human-Computer Interaction

Ein Gebiet, welches sich intensiv mit obigen Problemen befasst, nennt sich Human-Computer Interaction (HCI). Bereits heute ist die internationale Fachgruppe, die sich damit befasst, eine der grössten innerhalb der ACM (SIGCHI). Dabei kommen sowohl physiologische als auch psychologische Probleme zur Sprache und werden Schnittstellen für die verschiedensten Bereiche, vom Hardwaredesign bis hin zu Schnittstellen der Zukunft in der Virtuellen Realität untersucht.
In England und in den USA werden an vielen Universitäten eigene Studiengänge auf dem Gebiet der Ergonomie und HCI angeboten und das Gebiet der Arbeitswissenschaften und der Mensch-Maschine Kommunikation spielt in

den dortigen Forschungsinstituten und in der Industrie einen bedeutend höheren Stellenwert als hier in Europa.
Bei HCI geht es oft darum, die Benutzerfreundlichkeit eines technischen Produktes zu analysieren oder zu verbessern. Daher werden oft die folgenden grundlegenden Punkte näher betrachtet:

- Erlernbarkeit: Wenn ein Benutzer eine Aufgabe lernt und später wiederholt, sollte die dafür aufgewendete Zeit beim zweiten Mal signifikant kleiner sein.
- Erinnerung: Benutzer sollten in der Lage sein, sich an gewisse Dinge zu erinnern, um das System auch zu einem späteren Zeitpunkt bedienen zu können.
- Produktivität: Benutzer sollten in der Lage sein, die Aufgaben schnell und effizient lösen zu können.
- Minimale Fehlerrate: Benutzer sollten von Anfang an möglichst keine Fehler machen müssen und wenn sie Probleme bekunden, sollte ihnen das System genügend Feedback und Hilfe anbieten, so dass sie die Aufgaben selber beenden können.
- Hohe Benutzerbefriedigung: Benutzer sollten ein gutes Gefühl während ihrer Arbeit haben. Sie sollten das Gefühl haben, dass sie ihre Aufgaben erfolgreich beendet haben und dass ihnen das System während ihrer Arbeit positiven Feedback und konstruktive Hilfe bietet.

Vorlesungen

Das Nebenfach Arbeitswissenschaften beinhaltet die folgenden Vorlesungen:

- Arbeitsphysiologie I (Prof. H. Krueger, IHA, Propädeutische Vorlesung)

Folgende Themen werden in dieser Ergänzungsvorlesung behandelt:
Arbeitssicherheit, Hygiene, Gesetzliche Grundlagen, Institutionen, Ergonomie in der Praxis, Belastungs-Beanspruchungs-Konzept, statische und dynamische Anthropometrie, Arbeitsplatzdimensionierung, Blindleistung am Arbeitsplatz (Heben, Tragen, Stehen, Sitzen), Psychophysiologie, Sehen, Sensorische Behinderung, Beleuchtungstechniken, Gestaltungsrichtlinien, Gestaltung optischer Anzeigen, Informationsverarbeitung, Ergonomie von Benutzeroberflächen.
Im Allgemeinen muss man diese Vorlesung von Krueger jedem Informatiker wärmstens empfehlen. Das Thema ist interessant und sehr lehrreich. Man kann seinen eigenen Horizont über die reine Informatik hinaus erweitern und bekommt erst noch eine der amüsantesten Vorlesungen zu hören, da Krueger aus einem schier unermesslichen Erfahrungsschatz schöpfen kann, der gespickt ist mit lustigen Anekdoten. Die Geschichten, die das Leben

(oder die Designer) schrieb und die Art und Weise von Krueger's Erzählung garantieren für kurzweilige Stunden.

• Arbeitspsychologie I (Prof. G. Grote, IfAP, Propädeutische Vorlesung)

Folgende Themen werden in dieser Ergänzungsvorlesung behandelt oder kurz gestreift:

Die Bedeutung von Arbeit (Werte, Motivation, Persönlichkeitsentwicklung), Analyse und Bewertung von Arbeit, Gestaltung von Arbeit (Aufgabenerweiterung, Gruppenarbeit), Grundprinzipien der Gestaltung von Technik als Arbeitsmittel, Benutzergerechte Dialoggestaltung, Aufgabenverteilung Mensch-Technik, Veränderungen in Unternehmen durch Technik, Arbeit in Projektteams (Soziale Wahrnehmung, Kooperation, Konkurrenz, Führen von Gruppen, Veränderungen von Organisationen (Phasen und Strategien, Umgang mit Widerstand).

Frau Grotes Vorlesungsstil kann wohl nicht mit derjenigen von Krueger mithalten, zumal leider nicht alle Themen im gleichen Masse interessant sind. Jedoch hat man hier die Möglichkeit, erstmals selbständig Benutzeroberflächen nach in der Vorlesung besprochenen Gesichtspunkten zu analysieren, was eine überaus interessante Arbeit sein kann (z.B. kann man hier seine Wut über die Microsoft-Produkte schreibend auslassen).

• Arbeits- und Organisationspsychologie II (Prof. G. Grote, IfAP)

Diese Vorlesung wurde bei uns im Blocksystem durchgeführt und zwar mit folgenden Themen:

Psychologische Grundlagen der Dialoggestaltung, Arbeitsgestaltung und neue Technologien, Psychologische Aspekte der Systementwicklung und -einführung.

Die Atmosphäre in unserer kleinen Gruppe war sehr angenehm und der enge und direkte Kontakt mit Prof. Grote wiederum sehr lehrreich. Neben normalen Theoriestunden hatten wir auch selbständig wissenschaftliche Arbeiten zu studieren und vorzustellen und konnten ausserdem gewisse Themen in der Gruppe erarbeiten.

• Design interaktiver Systeme (vormals Arbeitsphysiologie II, Prof. H. Krueger, IHA)

Diese Vorlesung ist als Fortsetzung zur propädeutischen Vorlesung Arbeitsphysiologie I angesetzt und sollte darauf aufbauend eine einführlichere Behandlung zum Thema der interaktiven System beinhalten. Die Vorlesung behandelt dabei folgende Punkte:

Einführung in die Ergonomie interaktiver Systeme, Belastungs-Beanspruchungs-Konzept, Leistungsfähigkeit, Verarbeitung sensorischer Information durch den

Menschen, Visuelle Information (optische Anzeigen, grafischen Oberflächen), Akustische Information (akustische Signale), Feinmotorik, sensomotorische Prozesse (Eingabemedien), Zentrale Prozesse und Reaktionen, Kodierung, Navigationshilfen, Untersuchungsmethoden, Mensch als Regler in Systemen, Benutzerführung, Mehrfachaufgaben, lineare und vernetzte Systeme, Kooperation, Risikoverhalten, Zuverlässigkeit, Problemlösungsverhalten, Simulation, Virtuelle Realität, Designprozess für Software-Dialoggestaltung, Ergonomie in der Praxis.
Das Problem dieser Vorlesung ist jedoch, dass sie ebenfalls für Studenten aus anderen Abteilungen, insbesondere für die Maschinen- und Elektroingenieure, gehalten wird und dadurch für die Informatiker mindestens die Hälfte der Vorlesung eine Wiederholung bereits bekannter Themen darstellt. Krueger gefällt sich ein bisschen in der Dozentenrolle und bringt dadurch immer wieder die gleichen, wenn auch witzigen Experimente, zur Sprache. Vielleicht sollte hier eine bessere Koordination der Vorlesungen vorgenommen werden. Jedenfalls waren wir enttäuscht, dass nicht so viele praktische Beispiele besprochen und analysiert wurden.

- Methoden der benutzerorientierten Softwareevaluation (Usability, Dr. M. Rauterberg, Dr. D. Felix, Prof. H. Krueger, IHA)

Diese dritte Vorlesung ist die eigentliche Hauptvorlesung und behandelt im Detail Themen der benutzerpartizipativen Software-Gestaltung, Formen der Usability und die Anwendung von grundlegenden ergonomischen Prinzipien bei der Produkte- bzw. Schnittstellengestaltung. In einem ersten Teil des Semesters werden dabei die theoretischen Grundlagen erarbeitet, die darauf in einem zweiten, praktischen Teil angewendet werden. Dies oft mittels eines vollständigen Usabilitytests im Usabilitylabor der ETH im Technopark Zürich.
Die Atmosphäre mit den Dozenten ist sehr persönlich und äusserst sympathisch. Vor allem die beiden Hauptdozenten Rauterberg und Felix sorgen für ein positives Klima. Im meinem Fall war M. Rauterberg bereit, uns persönlich bei einer umfangreicheren Arbeit zu betreuen, die wir machen wussten, weil in diesem Semester diese Vorlesung gerade verschoben worden war. Dabei konnten wir einen vollständigen Usabilitytest im Multimedia-Labor der Universität Zürich auf dem Gebiet der Virtual Reality durchführen.

Zusammenfassung

Die Gestaltung von Schnittstellen zwischen Mensch und Maschine wird wohl auch in Zukunft eine immer grössere Bedeutung erhalten. Das Nebenfach Arbeitswissenschaften beschäftigt sich schon heute eingehend mit diesem Thema und bietet eine solide Grundausbildung für Leute, die sich nicht nur für Algorithmen und Datenstrukturen, sondern auch für die Bedürfnisse und Probleme der Benutzer interessieren und begierig sind, die physiologischen und psychologischen Möglichkeiten des Menschen kennenzulernen, um dieses Wissen in benutzerfreundlichere Softwareprodukte einbringen zu können. Insbesondere der Einbezug der Psychologie bietet für ein ansonsten sehr technisch orientiertes Studium etliche neue Aspekte ebenso wie der Kontakt mit 'normalen' Standardbenutzern und zukünftigen Endbenutzern äusserst lehrreich ist.

Wäre dies alles noch nicht Grund genug, Arbeitswissenschaften als Nebenfach zu wählen, so ist ausserdem eine kompetente und sehr freundliche und persönliche Betreuung von Seiten der Dozenten vorhanden und dazu viele Kontakte mit Testpersonen, die man gar nicht mehr missen möchte...

Für weitere Informationen verweise ich auf folgende Adressen:

- Institut für Hygiene und Arbeitsphysiologie (IHA): http://www.iha.bepr.ethz.ch
- Institut für Arbeitspsychologie (IfAP): http://www.ifap.bepr.ethz.ch
- SIGCHI: http://www.acm.org/sigchi/

Natürlich stehe ich auch persönlich gerne zur Verfügung:

Jonas Kurth
kurth@acm.org

Informationen aus dem Studiensekretariat:

Zur Unterstützung Ihrer Studienplanung steht Ihnen ab sofort der Katalog der Lehrveranstaltungen 1997/98 online unter

http://www.inf.ethz.ch/division/Katalog/Katalog.html

zur Verfügung. Sie koennen ihn aber auch in gedruckter Form beim Studiensekretariat beziehen.

S.J. Ackermann,
Fachberaterin,
Studiensekretariat, IIIC

Praktikum UBS London

Im Wintersemester 1996/7 habe ich mein Industriepraktikum bei der Schweizerischen Bankgesellschaft (UBS) in London verbracht.

Vorgeschichte

Ich wollte mein Praktikum nicht im deutschen Sprachraum verbringen. Die UBS als internationaler Konzern bot sich als mögliche Alternative an, da man als Schweizer Student nicht gerade zu den privilegierten Arbeitnehmern im Ausland zählt. Mit Hilfe der UBS in Zürich bin ich in Kontakt mit der Filiale in London gekommen. Das Vorstellungsgepräch hat anlässlich eines Geschäftsaufenthalts meines zukünftigen Chefs in Zürich stattgefunden. Nach fast 6 Monaten Warten habe ich dann schliesslich die Arbeitsbewilligung für England bekommen. Die Vorteile des rot-weissen Passes lassen grüssen...

UBS London

Die UBS beschäftigt in London rund 2500 Mitarbeiter. Im Gegensatz zur Muttergesellschaft in der Schweiz betreibt die UBS in London kein Retail Banking sondern konzentriert sich voll auf den Handel und das Investment Banking. Die UBS befindet sich in London in der sogenannten „City". In diesem Teil der englischen Hauptstadt befinden sich fast 500 Kapitalinstitute. Die City ist damit der grösste Finanzplatz Europas.

Arbeit

Auf der UBS in London arbeitete ich für die „Technology Management Group" (TMG). Die Aufgabe dieser Gruppe ist es, die neusten Entwicklungen im Technologiebereich zu verfolgen und deren Brauchbarkeit für den Bankbereich zu beurteilen. Die TMG realisiert damit vor allem konzeptuelle Studien oder steht anderen Abteilungen in beratender Funktion zur Seite. Die Gruppe besteht aus rund 10 Mitarbeitern, alles Spezialisten mit langjähriger Erfahrung auf ihrem Gebiet. So beschäftigt die TMG unter anderem einen Server-, einen Datenbank und einen Telekommunikationsspezialisten. Als erstes arbeitete ich für den „Desktop Product Manager". Dieser ist Ansprechpartner für sämtliche technologischen Belange im Zusammenhang mit dem Betriebssytem und den einzelnen Applikationen auf den PC's der Anwender. Für ihn entwarf ich eine „Datenbank für NT 4 System-Tests". Dazu zuerst eine Hinter-

G L A N C E

Software Engineering

Als eigenständiges Schweizer Ingenieurunternehmen mit 28 Mitarbeitern versteht sich Glance AG vor allem auf

- das Erbringen von Entwicklungs- und Beratungsdienstleistungen im Bereich innovativer Informationssysteme, sowie
- die beratende Unterstützung bis hin zur schlüsselfertigen Realisierung von technischen Software-Projekten wie Sanierung, Überarbeitung und Erneuerung bestehender Systeme, das Re-Engineering.

Wir arbeiten für namhafte Kunden aus der Industrie und dem Dienstleistungssektor mit einem vielseitigen Projektportfolio, welches unter anderem die Bereiche Electronic Document Management, Anlage-Portfolio-Management, Medizinische Informationssysteme und Gebäudeleittechnik umfasst.

Zur Verstärkung unseres Teams suchen wir initiative, selbständig arbeitende

Entwicklungs-Ingenieure

mit Interesse an anspruchsvoller Arbeit im Umfeld von grafischen Benutzeroberflächen (MS Visual C++, DSC++), relationaler sowie objektorientierter Datenbanken (ODBC, Oracle, Objectivity) und offenen Plattformen (Unix, Windows).

Sie arbeiten mit bei der Erstellung von Spezifikationen, Entwurf und Konzeption, Realisierung, Test sowie Dokumentation unter Anleitung eines erfahrenen Projektleiters.

Wir bieten moderne Arbeitsmittel in kollegialer Atmosphäre sowie ein interessantes und breites Betätigungsfeld mit Freiraum für Initiative und Eigenverantwortung — und nicht zuletzt Weiterbildung. Der Arbeitsplatz liegt im Grünen und ist 2 Minuten von der S-Bahn (S5) entfernt.

Rufen Sie uns an, wenn Sie mehr über diese Stelle wissen möchten, oder senden Sie Ihre Unterlagen an Herrn D. P. Bellmont.

GLANCE AG
Software Engineering
Gewerbestrasse 4, 8162 Steinmaur, Telefon 01 854 86 00

grundinformation. Ein grosses Problem mit dem sich die UBS im IT-Bereich zur Zeit herumschlägt sind die unterschiedlichen Betriebssysteme. Während UBS New York vor allem auf UNIX-Systeme setzt, findet sich in London auf fast allen Rechnern NT 3.51. Zürich schliesslich hat nach wie vor einen hohen Prozentsatz von Windows 3.11 Rechnern. Eine Harmonisierung in diesem Bereich würde die Bewirtschaftung wesentlich effizienter gestalten. Aus diesem Grund hat man sich für die Zukunft auf eine gemeinsame NT 4 Plattform geeinigt. Zürich hat dafür nun die nötigen Skripts geschrieben, die eine weitgehend automatisierte Installation des OS sowie der benötigten Applikationen erlauben. In London wird anschliessend ein unabhängiger Test durchgeführt. Meine Aufgabe bestand darin, die anfallenden Resultate der durchgeführten Tests sowie die eigentlichen Testskripts selbst in einer Datenbank abzulegen. Damit sollte ein hoher Wiederverwendbarkeitsgrad und eine rigorose Versionskontrolle gewährleistet werden. Als Entwicklungsumgebung standen mir zwei recht mächtige Tools zur Verfügung: „SQA Suite" erlaubt das weitgehend automatische Generieren von Testskripts und insbesondere auch das Aufspüren von Fehlern, und „Continuus" ermöglicht eine Versionskontrolle und eine klare Zugriffsberechtigung je nach Funktion des entsprechenden Benutzers. Ich benötigte fast 3 Wochen um mit den beiden Tools vertraut zu werden. Da ich keine genaue Spezifikation für meine Aufgabe erhielt, war mir recht lange nicht ganz klar welche Funktionalität die Datenbank für die NT 4 Systemtests eingentlich aufweisen sollte. Aus diesem Grund war ich gezwungen relativ oft die Gruppe, welche die Testskripts schliesslich schreiben sollte, mit Fragen zu belästigen. Dabei stellte ich vor allem fest, dass das Interesse an einer solchen Versionskontrolle- Datenbank nicht ausgesprochen gross war. Die Entwickler befürchteten vor allem einen zusätzlichen Verwaltungs-Aufwand. Insbesondere mein Chef musste deshalb viel Überzeugungsarbeit leisten.

Nach weiteren 2 Wochen hatte ich einen funktionsfähigen Prototypen feriggestellt. Dieser hätte dann eigentlich an der von Zürich gelieferten Installation ausprobiert werden sollen. UBS Zürich hatte schliesslich aber gravierende technische Probleme mit der automatisierten Installation, so dass die Test-Phase in London erst begonnen hat, nachdem ich die UBS bereits wieder verlassen hatte. Infolge dieser Vezögerung war ich gezwungen, dieses Projekt zu beenden. Als nächstes arbeitete

ich für den „Product Manager Tools and Methodologies". Dieser ist der technische Berater für alle Fragen bezüglich Methoden und Werkzeugen in der Entwicklung. Für ihn evaluierte ich Web-Tools im weitesten Sinne. Die erste Kategorie, die ich unter die Lupe nahm waren Konverter für Word Dokumente nach HTML. Die UBS in London will mittelfristig alle öffentlichen Dokumente auf das Intranet bringen und damit möglichst auf Papierversionen verzichten können. Da alle Dokumente mit Microsoft Word geschrieben werden, sind leistungsfähige Konverter nötig. Mit Hilfe des Internets verschaffte ich mir zuerst einen Überblick über die verfügbaren Programme. Bevor ich mit der eigentlich Produkte-Evaluation beginnen konnte, musste ich einen Anforderungskatalog zusammenstellen. Um diesen möglichst praxisorientiert zu gestalten, interviewte ich die unterschiedlichsten UBS-Mitarbeiter, von der Sekretärin über den Aktienhändler bis hin zum Support-Mitarbeiter.
In der Folge beschaffte ich mir Demoversionen über das Internet oder direkt über die offiziellen Vertriebskanäle. Die Evaluation ergab schliesslich, dass „HTML Transit" das Anforderungsprofil am besten erfüllte. Dieses Programm wurde dann beschafft und ich war darauf 2 Wochen lang beschäftigt interessierten IT- und Forschungsmitarbeitern, Demonstrationen und Einführungen zu geben. Dieser umfangreichen Evaluation folgten diverse kleinere, die keine konkreten Beschaffungen zum Ziel hatten, sondern den zuständigen Führungsmitarbeitern einen Marktüberblick geben sollten.
Nach den Konvertern beschäftigte ich mich dann mit „Authoring Tools" (grafischen Editoren für HTML-Seiten), „Site Management Tools" (Werkzeug für den Unterhalt von umfangreichen Webservern) und „Firewalls". Auch bei diesen kleineren Projekten ging ich wieder ähnlich vor: Nachdem ich mir einen Überblick über die Marktlage verschafft hatte, stellte ich einen Anforderungskatalog zusammen und testete und beurteilte anschliessend die Produkte nach diesen Kriterien. Das ganze schloss ich jeweils mit einem Bericht ab.
Nach all diesen Technologieabklärungen hatte ich in den letzten drei Wochen dann doch noch die Möglichkeit, ein kleines Prográmmchen zu schreiben: Umfangreiche HTML-Seiten werden üblicherweise in mehrere kleinere Files zerlegt und miteinander gelinkt. Wenn jemand solche Seiten ausdrucken will, ist das mitunter äusserst mühsam, da man jede Seite einzeln ausdrucken muss. Mein

Programm fasste all die einzelnen HTML-Seiten zu einem einzigen Dokument zusammen und entfernte dabei alle unnötigen Links.

Fazit

Mein Praktikum in England war in jeder Hinsicht ein voller Erfolg: Mein Hauptziel war es in einem anderen Kulturkreis zu arbeiten und mit einer fremden Sprache vertraut zu werden. Nach einem halben Jahr London wandelte sich mein holpriges Matura-Englisch in verständliche Umgangssprache, die auch den Schotten und den Iren in den Pubs standhielt. Das Arbeiten in der englischen Kultur war eine echte Bereicherung. Obwohl nur 600 km von der Schweiz entfernt, unterscheiden sich die Engländer doch ziemlich von den Schweizern. Das Augenfälligste für mich war das konsequente Trennen von Arbeit und Privatleben. Langjährige Mitarbeiter wussten beispielsweise voneinander nicht, ob sie verheiratet waren und Kinder hatten! Die Arbeit in den IT-Abteilungen der englischen Finanzwelt ist eher kurzlebiger als in der Schweiz. Head-Hunting ist an der Tagesordnung und Jobwechsel im Jahresrhythmus nichts aussergewöhnliches. Das ganze System ist ausgesprochen leistungs- und lohnorientiert. Die Umgebung war am Anfang etwas gewöhnungsbedürftig: Die durchschnittliche Bürogrösse ist auf etwa 60 Leute ausgelegt. Separate Büros sind gänzlich unbekannt. Selbst die Abteilungsleiter haben ihr Pult im gleichen Raum. Nachdem ich mich an den Dauerlärm gewöhnt hatte, empfand ich die hektische Atmosphäre als äusserst stimulierend.

Zum ersten Mal seit der RS war ich zudem wieder gezwungen, in „Schale" zu arbeiten. Nicht nur die Händler, sondern auch alle IT-Leute tragen in London Krawatte und Anzug. In der Bank selbst wurde ich sehr gut aufgenommen. Ich hatte ein wenig den Status eines Exoten, da im IT-Departement ausser mir nur die beiden höchsten Chefs Schweizer waren. Mit der Zeit wussten diverse Leute, dass da „so ein Schweizer Student" arbeitet, der nicht nur Englisch sondern auch Französisch und Deutsch kann. Diverse Male musste ich deshalb Publikationen im Intranet auf Englisch übersetzten (selbst für politisch brisante emails, die in Deutsch abgefasst waren, wurde ich einmal unter Schweigepflicht beigezogen). Mein direkter Chef Paul Wyndham war sehr zuvorkommend, er unterstützte mich nicht nur in allen technischen Belangen sondern auch bei kulturellen Problemen: Weshalb dauert die Mittagspause nur 15 Minuten und wird Sandwich-kauend vor dem Monitor abgehalten? Im nachhinein bin ich sehr froh, dass

ich fast nicht programmieren musste. Meine Evaluationen mit all den Interviews gaben mir ein viel breiteres Bild der Probleme in grossen IT-Departementen. Zudem war die Kommunikation mit anderen Mitarbeitern wesentlich motivierender als das Hacken von Programmzeilen vor dem eigenen Monitor. Zum Schluss noch ein paar wenige Worte zu London: Wer geglaubt hat, Zürich sei gross und biete alles, dem kann ich nur London empfehlen. Für mich war es eine der faszinierendsten Erfahrungen, ein halbes Jahr in dieser 24-Stunden Metropole zu leben. Genauso hektisch wie sich der Verkehr um den Picadilly Circus quält, spielt sich auch das Leben ab. Überall Bewegung, überall Leute, aus allen Kulturen, 7 Tage, 24 Stunden. Last but not least: Das Guiness ist nicht nur besser, sondern auch billiger als in Zürich! Folgenden Personen gebührt mein herzlichster Dank: Meinem Chef Paul Wydham für seine enthusiastische Unterstützung, Hans-Jörg Baumann und Emil Bleichenbacher für die Vermittlung und Werner Müller für die Organisation und Wertschätzung in London.

Thomas Kühne, DS
thkuehne@iiic.ethz.ch

(Wer sich für ein Praktikum bei der UBS in London interessiert, kann sich gerne mit mir in Verbindung setzen.)

WANTED 1

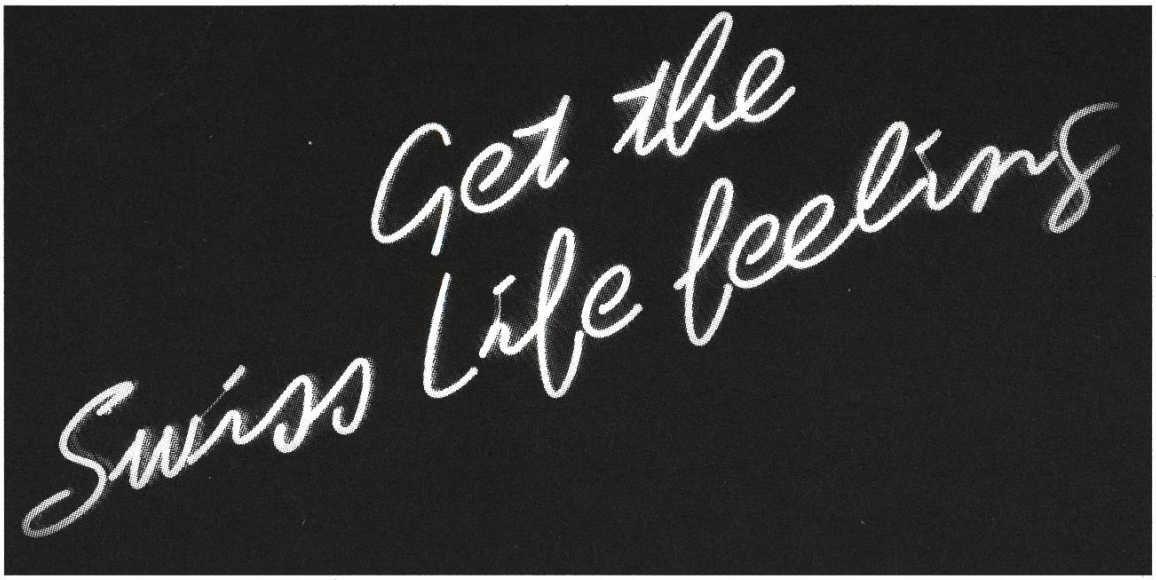
Hast Du Deine Prüfungen erfolgreich abgelegt? Hast Du wiedermal mit Deinem immensen Wissen sogar den Professor geblendet?
Dann **brauchen wir DICH**: um Deinen Nachkömmlingen das Lernen etwas zu erleichtern, wäre es schön wenn Du uns Deine mündlichen Prüfungsfragen mitteilen könntest und vielleicht sogar eine Musterlösung zu einer schriftlichen Prüfung liefern würdest.

WANTED 2

Hast Du manchmal den Kopf und die Nase voll von der ewigen Mathe? Sehnst Du Dich nach etwas mehr Kreativität und Selbstverantwortung?
Dann **brauchen wir DICH**: als Bereicherung für unser Vorstandsteam. Man lernt organisieren, verhandeln, Leute kennen und es ist sicher auch nicht hindernd für Deine zukünftigen Bewerbungen. Es gibt viel zu tun, pack's an!

Rentenanstalt

Swiss Life



Die Rentenanstalt/Swiss Life ist eine Lebensversicherungsgesellschaft zwischen Tradition und Moderne: 1857 als Genossenschaft gegründet – heute als Aktiengesellschaft auf dem Weg, unsere führende Position im Schweizer Markt auch auf Europa auszudehnen.

Im Versicherungs- und Kapitalanlagemarkt bildet eine hochstehende Informatik- und Kommunikationstechnologie den Hintergrund für die erfolgreiche Marktbearbeitung.

Rund 300 Informatikerinnen und Informatiker realisieren in Zusammenarbeit mit den Fachabteilungen laufend neue Softwarelösungen oder befassen sich mit der Integration und Konfiguration zugekaufter Produkte – beispielsweise SAP – in die Systemumgebung. Die Umsetzung dieser herausfordernden und vielseitigen Aufgaben erfolgt nach modernen Software-Engineering-Methoden.

Der Zugriff auf eine grosszügig konzipierte Infrastruktur, neueste Entwicklungswerkzeuge wie UNIX, C/C++, Oracle, Galaxy, Case-Tools, Repository, GUI-Builder und gut ausgebaute Aus- und Weiterbildungsprogramme erachten wir als wesentliche Voraussetzung für die erfolgreiche Arbeit unserer Informatikfachleute.

Für den Einsatz dieser neuer Technologien suchen wir junge, gut ausgebildete Nachwuchskräfte.

Sie als Absolventin oder Absolvent einer Hochschule verfügen über eine solide Ausbildung – wir bieten Ihnen verschiedene Möglichkeiten, Ihr Wissen in die Praxis umzusetzen und Ihre berufliche Laufbahn in einem interessanten, lebendigen Umfeld zu starten.

Kontaktieren Sie uns – Sie erreichen den Personalverantwortlichen für die Informatik, Herrn Reto Handschin, unter Tel. 01/711 45 32 oder via E-Mail reto.handschin@swisslife.ch.

Rentenanstalt/Swiss Life, Hauptsitz Zürich, General Guisan-Quai 40, Postfach, 8022 Zürich

Feedback

Anregungen, Wünsche, Bemerkungen zu den Visionen? Schreibt einfach eine Mail an die Redaktion: redaktion@vis.inf.ethz.ch

Redaktionsschluss

Die Artikel, die in der Oktoberausgabe erscheinen sollen, müssen bis spätestens **Ende September** bei der Visionen-Redaktion eingetroffen sein.

Hotlinks

www.iti.gov.sg/staff/kcchiang/bug
Der Spion des Netscape

www.eventhorizonmovie.com
Das schwarze Loch des Internets

www2.metropolis.de/innerwelt/chiya_walker
Die Liebe auf der Datenautobahn

www.escor.ch
Das Casino im Cyberspace

Termine

DO 25.9. - SO 5.10.	Interessante Abwechslung nach der Prüfungssession ist zweifelsfrei die **Züspa** für Studenten 5.- SFr.
MO 20.10.	**Semesterbeginn** ausserdem Notenkonverenz um 16:15, ich wünsche viel Glück!
DO 6.11.	Jetzt beginnt wieder die Zeit der Parties, gleich zu Beginn das **Erstsemestrigenfest** in der Polyterasse nicht nur für Erstsemestrige
SA 22.11.	Für etwas stilvollere und gediegenere Ansprüche, der legendäre **Polyball**
MO 24.11.	Die wichtige **Mitgliederversammlung** des VIS, mit Apéro, alle Informatikstudenten sind herzlich willkommen im GEP-Pavillon (Terminänderung vorbehalten)

P.P. 8304 Wallisellen

Falls unzustellbar bitte zurück an:

Verein der Informatikstudierenden
IFW B29
ETH-Zentrum

CH-8092 Zürich

Inhalt