Gefahren in der IT -

Ist Ihre Produktion sicher vor Angriffen?

VM/VSE GSE-Frühjahrstagung
2011 - Düsseldorf

Ingo Franzki – IBM
Dr. Manfred Gnirss – IBM
Heinz Peter Maassen – Lattwein GmbH

AGENDA

Überblick :

E-Mail

Telnet

FTP

HTTP Server mit z/VSE

- Rundum sorglos ?
- Sind Ihre Daten sicher ?
- Gefahren bei System z Umgebungen
- Machen Sie alles dicht - wie kann IBM hier helfen

Aktuelle Meldung 27.4.2011

E-MAIL UND VERSCHLÜSSELUNG

- Herkömmliche E-Mails sind mit einer Postkarte vergleichbar.
- Der Inhalt liegt offen und kann von jedem mitgelesen werden.
- Auch beim Mail Dienstleister lassen sich die E-Mail Daten sogar einfach und automatisch per Programm auswerten oder als Kopie aufbewahren zur späteren Analyse.

E-Mail und Verschlüsselung

- E-Mail ersetzt heute immer häufiger den Brief, Telegramm, Fernschreiben und Teletex.
- 1. E-Mail in Deutschland – wurde am 24. 8. 1984 von Michael Rotert an der TH Karlsruhe empfangen.
- 2010 wurde 107 Mrd. E-Mails versendet (90 % SPAM).
- Das heute verwendete Protokoll ist SMTP zum senden und POP3 oder IMAP zum empfangen.

E-Mail und Verschlüsselung

- Beim Versand werden die Daten meist über SMTPS verschlüsselt zum Mailserver übertragen.
- Auch das Abholen der Mails erfolgt meistens über POP3S oder IMAPS Protokolle.
- Jedoch auf den Servern liegen die Mails – wenn nicht verschlüsselt – lesbar.
- Das gilt nicht nur für den Body der Mails, sondern auch für die Anhänge.

E-MAIL UND VERSCHLÜSSELUNG

- Die meisten Angriffe gegen Unternehmen erfolgen von Innen.
- Welchen Weg eine Mail über das Internet geht und auf welchen dieser Server Mails gespeichert und mitgelesen werden ist nicht bekannt.
- Auf dem Weg zum Empfänger kann eine Mail auch verändert und deren Inhalt verfälscht werden.

E-MAIL UND VERSCHLÜSSELUNG

- Alles gute Gründe E-Mails zu verschlüsseln.

  Aber -

Warum macht das niemand ?

E-Mail und Verschlüsselung

- Alle heutigen E-Mail Programme unterstützen die Verschlüsselung von Mails
- Man muss sich nur einen Public/Private Key generieren – und entsprechende Programme zur Verschlüsselung nutzen
- Aber je nach Mail Programm werden verschiedene Methoden verwendet.

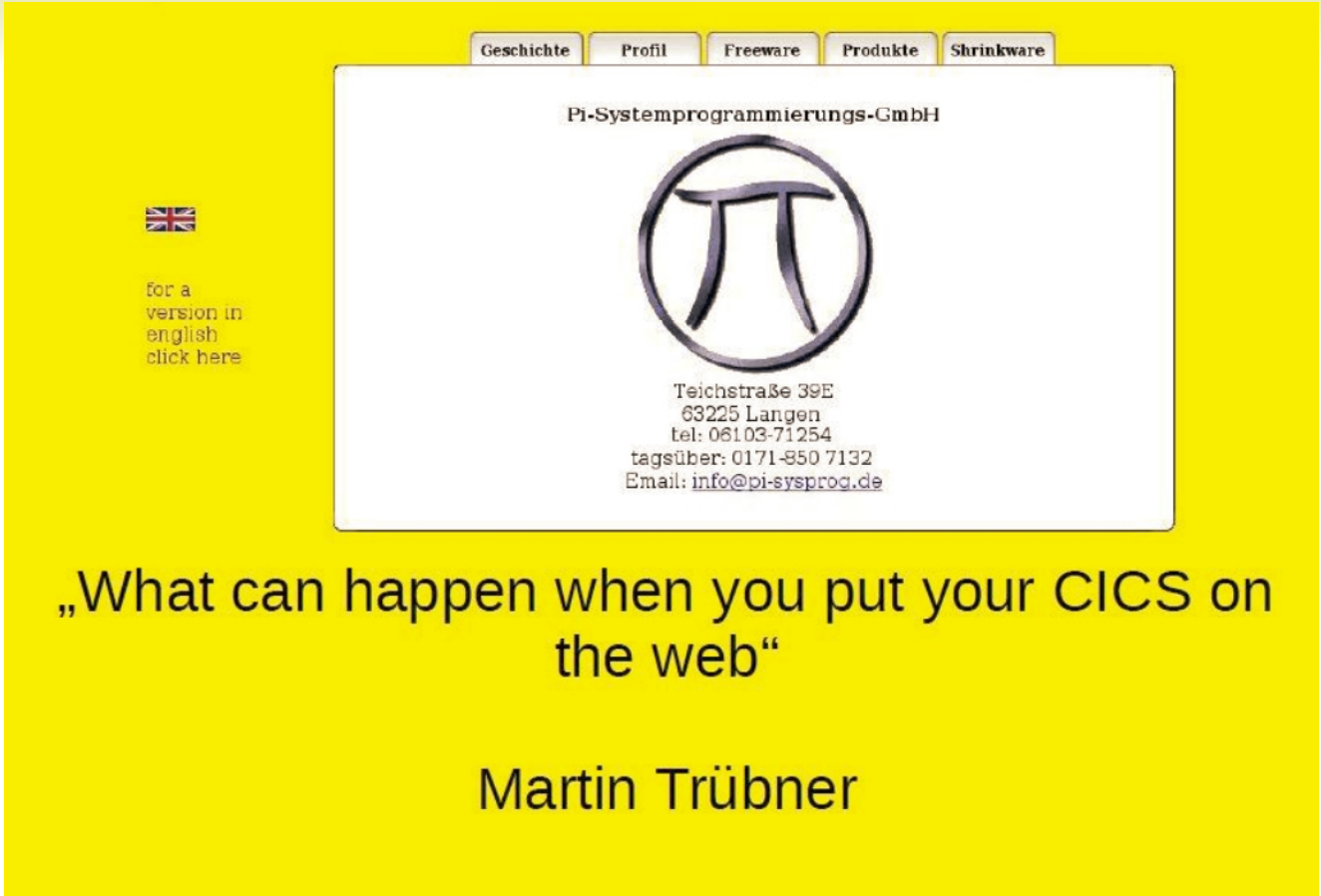
VORTRAG: MARTIN TRÜBNER 2010

Initiator: Martin →

Mal sehen ob es

noch mehr CICS

Websites gibt

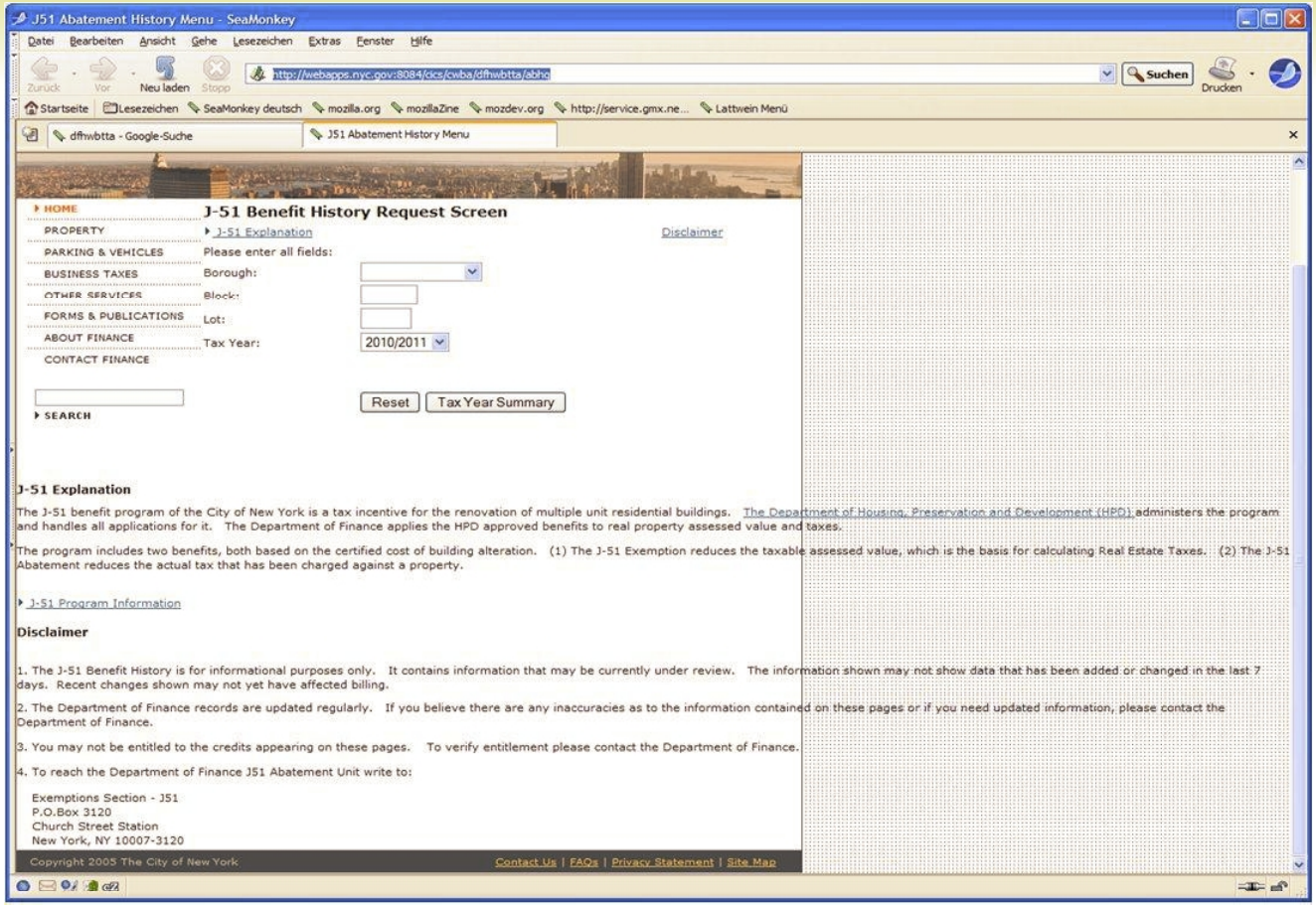


Auf der Suche nach VSE Servern im WWW

Reichlich, wenn man nach CICS/CWBA googelt.

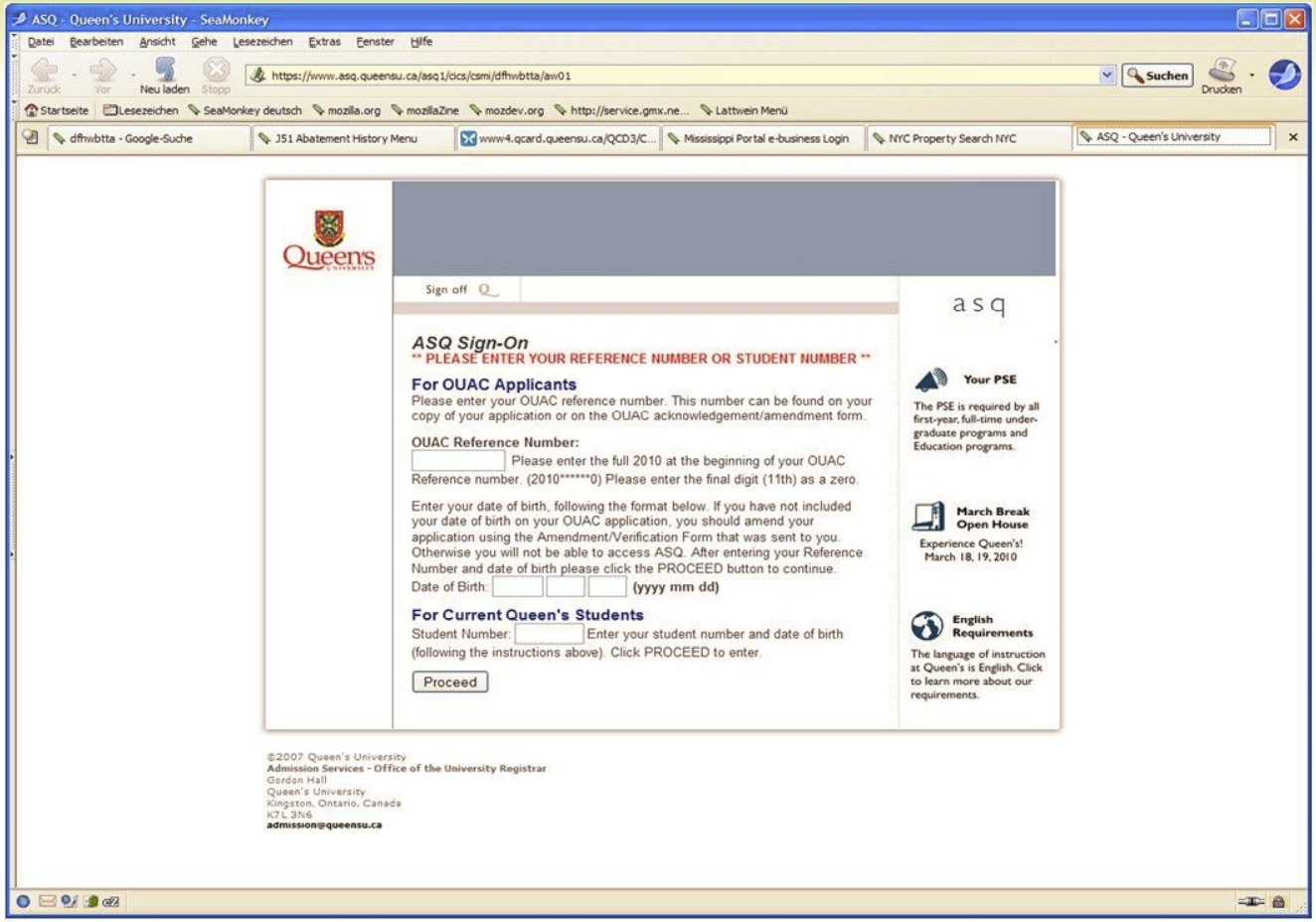
- Nur einige der 106000 Treffer bei CWBA oder 3660 Treffer auf DFHWBTTA
- http://webapps.nyc.gov:8084/cics/cwba/dfhwbtta/abhq
- http://xmarks.com/site/www4.qcard.queensu.ca/QCD3/CICS/CSMI/DFHWBTTA/CW01
- https://www.state.ms.gov/taxtitle/cics/dfhwbtta/TNIQ
- https://accounts.swbno.org:8084/cics/cwba/dfhwbtta/wa00
- https://techmvs.technion.ac.il/cics/CWBA/WGRNSE1?SUB=134065

NY Gov Application

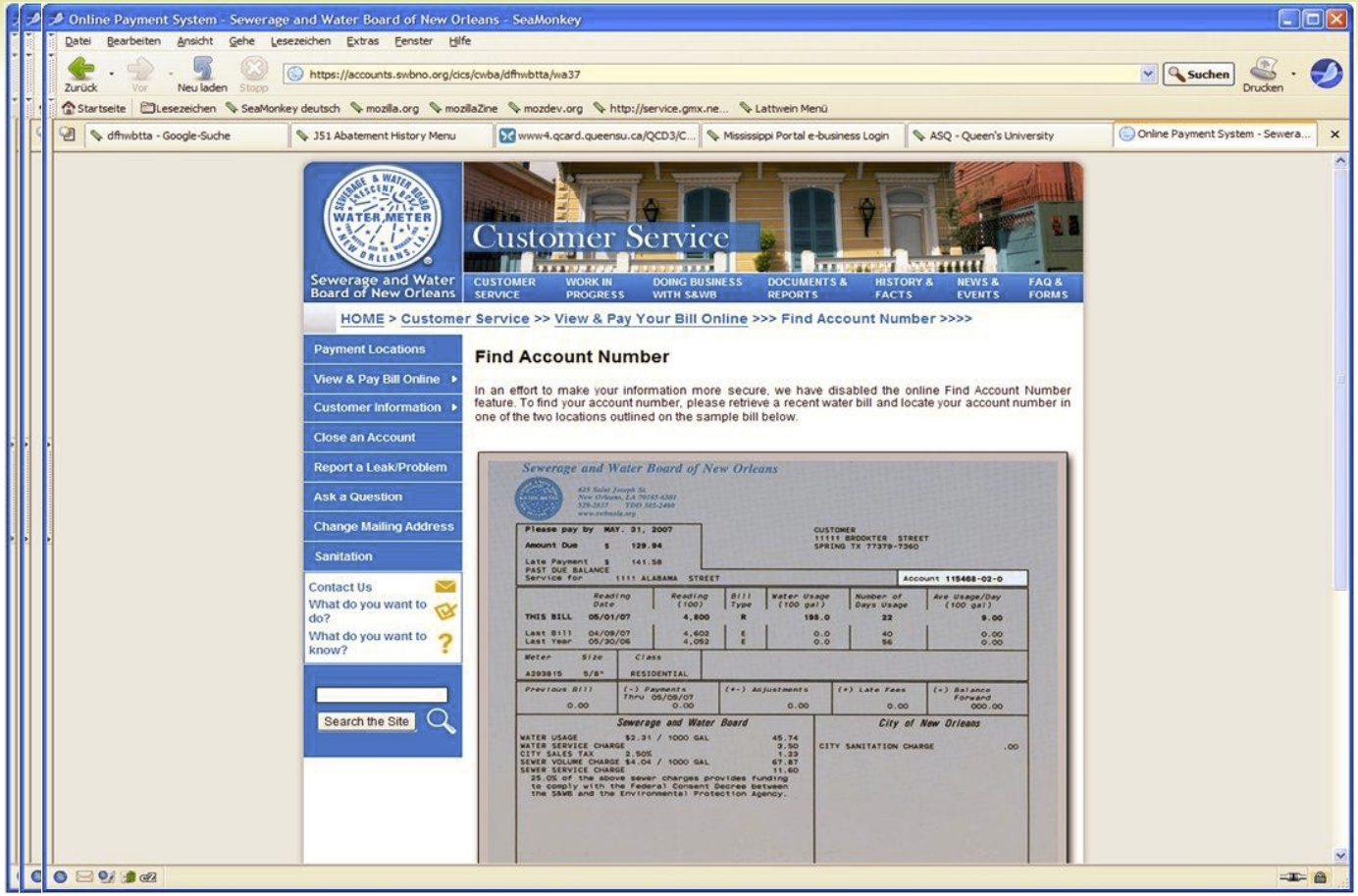


WWW.STATE.MS.GOV

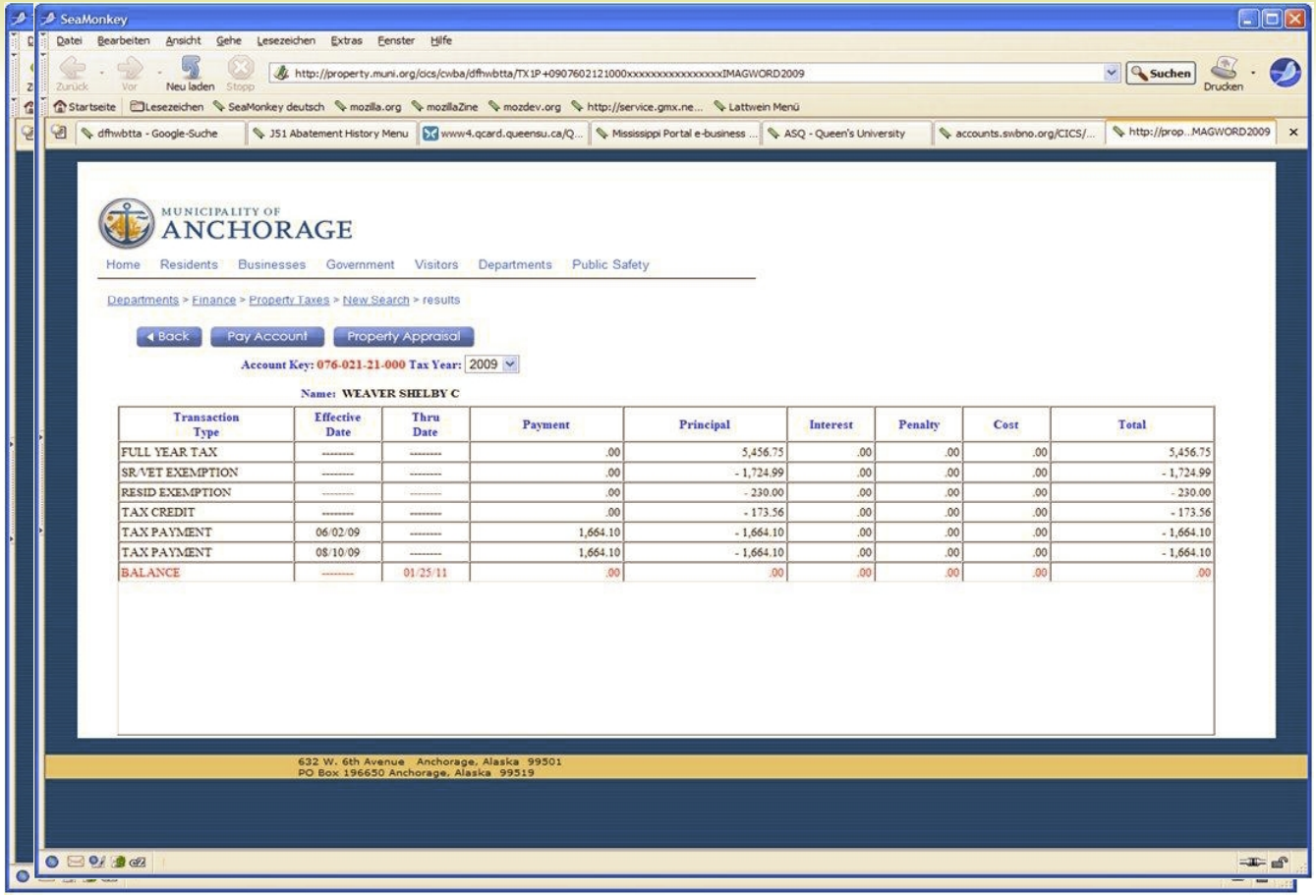
QUEEN UNIVSERSITY CA



NEW ORLEANS: ACCOUNTS.SWBNO.ORG:8010

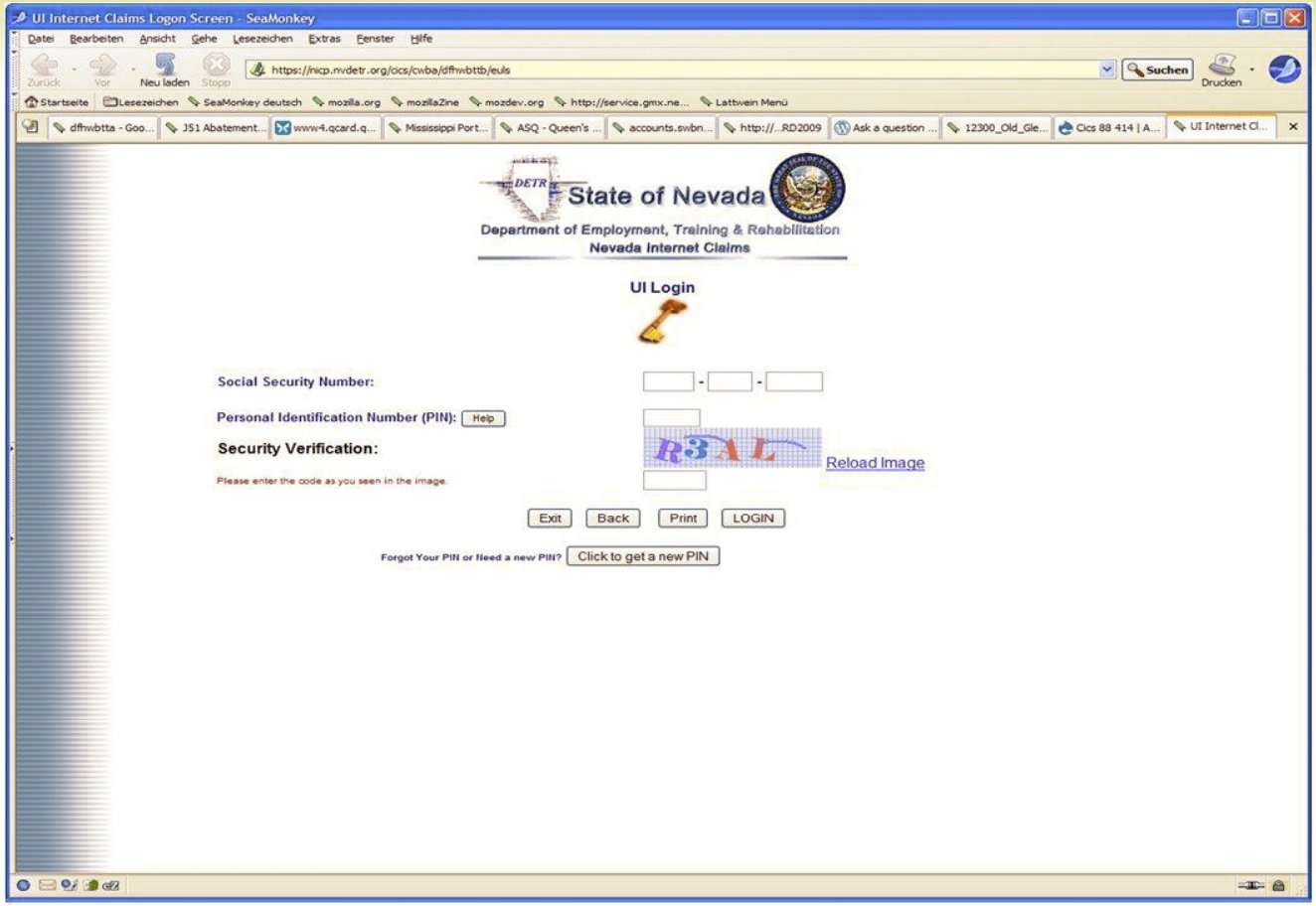


MUNICIPALITY OF ANCHORAGE



Transaction Type	Effective Date	Thru Date	Payment	Principal	Interest	Penalty	Cost	Total
FULL YEAR TAX	--------	--------	.00	5,456.75	.00	.00	.00	5,456.75
SR/VET EXEMPTION	--------	--------	.00	- 1,724.99	.00	.00	.00	- 1,724.99
RESID EXEMPTION	--------	--------	.00	- 230.00	.00	.00	.00	- 230.00
TAX CREDIT	--------	--------	.00	- 173.56	.00	.00	.00	- 173.56
TAX PAYMENT	06/02/09	--------	1,664.10	- 1,664.10	.00	.00	.00	- 1,664.10
TAX PAYMENT	08/10/09	--------	1,664.10	- 1,664.10	.00	.00	.00	- 1,664.10
BALANCE	--------	01/25/11	.00	.00	.00	.00	.00	.00

State of Nevada



Und wie sicher sind unsere Standard Anwendungen

- Auch Inhouse Anwendungen sind nicht sicher!
- Sei es CICS Sign-ON über Telnet
- FTP von oder zum z/VSE
- Email im zVSE versendet

Diese Folien sollen **nicht** dazu auffordern VSE Systeme auszuspionieren.
Sie wollen auf die Gefahren hinweisen, die vorhanden sind.
Obwohl die Verwendung von Traces sowie Wireshark normaler-weise verboten sind- richtet sich auch derjenige sich nicht daran, der ein System ausspionieren will!

WikiPedia

Wireshark (engl. „wire“: Draht, Kabel; „shark“: Hai; alte Bezeichnung: **Ethereal**) ist ein freies Programm zur Analyse von Netzwerk-Kommunikationsverbindungen („Sniffer“).

Telnet Login Data

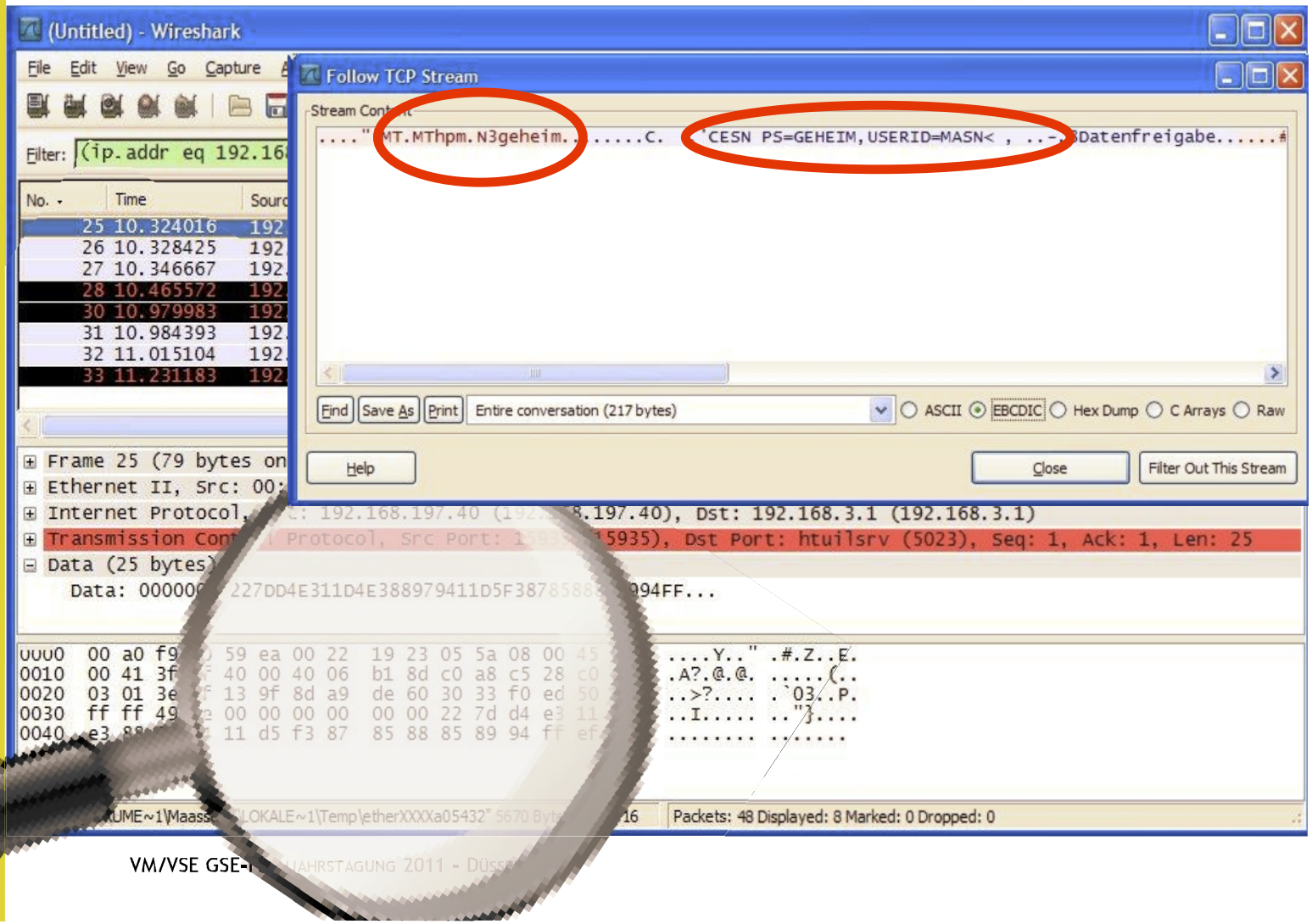
LOGIN über

Benutzer

Programm

Und anschließend

CESN



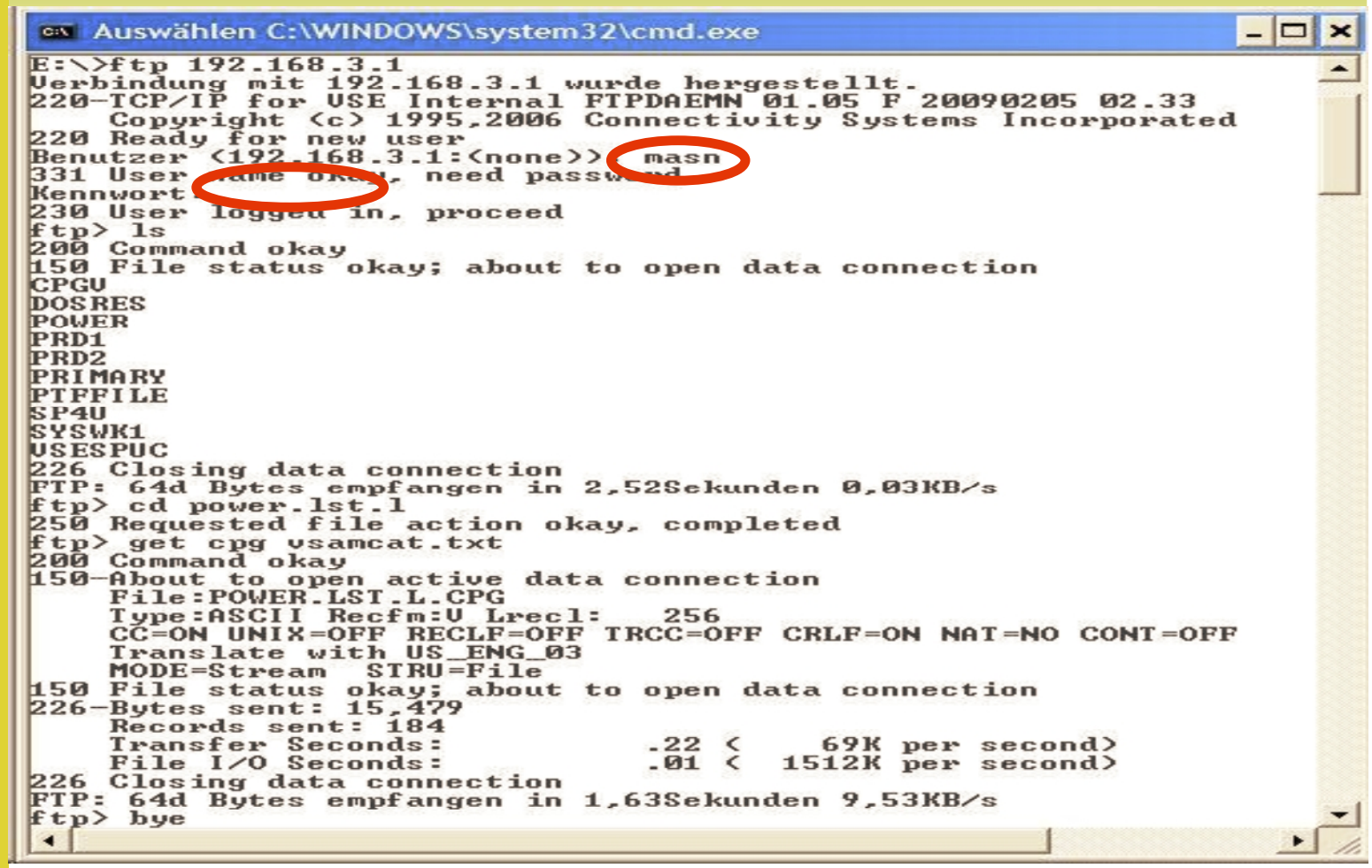
FTP

Command Fenster

mit FTP zum

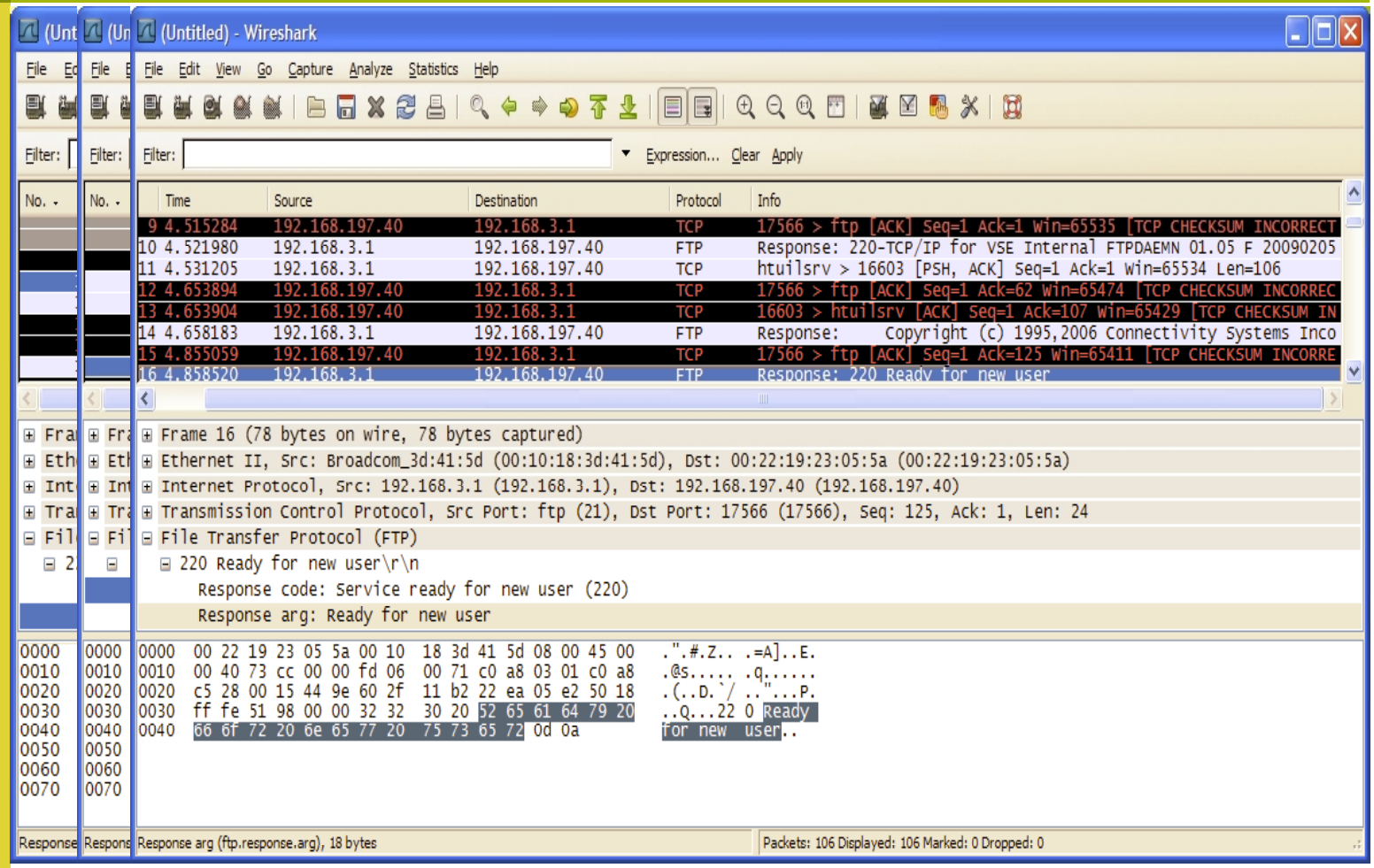
z/VSE.

TCPIP 1.5.F



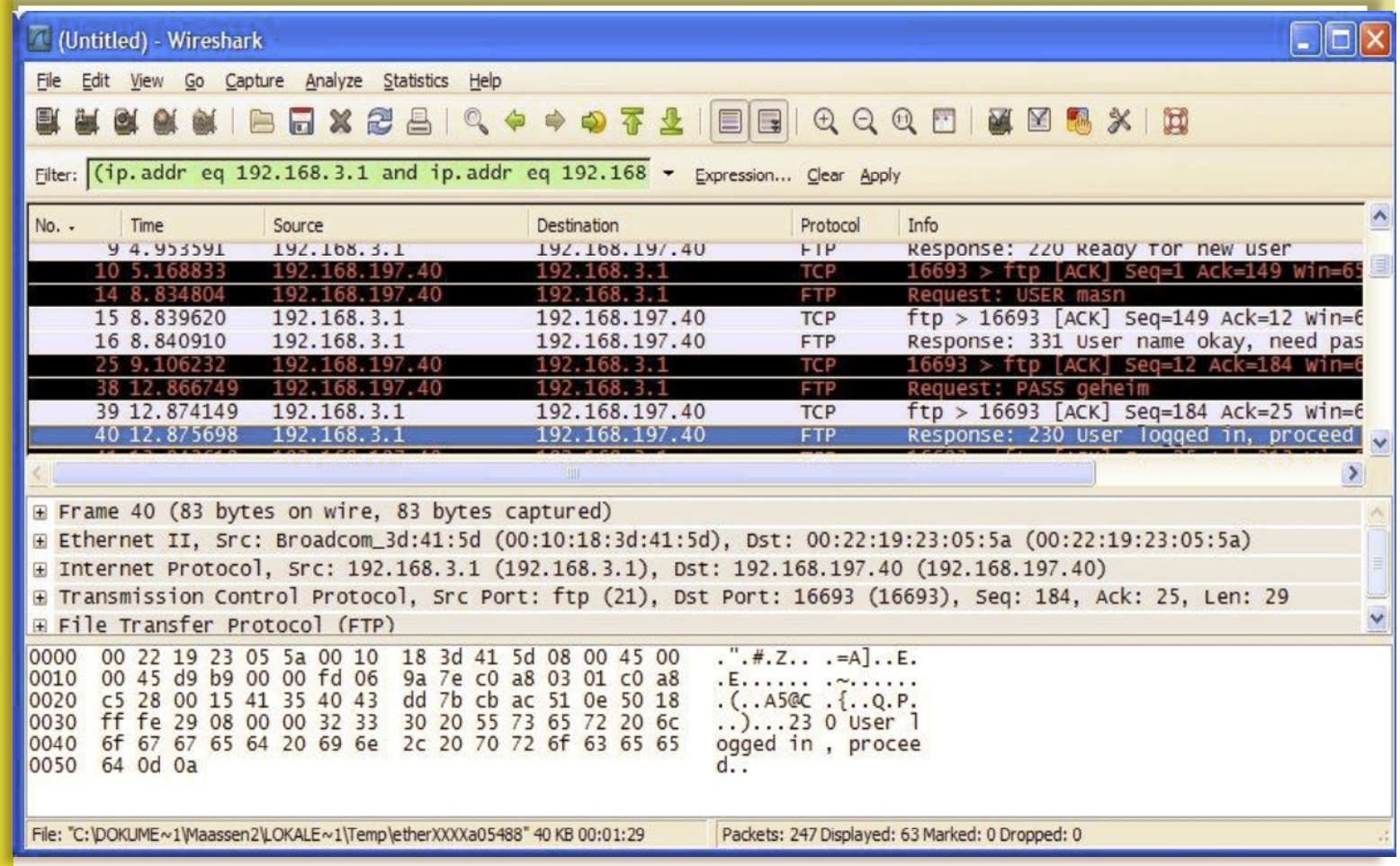
FTP Daemon Response

Im Wireshark sieht man die Konversation vom z/VSE zum Client



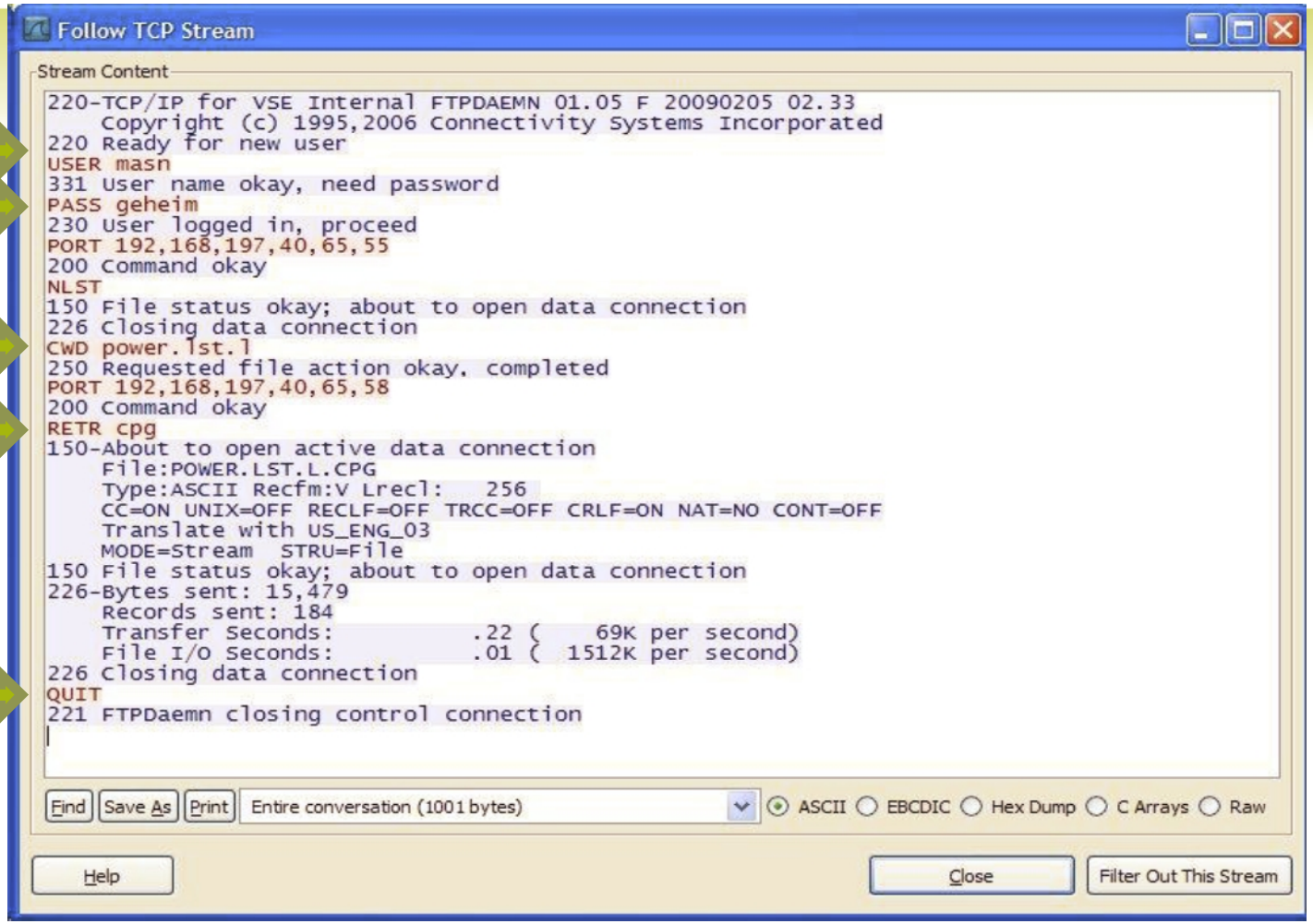
FTP USER MASN

Userid und Passwort im Klartext !



FTP Follow TCP Stream

FTP LS Data



PASSWORT SCHUTZ

Was ein sicheres Passwort ist:

Wa$ 31n 51ch3r3$ Pa5$w0r7 157

Wa$ 31n 51ch3r3$ Pa5$w0r7 157

Wa$ 31n 51ch3r3$ Pa5$wor7 157

Passwörter sind im z/VSE normalerweise nur 8 Stellen lang, es sei Denn man verwendet LDAP Anmeldung- dann bis zu 64 Stellen.

Passwörter sind normalerweise in Uppercase und bestehen aus Buchstaben, Ziffern und Sonderzeichen.

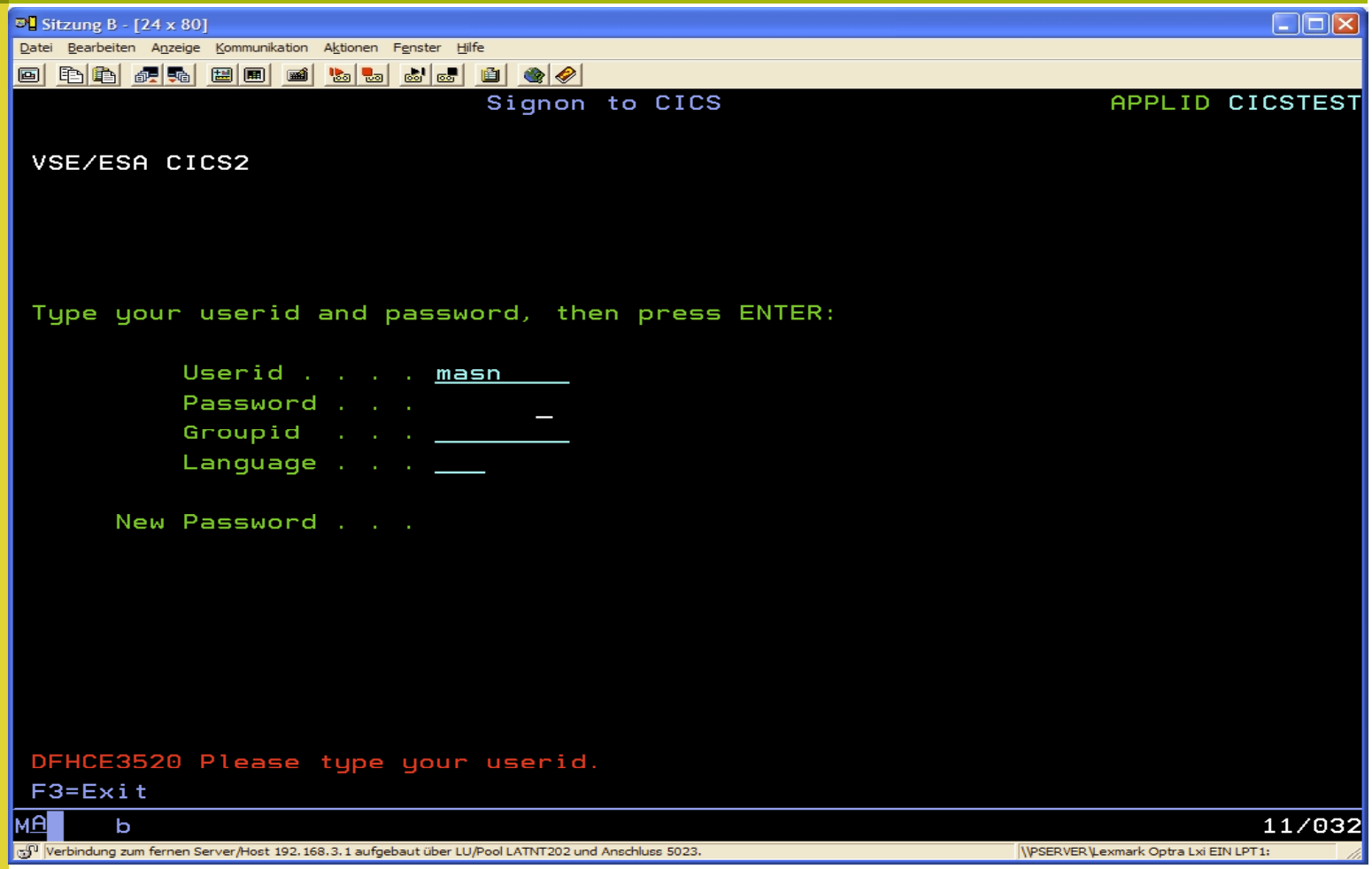
Sind diese denn sicher ?

CESN DATA

CESN:

SignOn to CICS

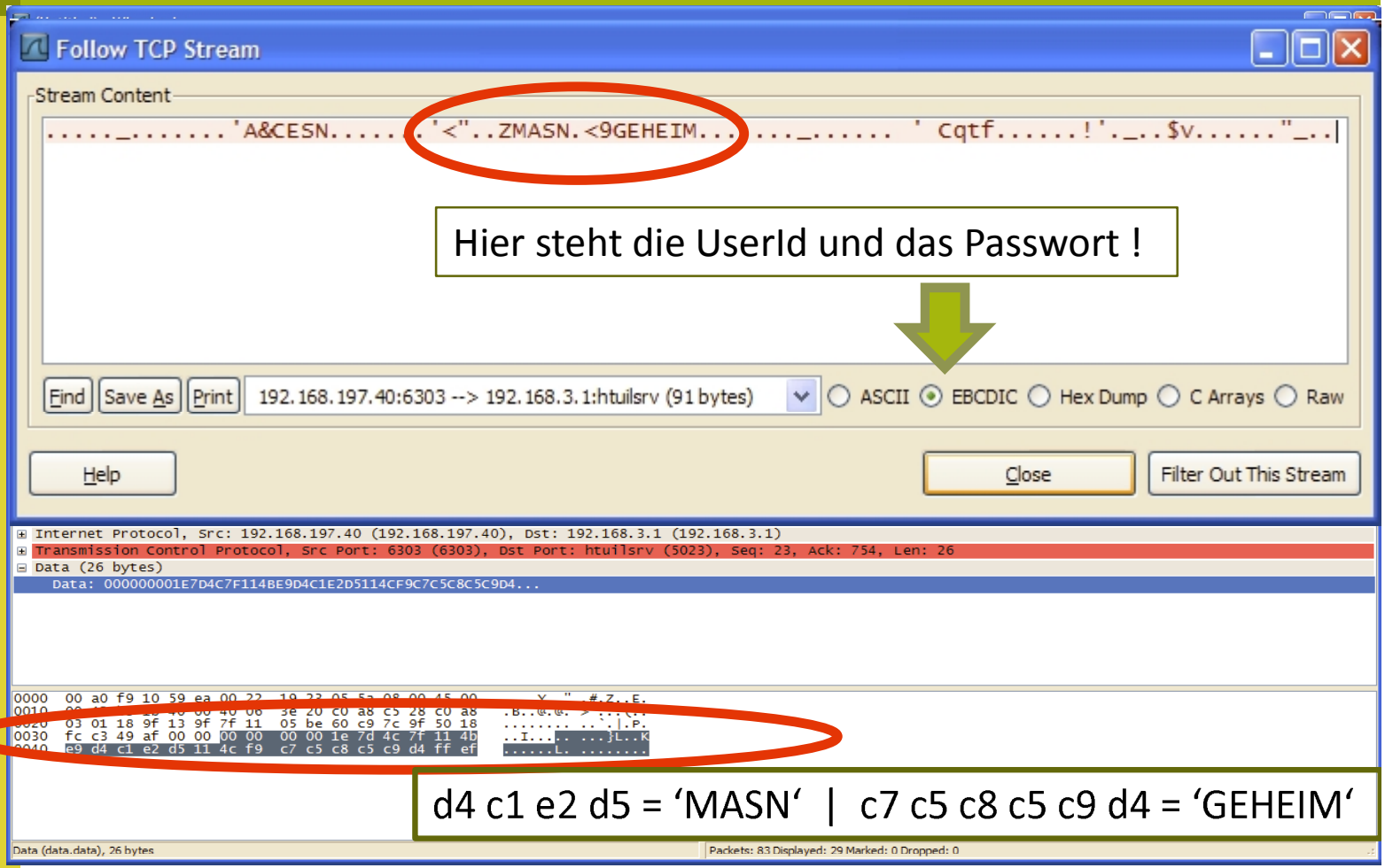
Alles geheim - da keine Anzeige im 3270 erfolgt ?



CESN User/Password

Nicht falls man EBCDIC Hex lesen kann !

Geht aber auch im Klartext . . .



EMAIL IM zVSE TRACE

- Wie bei IPTRACE dokumentiert, kann Email Trafic im VSE aufgezeichnet und anschließend von Wireshark ausgewertet werden.

Dieser Text stammt aus der HTML Dokumentation: ~/doc/ipTraceTool.html

How to take a trace
Enter the following commands on your VSE console:

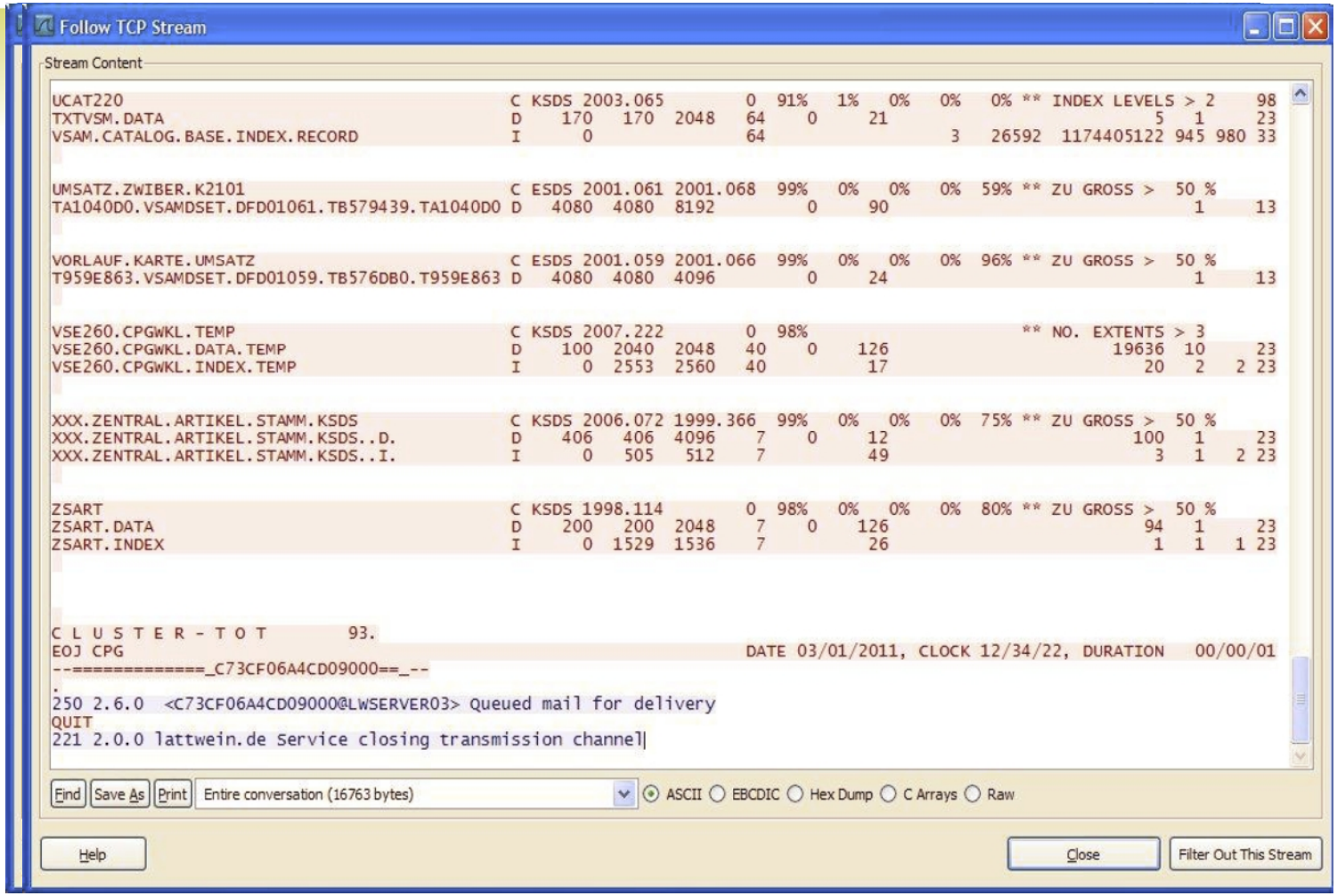
MSG xx (xx = partition ID of target TCP/IP partition)
DEFINE TRACE,ID=xxxx, IPADDR=ipaddr-of-target-system
--> recreate the problem
DUMP TRACES SEGMENT NEW
DELETE TRACE,ID=xxxx
Download the SYSLST output containing the trace data to your PC in ASCII format.
Now you can use the IP Trace Tool to convert and view this trace in Wireshark.

Note: The trace data is taken in the TCP/IP partition GETVIS.

EMAIL NOCH EINFACHER IM KLARTEXT

Email von VSE

mit Anhang



CICS Transaction Dump

Name/

Password

im CICS DUMP

Auch im CICS Transaction DUMP können
UserId‘s und Passwörter im Klartext stehen.

Deshalb Vorsicht, wenn man Dumps weiterreicht oder ausgedruckt jemandem zur Ansicht gibt.

```
TRANSACTION STORAGE-USER24                ADDRESS 00681770 TO 0068276F    LENGTH
00000000   C2F0F0F2 F0F7F9F2 85000000 00000000  000F5DD2 11D4E3C8 D7D411D5 F3C7
00000020   C5C9D400 00000000 00000000 00000000  00000000 00000000 00000000 0000
00000040   00000000 00000000 00000000 00000000  00000000 00000000 00000000 0000
00000060   LINES TO 00000B20 SAME AS ABOVE
```

```
1770 TO 0068276F    LENGTH 00001000
DD2 11D4E3C8 D7D411D5 F3C7C5C8   *B0020792E.........)K.MTHPM.N3GEH*   00681770
000 00000000 00000000 00000000   *EIM.............................*   00681790
000 00000000 00000000 00000000   *.................................*   006817B0
```

Das sind Terminal Input Daten – das kann auch in der Common Area oder in Temporary Storage Records stehen.

CICS Transaction Dump

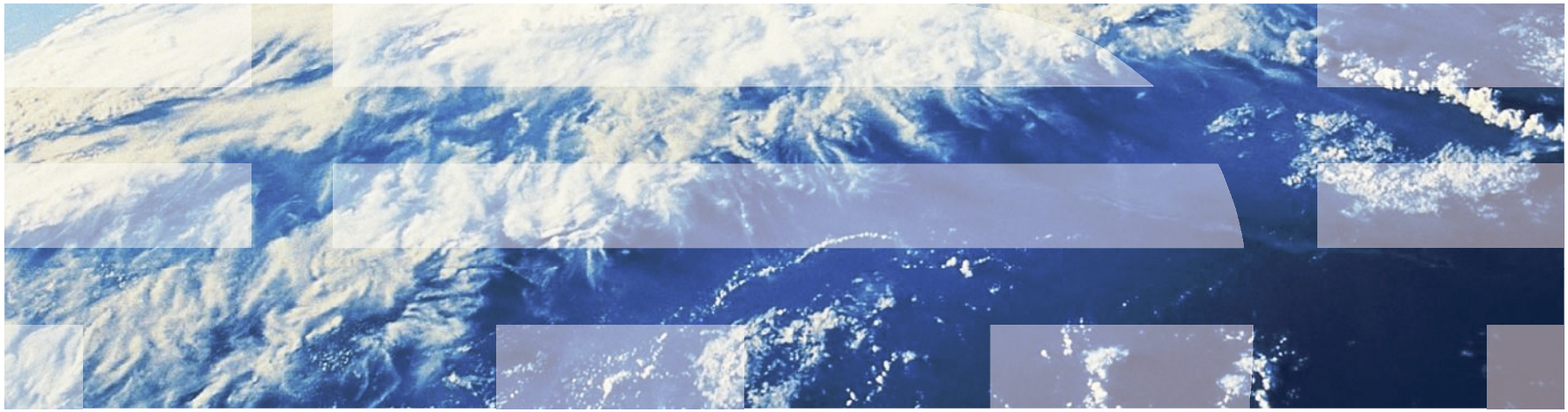
Positiv:

Bei CEDF wird das Password unterdrückt!

- Nur bei CEDF wird das Passwort beim EXEC CICS SIGNON unterdrückt.
- When processing an EXEC CICS SIGNON command, CEDF ***suppresses*** display of the ***password*** value to reduce the risk of accidental disclosure.

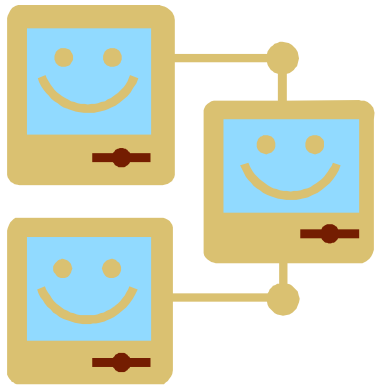
Fortsetzung: Ingo Franzki, IBM – Security Franzki

G05
Gefahren in der IT – Ist Ihre Produktion sicher vor Angriffen?

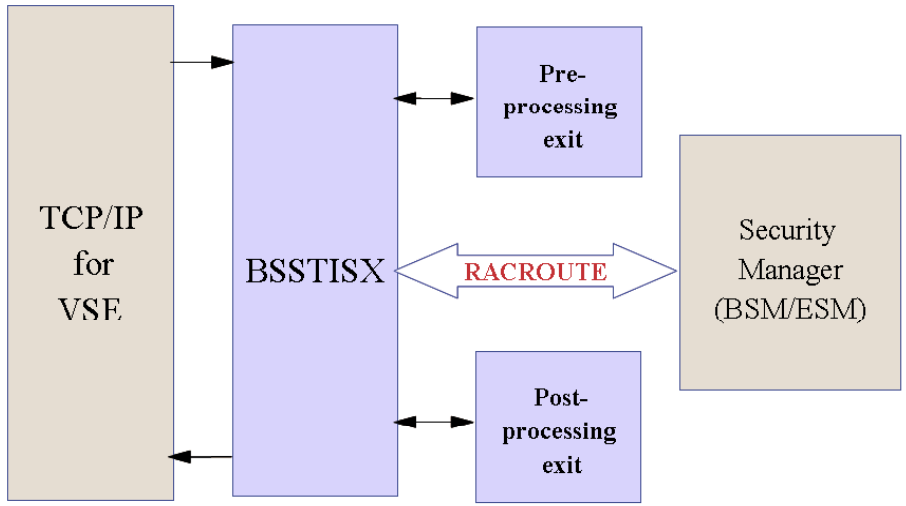


TCP/IP Security

- **In general TCP/IP uses its own user id definitions**
  - Readable in initialization member (IPINITxx.L)
    - **`DEFINE USER,ID=user,PASSWORD=pwd`**
  - Duplicate user definitions

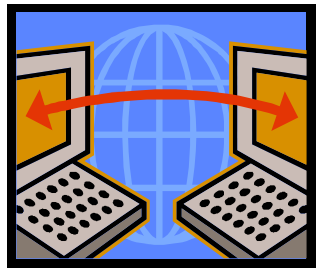


- **Security Exit available from IBM to check the user ids and resource access via Security Manager**
  - Issues RACROUTE calls for
    - User identification and verification
    - Resource access control
    - VSE files, libraries, members
    - POWER entries
    - SITE commands



Cryptography and data encryption

Main areas of cryptography:



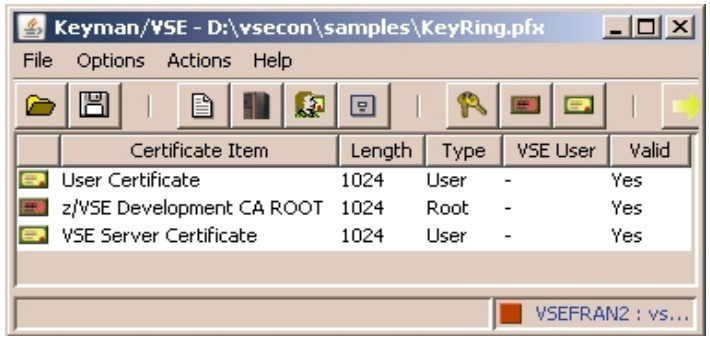
- **Encryption of data transmitted over network connections**
  - SSL, HTTPS
  - SecureFTP, Secure Telnet

- **Encryption of data stored on disk or tape**
  - Encryption of backups or archives
  - Exchange of encrypted and/or signed data with customers or business partners
  - TS1120 Encrypting Tape Drive
  - Encryption Facility for z/VSE

Key & Certificate Management

Cryprography uses Keys and Certificates

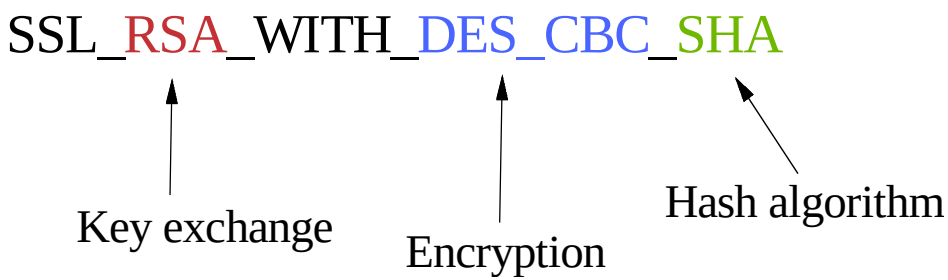
- **Key Management is not trivial**
  - Key must often be kept secure for a very long time
  - You must be able to associate the encrypted data with the corresponding key(s)
  - Encrypted data and the corresponding key(s) must be strictly separated

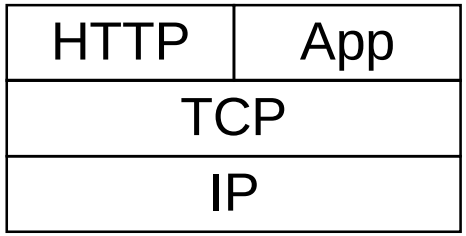


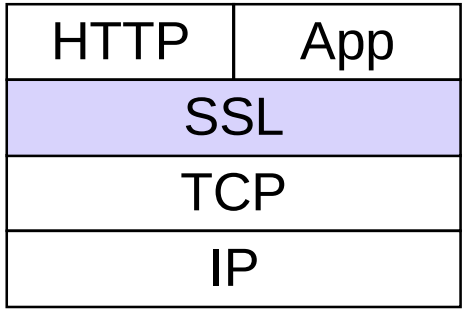
- **Keyman/VSE**
  - Creation of RSA keys and digital certificates
  - Upload of keys and certificates to VSE
  - Creation of PKCS#12 keyring files (use with Java-based connector or import into a Web browser)
  - Download from VSE Homepage http://www.ibm.com/systems/z/os/zvse/downloads/#vkeyman

Secure Socket Layer – Encrypted data transfer over a network

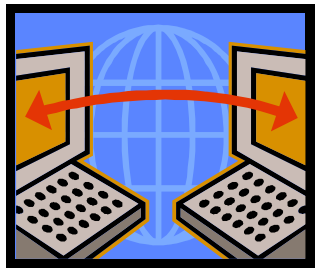
- **SSL provides a communication channel with message integrity, authentication, and confidentiality**
- **SSL is a widely used protocol**
  - Secure HTTP (HTTPS) is used very often in the Internet
- **SSL uses a TCP connection to transfer encrypted messages**
  - Uses asymmetric cryptography for session initiating
  - Uses symmetric cryptography for data encryption
- **As the name implies, SSL is a layer on top of TCP**
- **Cipher suites defines the algorithms used:**
  - For key exchange
  - For encryption
  - For hash algorithm







SecureFTP



- **The FTP protocol provides a easy and straight forward protocol for transferring files between systems on different platforms**
  - Many installations rely on it to efficiently transmit critical files that can contain vital information such as customer names, credit card account numbers, social security numbers, corporate secrets and other sensitive information
  - FTP protocol transmits data without any authentication, privacy or integrity
- **SecureFTP provides user authentication, privacy and integrity by using RSA digitally signed certificates, DES encryption and SHA-1 secure hash functions**
  - SecureFTP is integrated into TCP/IP for VSE with z/VSE V4.1 or later (at no additional charge) or offered as separately priced product by CSI
- **How to setup Secure FTP with VSE:**
  ftp://ftp.software.ibm.com/eserver/zseries/zos/vse/pdf3/How_to_setup_SecureFTP_with_VSE.pdf

Telnet 3270 over SSL

- **Define a TELNETD:**

```
DEFINE TELNETD,ID=LU,TERMNAME=TELNLU,TARGET=DBDCCICS,PORT=992,COUNT=4,
  -
       LOGMODE=S3270,LOGMODE3=D4B32783,LOGMODE4=D4B32784, -
       LOGMODE5=D4B32785,POOL=YES
```

- **Define TLSD:**

```
DEFINE TLSD,ID=TLSDTELNET,          Id of this SSL/TLS daemon
       PORT=992,                    Secure telnet port
       PASSPORT=992,                Port data is passed to
       CIPHER=2F350A0962,           Allowed cipher suites
       CERTLIB=CRYPTO,              Library name
       CERTSUB=KEYRING,             Sublibrary name
       CERTMEM=SECTELN,             Member name
       TYPE=1,                      SSL server authentication
       MINVERS=0300,                Minimum version required
       DRIVER=SSLD                  Driver phase name
```

With the above definition the TELNETD will natively support SSL, but pick up the necessary SSL configuration information from the DEFINE TLSD keywords.

- **How to setup Telnet with VSE:**
  ftp://public.dhe.ibm.com/eserver/zseries/zos/vse/pdf3/How_to_setup_Secure_Telnet_with_VSE.pdf

Hardware Crypto Support on System z and VSE

by release

	z/VSE 4.3	z/VSE 4.2	z/VSE 4.1	z/VSE 3.1	VSE/ESA 2.7	VSE/ESA 2.6
PCICA	Yes	Yes	Yes	Yes	Yes	-
CEX2C	Yes	Yes	Yes	Yes	-	-
CPACF	Yes	Yes	Yes	Yes	-	-
CEX2A	Yes	Yes	Yes	Yes	-	-
PCIXCC	Yes	Yes	Yes	-	-	-

by server

	prior z800	z800	z900	z890	z990	z9	z10	z196
PCICA	-	Yes	Yes	Yes	Yes	-	-	-
PCIXCC	-	-	-	Yes	Yes	-	-	-
CEX2C	-	-	-	Yes	Yes	Yes	Yes	Yes
CPACF	-	-	-	Yes	Yes	Yes	Yes	Yes
CEX2A	-	-	-	-	-	Yes	Yes	Yes

CEX2C = Crypto Express2/3 in coprocessor mode
CEX2A = Crypto Express2/3 in accelerator mode
See: http://www.ibm.com/systems/z/security/cryptography.html

VSE Hardware Configuration

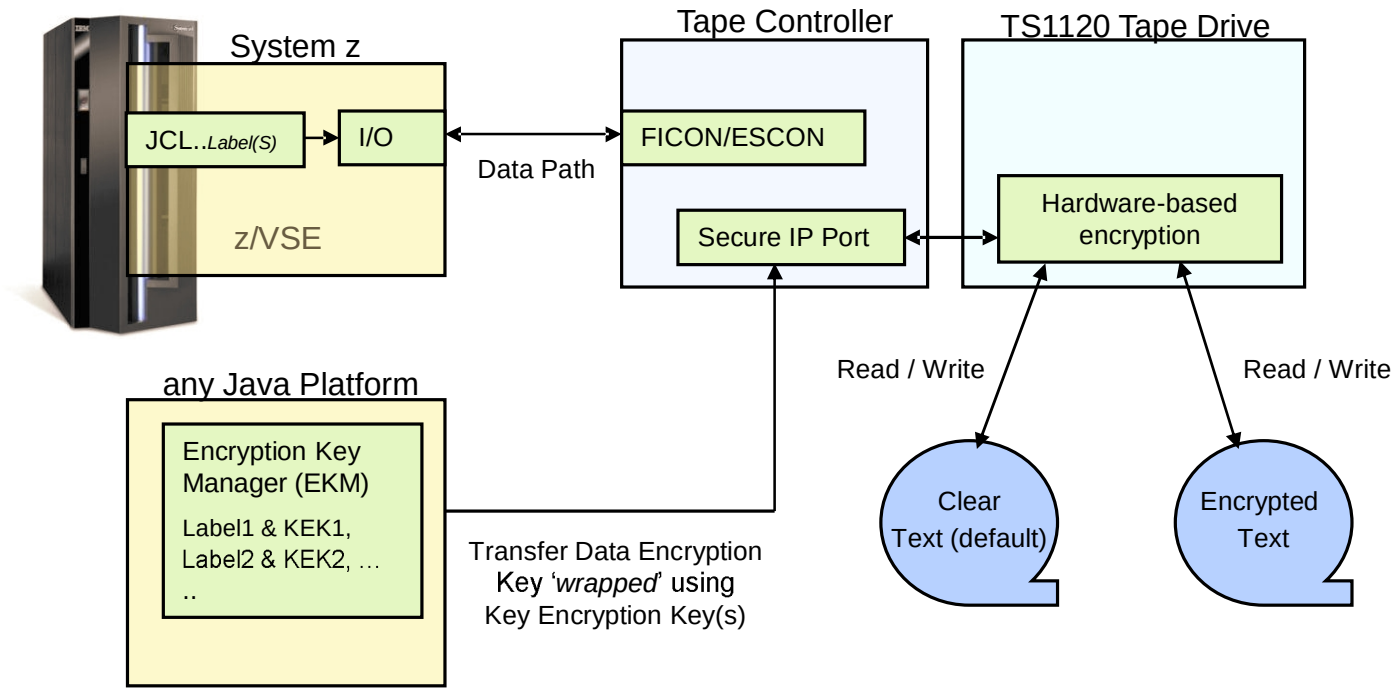
- **VSE hardware configuration not necessary for crypto hardware**
  - No IOCDS definition in VSE
  - No device type
  - No ADD statement
  - You may have to define the devices in the HMC (LPAR) or z/VM directory

- **Use of crypto hardware is transparent to end users and TCP/IP applications**
  - But use of crypto hardware can be disabled via TCP/IP SOCKOPT phase

- **How to setup cryptographic hardware for VSE:**
  - http://www.ibm.com/systems/z/os/zvse/documentation/security.html#howto

```
FB 0095 1J023I FOUND A CRYPTO EXPRESS2 CARD AT DEVICE INDEX 0
FB 0095 1J023I FOUND A CRYPTO EXPRESS2 CARD AT DEVICE INDEX 1
FB 0095 1J014I FOUND A PCICA CARD AT DEVICE INDEX 6
FB 0095 1J014I FOUND A PCICA CARD AT DEVICE INDEX 7
FB 0095 1J005I HARDWARE CRYPTO ENVIRONMENT INITIALIZED SUCCESSFULLY.
FB 0095 1J006I USING CRYPTO DOMAIN 0
FB 0095 1J022I CPU CRYPTOGRAPHIC ASSIST FEATURE AVAILABLE.
```

IBM Tape Encryption – TS1120 & TS1130



encryption mode (03=write)

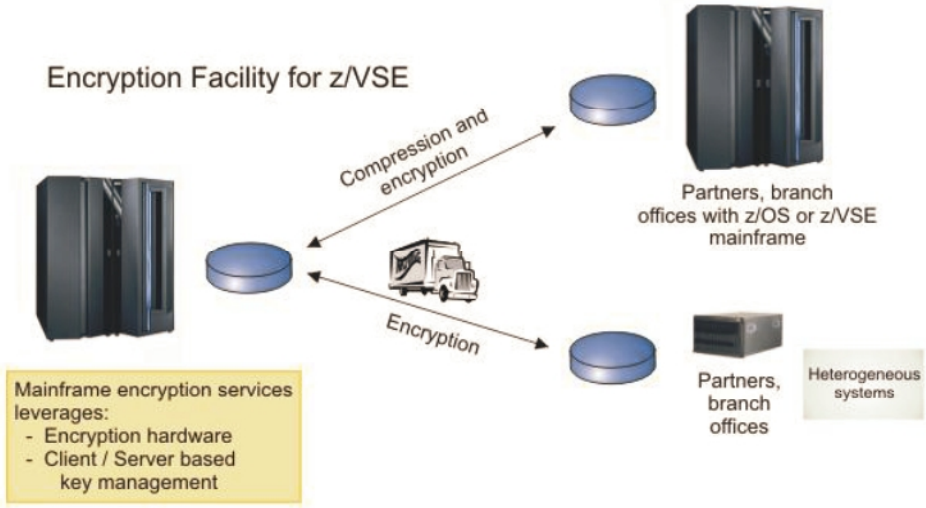
```
// JOB ENCRYPT
// ASSGN SYS005,480,03
// KEKL UNIT=480,KEKL1='MYKEKL1',KEM1=L,KEKL2='MYKEKL2',KEM2=L
// EXEC LIBR
  BACKUP LIB=PRD2 TAPE=SYS005
/*
/&
```

encoding mechanism (L=Label, H=Hash)

key label1 (name of the 1. KEK-key in EKM)

Encryption Facility for z/VSE

- Secure business and customer data
- Address regulatory requirements
- Protect data from loss and inadvertent or deliberate compromise
- Enable sharing of sensitive information across platforms with partners, vendors, and customers
- Enable decrypting and encrypting of data to be exchanged between z/VSE and non-z/VSE platforms



- The Encryption Facility for z/VSE is packaged as an optional, priced feature of VSE Central Functions V8.1 (5686-CF8-40).

- The Encryption Facility for z/VSE V1.1 uses System z data format

- The Encryption Facility for z/VSE V1.2 uses the standard OpenPGP data format
  - PGP stands for „Pretty Good Privacy“, invented by Phil Zimmermann in 1991
  - Open Standard, decribed in RFCs 2440 and 4880
  - Compatible with Encryption Facility for z/OS V1.2 and many other OpenPGP implementations

New technical articles on VSE homepage

http://www.ibm.com/systems/z/os/zvse/documentation/security.html#howto

How to setup hardware crypto with VSE

How to setup SSL with the VSE Script Connector (PDF, 900KB)
Updated: January 2010
Joerg Schmidbauer, IBM

How to setup WebSphere MQ for z/VSE V3.0 and WebSphere MQ for Windows V7.0 with secured connections using SSL (PDF, 3.0MB)
Updated: March 2009
Joerg Schmidbauer, IBM

How to use Encryption Facility for z/VSE (PDF, 380KB)
Updated: June 2010
Joerg Schmidbauer, IBM

How to setup SSL with CICS Web Support (PDF, 1.5MB)
Updated: May 2009
Joerg Schmidbauer, IBM

How to setup Secure Telnet with VSE (PDF, 1.7MB)
Updated: January 2010
Joerg Schmidbauer, IBM

How to setup Secure FTP with VSE (PDF, 1.2MB)
Updated: August 2009
Joerg Schmidbauer, IBM

How to setup SSL with VSE (PDF, 810KB)
New: August 2009
Joerg Schmidbauer, IBM

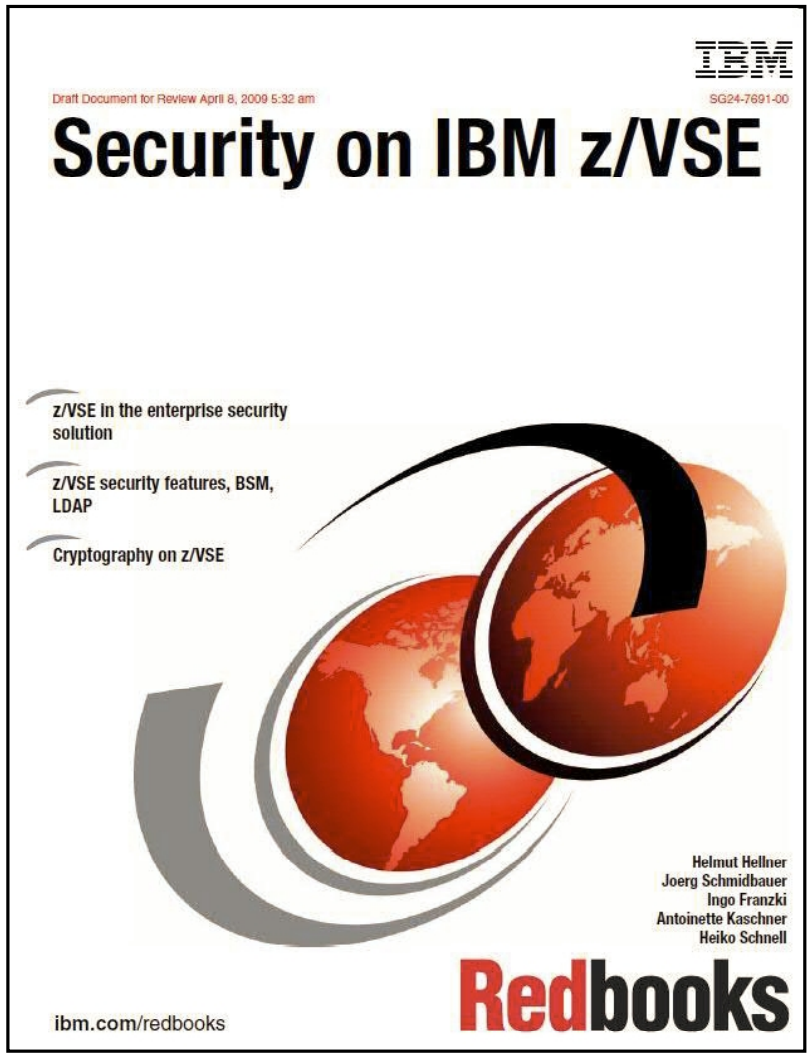
How to setup cryptographic hardware for VSE (PDF, 1.4MB)
Updated: December 2008
Joerg Schmidbauer, IBM

New Redbook: Security on IBM z/VSE - SG24-7691

Available since October 20, 2009
http://www.redbooks.ibm.com/redpieces/abstracts/sg247691.html

Explains security concepts as well as step by step setup

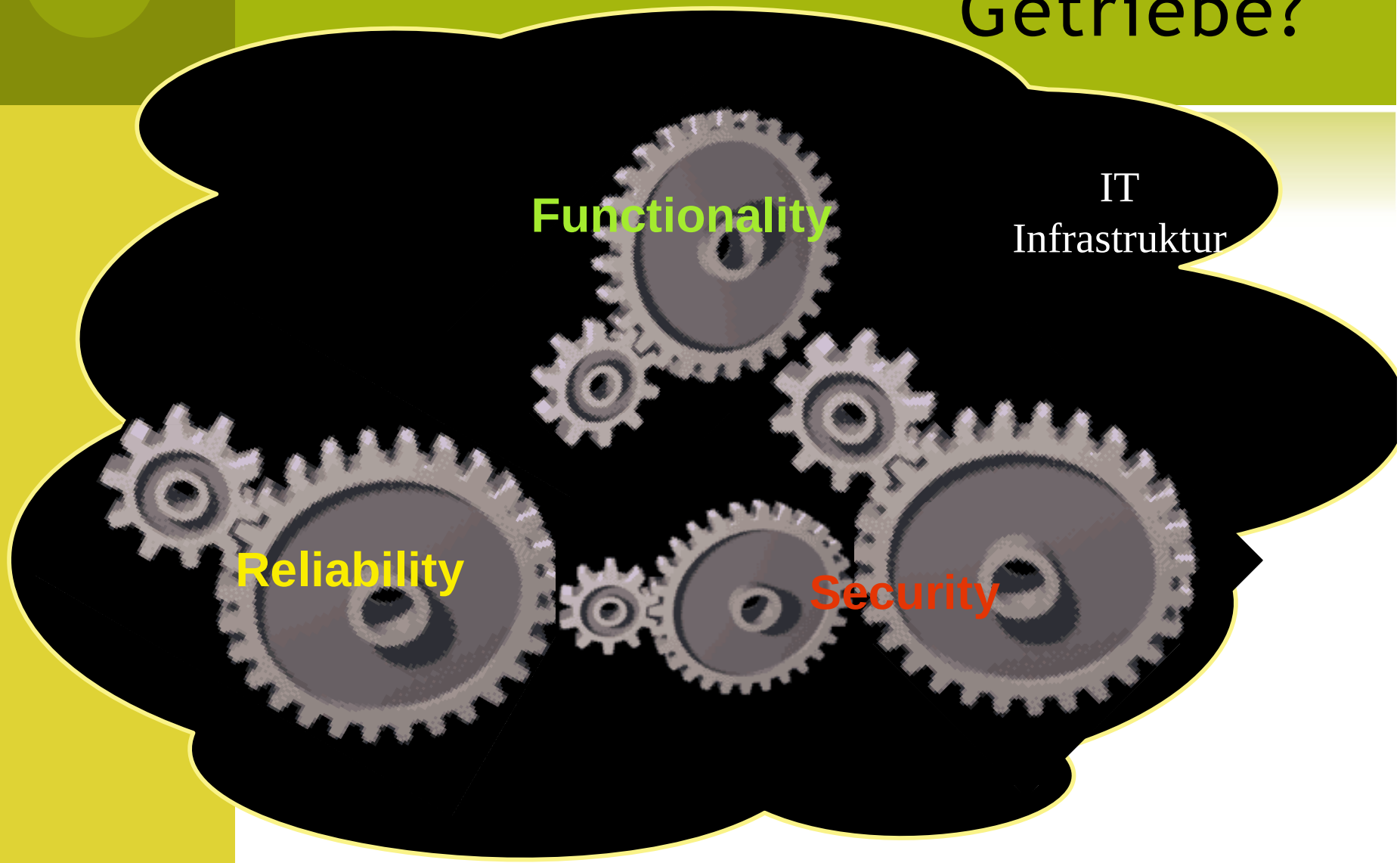
It covers:
- Basic Security Manager
- LDAP Authentication
- Cryptography & SSL
- TCP/IP Security
- SecureFTP & Secure telnet
- CICS Web Support Security
- Connector Security
- Security APIs



Questions ?

Fortsetzung Dr. Manfred Gnirss, IBM Security zVM

Sicherheit: Sand im Getriebe?



No Security by Obscurity

- Philosophie
- Open Source ? Closed Source ?
  - Algorithmen und Verfahren bekannt
  - Implementierung
- Vertrauen und Garantie
- Kontrolle (Auditfähigkeit, 4 Augen)

Und eine “Security Policy” gehört zwingend dazu

Linux auf System z

- Als Server per se nicht besser oder schlechter, nur weil es auf System z läuft.
- Muss gehärtet werden
  - Standardvorgehen
  - SELinux, AppArmor, . . .
- Kann HW Crypto von System z nutzen

z/VM

Für Anwendungen oder als Hypervisor für z/VSE, Linux oder z/OS

- Muss abgesichtert werden
  - Zugang (Netz, Passwörter)
  - Vermeide z.B. maint/maint !!!
  - Rechte und Privilege classes: sparsamer Umgang
- Unterschiedliche Security Zones innerhalb eines z/VM sind sicher realisierbar
  - Beachte Admin- und Organisationsaspekte
- RACF?

Danke für Ihre Aufmerksamkeit

Anhang

Sicherheit – wichtig(st)e Aspekte

Kunden

und

Nutzer

tragen

Verantwortung.

- Define Security Policy
- Implement Secure Solution to meet policy
- Ensure Secure Configuration
- Patch Management Strategy/Execution
- Secure Administration
- Client Policy Enforcement
- User Training
- Ensure adequate physical security
- Disaster preparedness & recovery plans
- Personnel recruitment and separation strategies
- Automated tools to help user community

Sicherheit – Härten eines Linux Servers

Kunden

und

Nutzer

tragen

Verantwortung.

Hier ein paar

ausgewählte

HOWTO - Aspekte

- Patch/upgrade strategy
- Set UID/Set GID programs
- Limit privileged accounts – superuser
- Password policy
- Unused services/ports – turn them off
- Insecure services – use secure version
- Intelligent and secure logging – "over-applied/under-utilized"
- Secure configuration
- Applications security – vulnerable CGI programs, buffer overflows
- Kernel security – patches, specialized kernels, LSMs,.....
  - Industry (LIDS, SELinux, Owl,.....)
  - Commercial (Pitbull, HPLX, Immunix, Engarde, Trustix,.....)
- Use of tools – 100s of tools available
  - Nmap, ethereal, snort, port sentry, nessus, saint, sara, tripwire,.....

Weitere Informationen

- z/VM Security resources
  http://www.VM.ibm.com/security
- IBM Redbook “Security on z/VM”
  http://www.redbooks.ibm.com/abstracts/sg247471.html?Open
- System z Security
  http://www.ibm.com/systems/z/advantages/security/
- z/VM Home Page
  http://www.vm.ibm.com
- IBM Redbook “Security for Linux on System z”
  http://www.redbooks.ibm.com/abstracts/sg247728.html?Open
- Using Hardware Cryptographic Support With OpenSSH in Linux on System z
  http://www.mainframezone.com/it-management/using-hardware-cryptographic-support-with-openssh-in-linux-on-system-z
- First experiences with hardware cryptographic support for OpenSSH with Linux for System z
  http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP101690

Weitere Informationen …

- Rob van der Heij, Running Linux Guest in less than CP Privilege Class G
  http://www.redbooks.ibm.com/abstracts/redp3870.html?Open
- BSI IT-Grundschutz-Kataloge (früher bis 2005: Grundschutzhandbuch)
  - Kap M4.212 Absicherung von Linux für zSeries, B3.102 Server unter Unix, B3.204 Client unter Unix
    https://www.bsi.bund.de/ContentBSI/grundschutz/kataloge/kataloge.html
- Mit Suchmaschine suche im web
  - nach “securing” oder “hardening” und “Linux” liefert genügend Material, z.B.:
    http://www.puschitz.com/SecuringLinux.shtml
  - oder nach “Linux” und “Security” und “HOWTO”
    liefert ebenfalls genügend Material, z.B.:
    http://www.linuxsecurity.com/component/option,com_howto/doc,Security-HOWTO/