# Production Security for Linux, z/VM and z/VSE

## Are you sure, not being attacked via the internet?

5th European GSE / IBM Technical University for
z/VSE, z/VM and Linux on System z

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

# AGENDA

Agenda :

E-Mail

Telnet

FTP

HTTP Servers using z/VSE

- Allround No-Worry ?
- Are all IT information data secure/protected ?
- Danger for attacks on System z platforms
- Protect your data - how IBM can help us protecting System z platforms

# The latest news 27.4.2011 / 12.10.2011

Computer 03.05.2011
**Sony: Weitere Millionen Kundendaten geklaut**
Auch Sony Online Entertainment gehackt

Computer 08.05.2011
**Die gehackte Branche**
Nach dem Sony-Datenklau herrscht Nervosität

Computer 03.06.2011
**Hacker vermelden neuen Angriff auf Sony**
Angeblich sensible Nutzerdaten geklaut

Computer 12.10.2011
**Neuer Hacker-Angriff auf Sony**
Wieder knacken Unbekannte Passwörter und Kundennummern

Computer 01.05.2011
**Sony entschuldigt sich für Sicherheitslücken**
Konzern bietet einige Dienste für Nutzer kostenlos an

Volle Kanne 05.05.2011
**So wenig wie möglich preisgeben**
Nach dem Sony-Hack: Wie sicher sind meine Daten?

Computer 27.04.2011
**PlayStation Network: Hacker klauen 77 Millionen Kundendaten**
Sony sperrt Online-Dienste - Racheakt aus der Szene?

Computer 07.06.2011
**E3: Neue Konsolen und eine Xbox, mit der man reden kann**
Messe in Los Angeles präsentiert Innovationen von Nintendo, Microsoft und Sony

Computer 21.06.2011
**Neues Hacker-Bündnis zielt auf Regierungsdaten**
Anonymous und LulzSec verbrüdern sich - London meldet Festnahme

Computer 27.04.2011
**"Hacker-Attacke hat gewaltige Ausmaße"**
Internetsicherheitsexperte im heute.de-Interview

ZDF.de | Programm | heute-Nachrichten | Sport | Wetter | ZDFmediathek | Inhalt | Suche in ZDF.de

ZDF.de Startseite / heute-Nachrichten / Computer — 13. Oktober 2011

heute.de computer

heute-Nachrichten
- Startseite
- Schlagzeilen
- Politik
- Magazin
- Wirtschaft
- Computer
- Sport
- Wetter
- Börse

ZDFmediathek
Sendung verpasst?
Jetzt ansehen
- ZDF heute
- ZDF heute journal
- ZDF heute nacht

Sendungen von A-Z

Service
- Podcast-Angebot
- heute-Telegramm

## Neuer Hacker-Angriff auf Sony

### Wieder knacken Unbekannte Passwörter und Kundennummern

dpa

Der japanische Elektronikriese Sony ist erneut Ziel eines Hackerangriffs geworden. In rund 93.000 Fällen hätten Unbekannte Kundennummern und Passwörter von Onlineportalen geknackt, teilte der Konzern mit. Kreditkartendaten seien nicht in Gefahr.

Drucken | Versenden — 12.10.2011

MEDIATHEK


Video Nur sichere Passwörter bieten Schutz

Die Konten der Online-Netzwerke seien in der Zeit vom 7. bis 10. Oktober Ziel des Hackerangriffs gewesen, teilte Sony mit. Die betroffenen Kunden würden informiert und aufgefordert, ihr Passwort zu ändern. Betroffen von dem Hackerangriff seien verschiedene Netzwerke wie das "Playstation Network", das "Sony Entertainment Network" und das Onlinespiele-Netzwerk "Sony Online Entertainment." Viele Menschen nutzen dasselbe Passwort bei verschiedenen Online-Diensten. Das ist gefährlich - werden die Schutzmaßnahmen bei einer Firma geknackt, sind auch die anderen Nutzerkonten in Gefahr.

### Erst im April im Visier von Hackern

Erst im April war Sony Opfer eines Hackerangriffs geworden. Dabei waren sensible Daten von weltweit etwa 100 Millionen Kunden des "Playstation

ZDFmediathek
- Video Datensicherheit im Netz
- Video Hacker stehlen Daten von Sony-Kunden
- Video Hacker testen Technik-Grenzen
- Video USA: Datenklau im Pentagon
- Video Britische Zeitung hört Handys ab
- Video Haftstrafen für Promi-Hacker
- Video Nationales Cyber-Abwehrzentrum eröffnet
- Video Nur sichere Passwörter bieten Schutz

zur ZDFmediathek

# E-MAIL AND ENCRYPTION



- Electronic Mails = E-Mails do not have an envelope - they are like a postcard.
- Anybody can read when looking at it.
- Even at the site of your provider the contents of E-Mails can be stored and scanned via a program.
- Also it may be possible to take a copy for later use or analysis.

# E-MAIL AND ENCRYPTION



- Today E-Mails are used instead of letters, telegram, and telefax.
- The first E-Mail in Germany – was received by Michael Rotert from the university of Karlsruhe dated on August , 24  1984.
- 2010 there have been about 107 billion E-Mails sent (90 % SPAM).
- Today the protocol used is SMTP for sending and POP3 or IMAP for receiving E-Mails.

# E-MAIL AND ENCRYPTION



- When sending E-Mails to the mail server, the protocol used is mostly done via SMTPS (secured) encrypted.
- If mails are received from the mail servers, the protocol used is secured POP3S or IMAPS.
- But what happens in the servers – the mails are not encrypted and readable for anybody.
- This is true, not only for the body, but also for the attachments.

# E-MAIL AND ENCRYPTION



- Most attacks against companies are done from inside
- Nobody knows the way, an E-Mail takes to cross the internet, and nobody can tell you where copies of your mails are stored and can be read.
- Even by passing an hacker, the mail can be modified and the contents can be changed, so it gets another sense.

# E-MAIL AND ENCRYPTION



- Very good reasons to use E-Mails encryption.

  But -

**Why does nobody use encryption?**

# E-MAIL AND ENCRYPTION

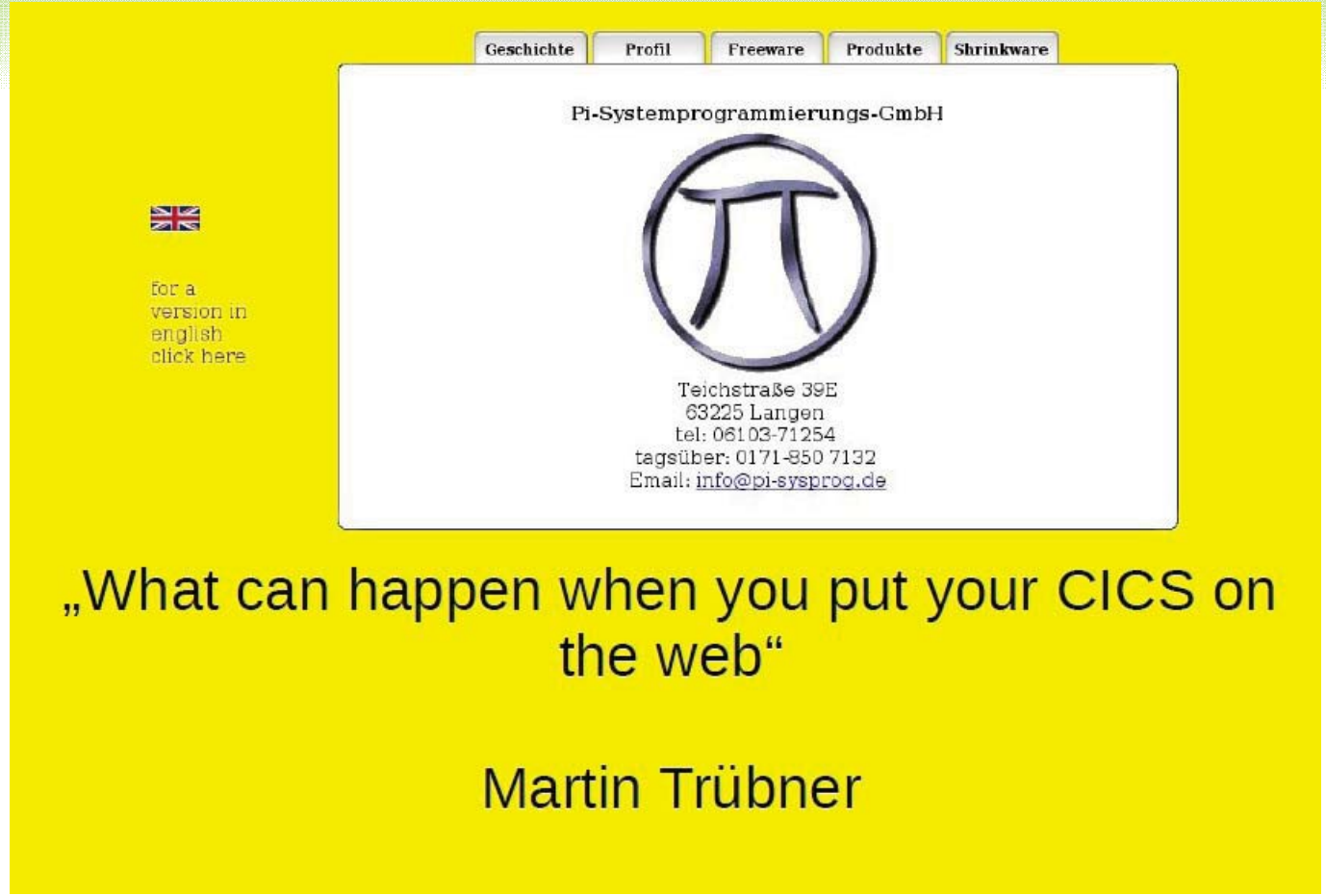


- Actual nearly all E-Mail applications can handle encryption for mails and attachments.
- The only task is to generate public and private keys – and using Add-Ons to enable encryption.
- But there may be different methods by each E-Mail application how to use encryption.

# Session VS04 Munich: MARTIN TRÜBNER 2010

Initiator: Martin →

Let us have a look at the internet where another z/VSE exists !



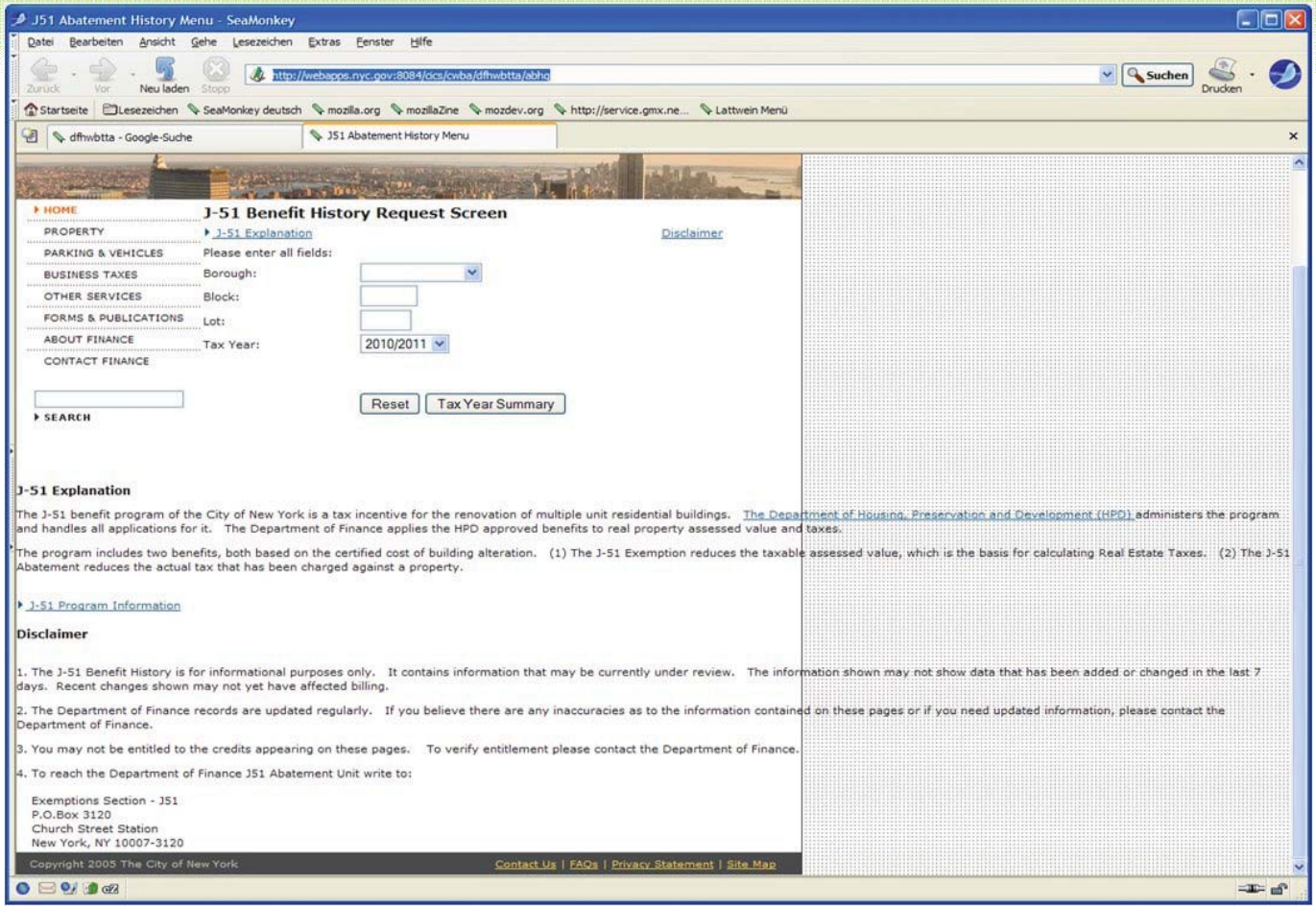
# Let us google for z/VSE Servers in www

There are many websites as result, if you Google for the Eye catchers CICS/CWBA

- Only some of 106,000 hits on CWBA or 3660 hits for 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

Samples of web sites using z/VSE or z/OS

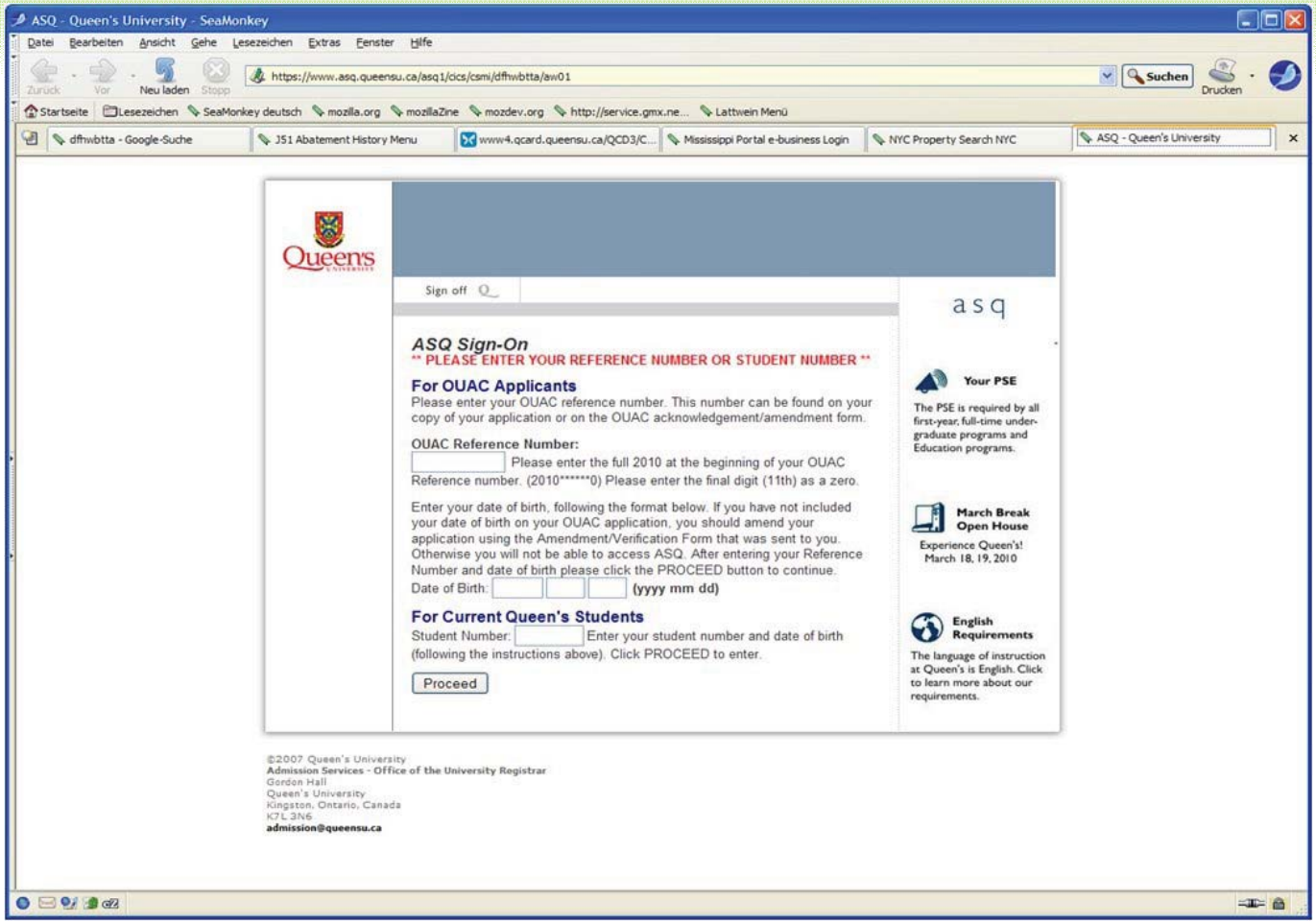


# WWW.STATE.MS.GOV

Samples of web sites using z/VSE or z/OS

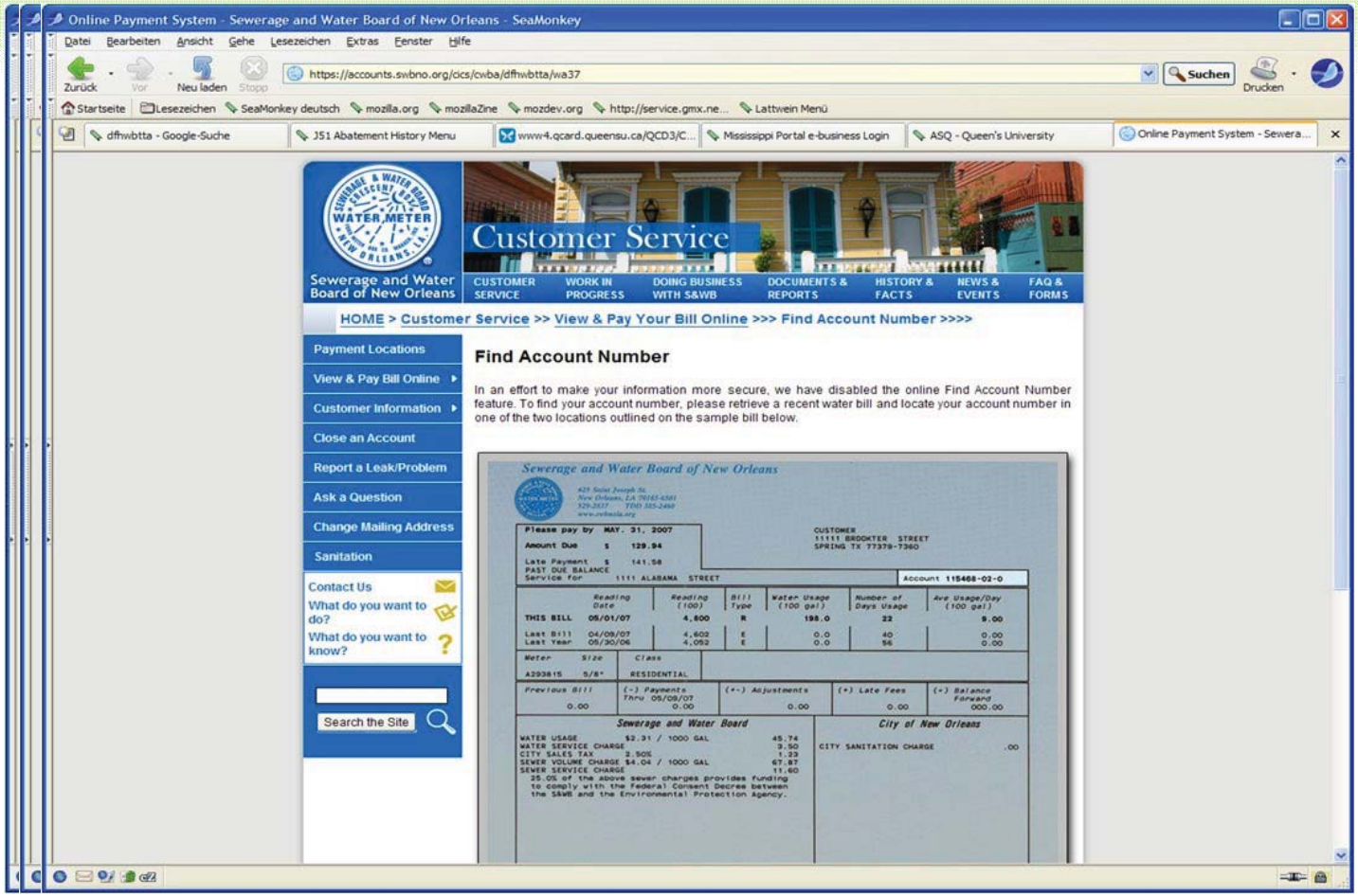
# QUEEN UNIVSERSITY CA

Samples of web sites using z/VSE or z/OS



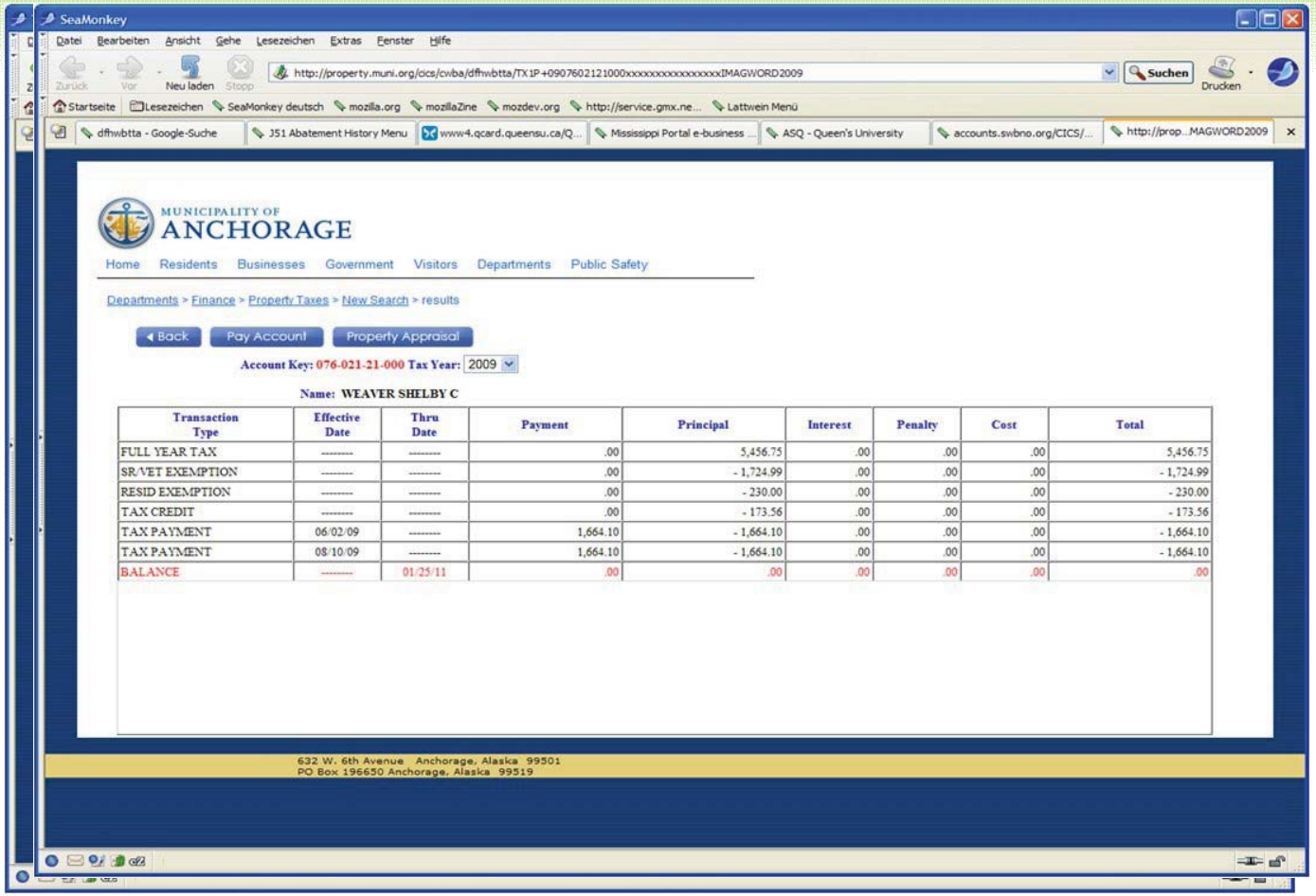
# NEW ORLEANS: ACCOUNTS.SWBNO.ORG:8010

Samples of web sites using z/VSE or z/OS



# MUNICIPALITY OF ANCHORAGE

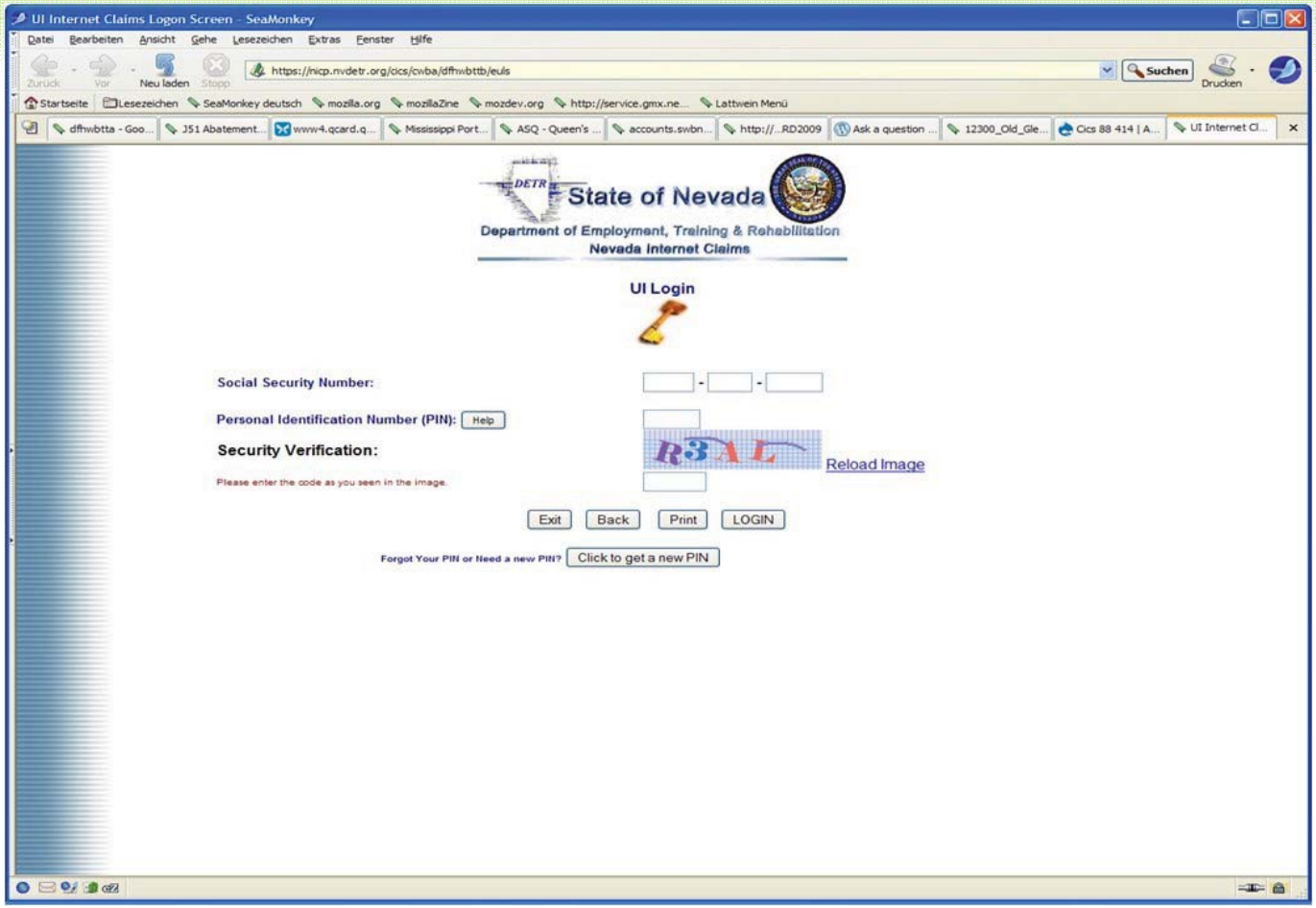
Samples of web sites using z/VSE or z/OS




| 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

Samples of web sites using z/VSE or z/OS



# What‘s about security when using standard applications?

- But even Inhouse applications seem to be unsecure!
- Using CICS Sign-ON via Telnet
- FTP to or from z/VSE
- E-Mails generated with z/VSE

These follies are not created to be a spy in a z/VSE System. This should show the dangers for being attacked with mainframes in a network. Although the using of network traces, like Wireshark, should be forbidden for business networks, but does a hacker use your rules ???

WikiPedia

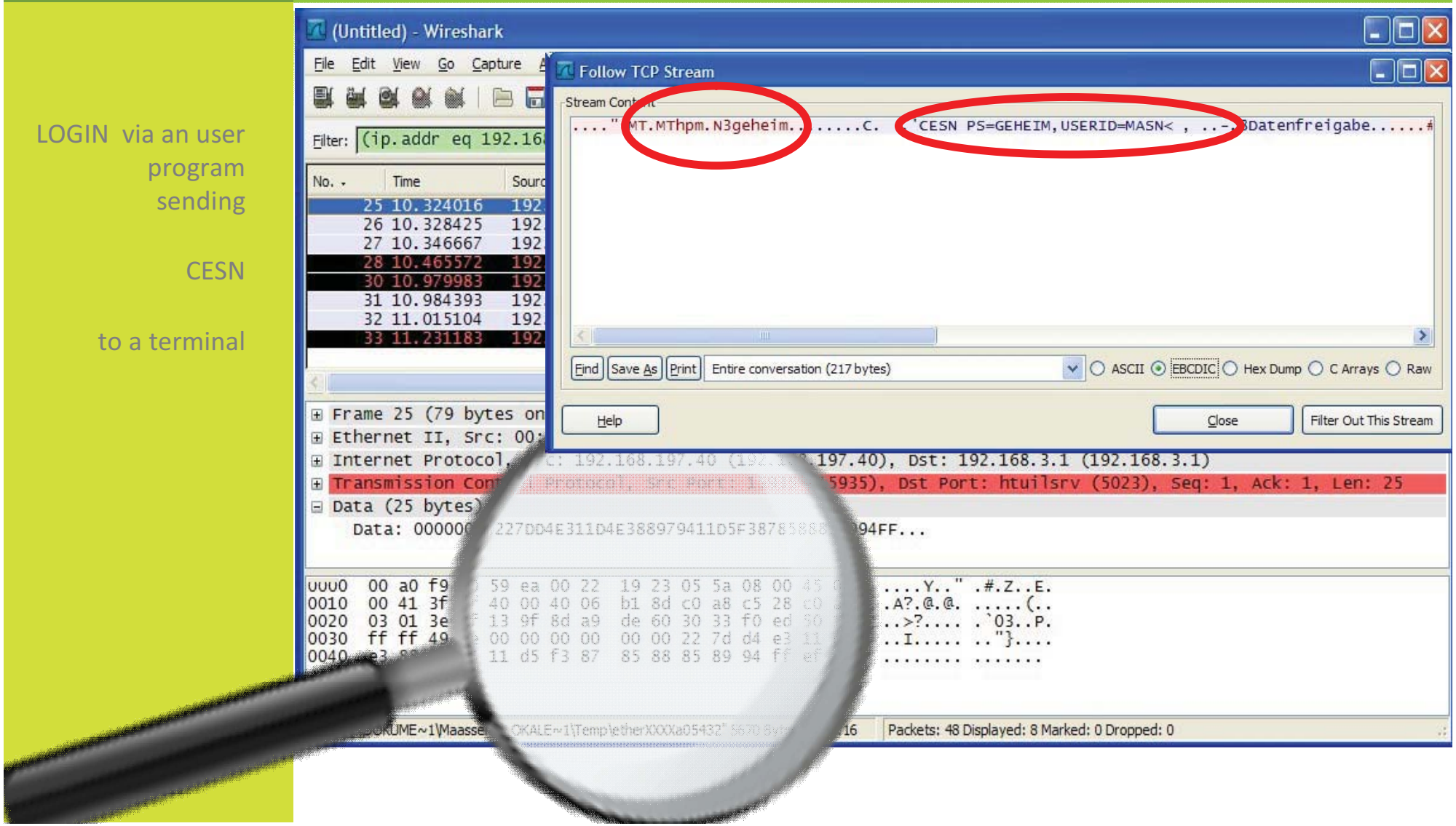
Wireshark is a free and open-source packet analyzer. It is used for network trouble-shooting, analysis, software and communications protocol development, and education. („Sniffer“).

# TELNET LOGIN DATA

LOGIN via an user program sending

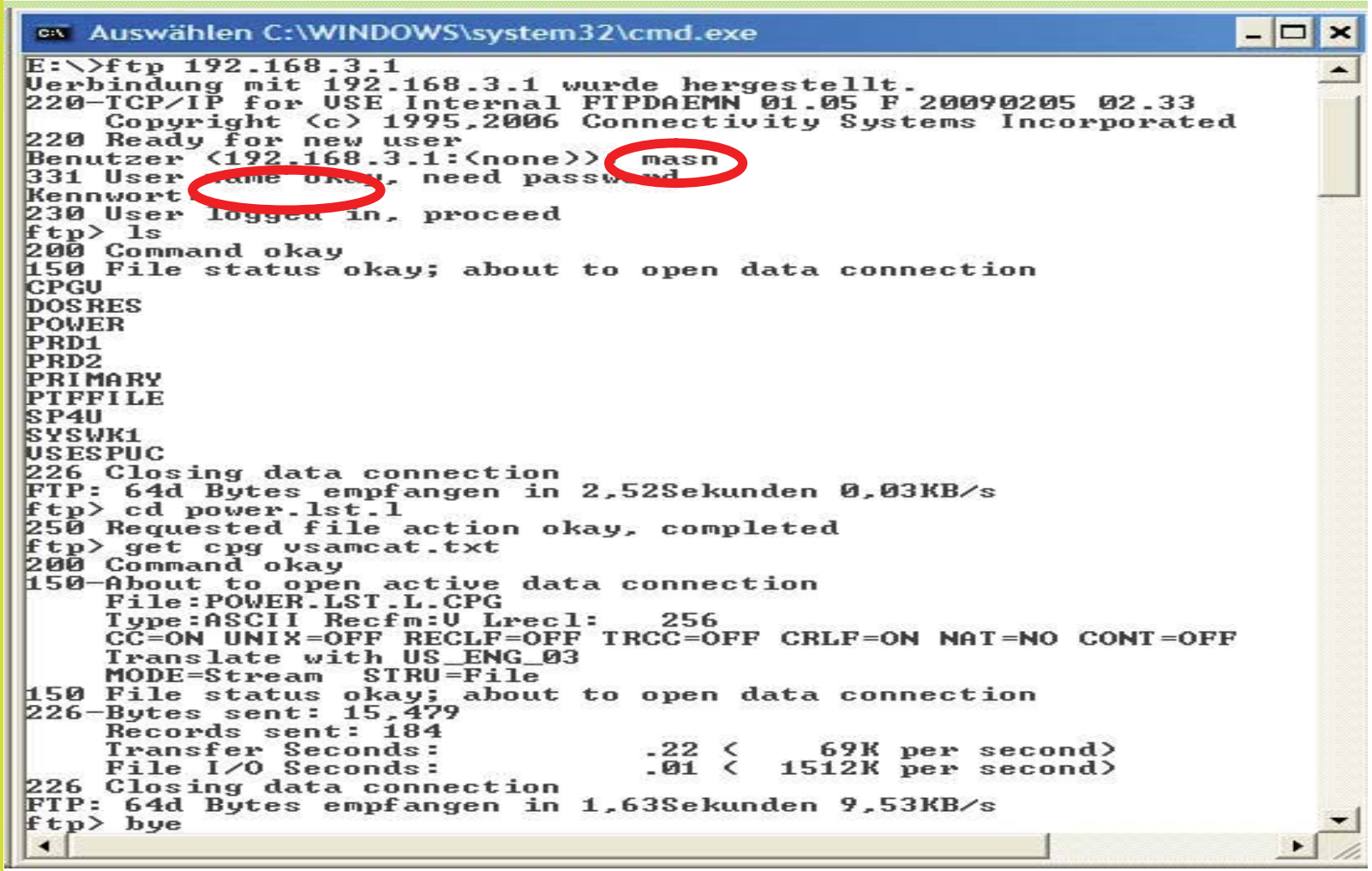
CESN

to a terminal



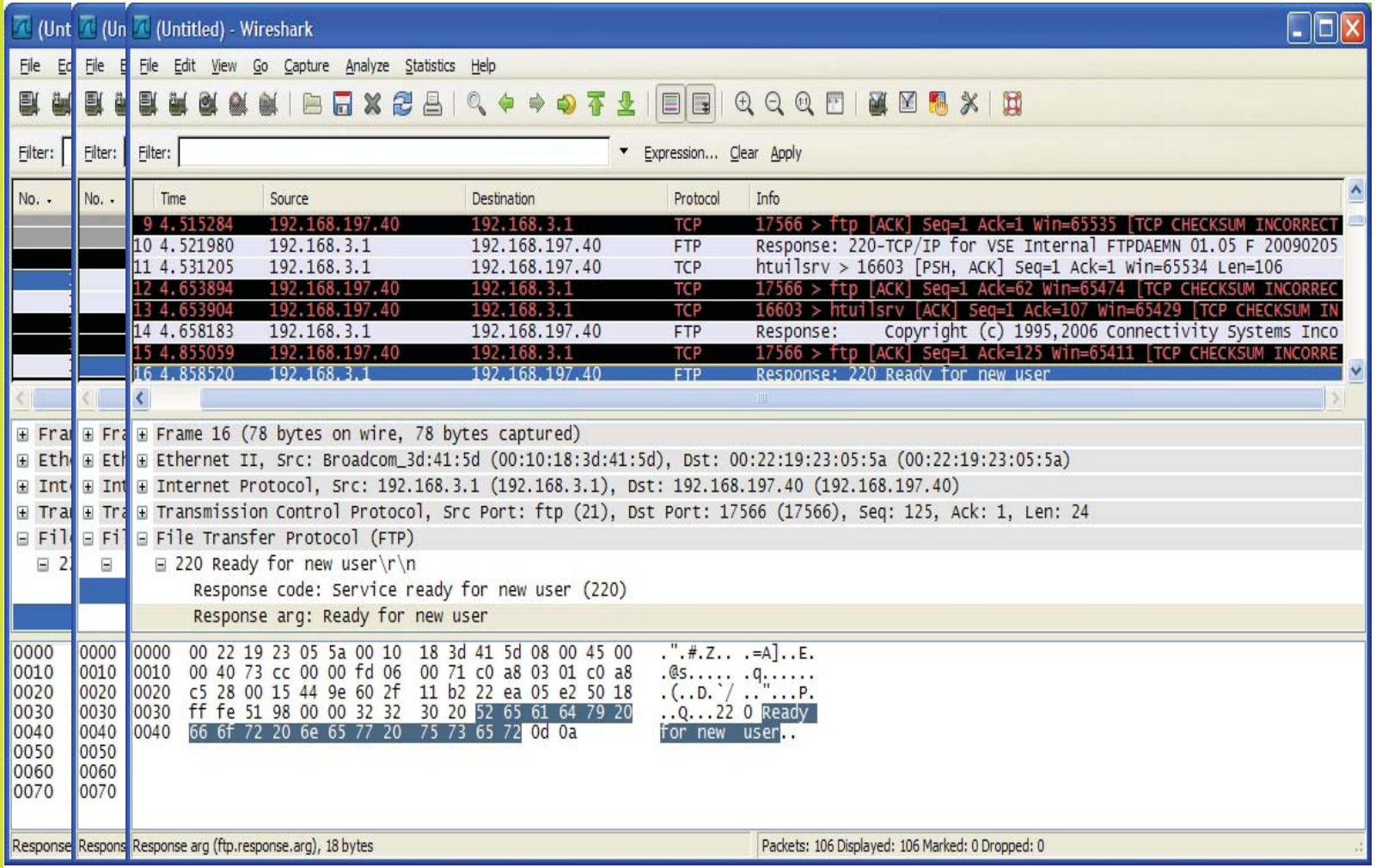
# FTP

Windows cmd using ftp seems to be secure?



# FTP DAEMON RESPONSE

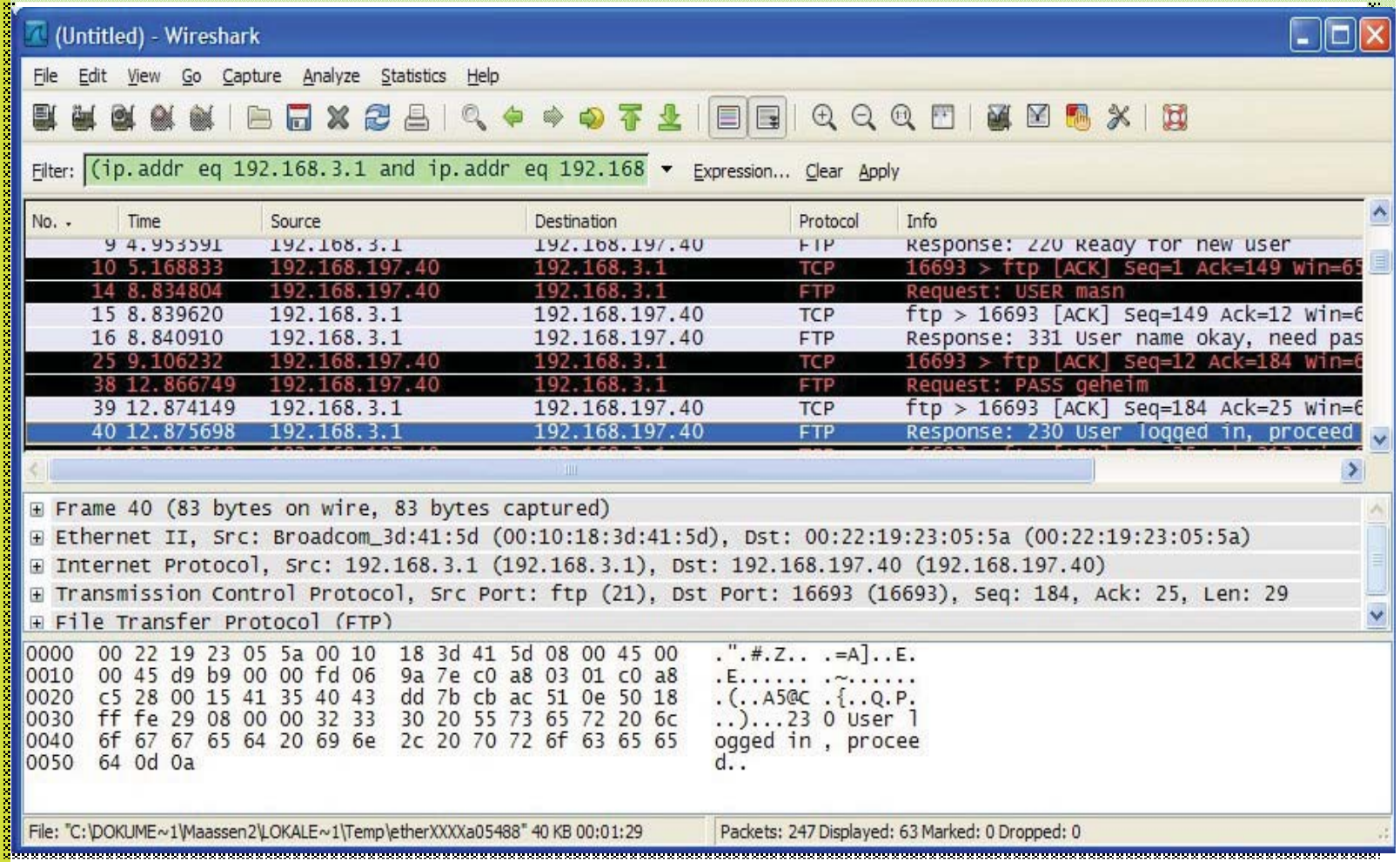
Using Wireshark you can follow the conversation between z/VSE and this client.



# FTP USER MASN

User id and password

as it was typed in.



# FTP FOLLOW TCP STREAM

FTP

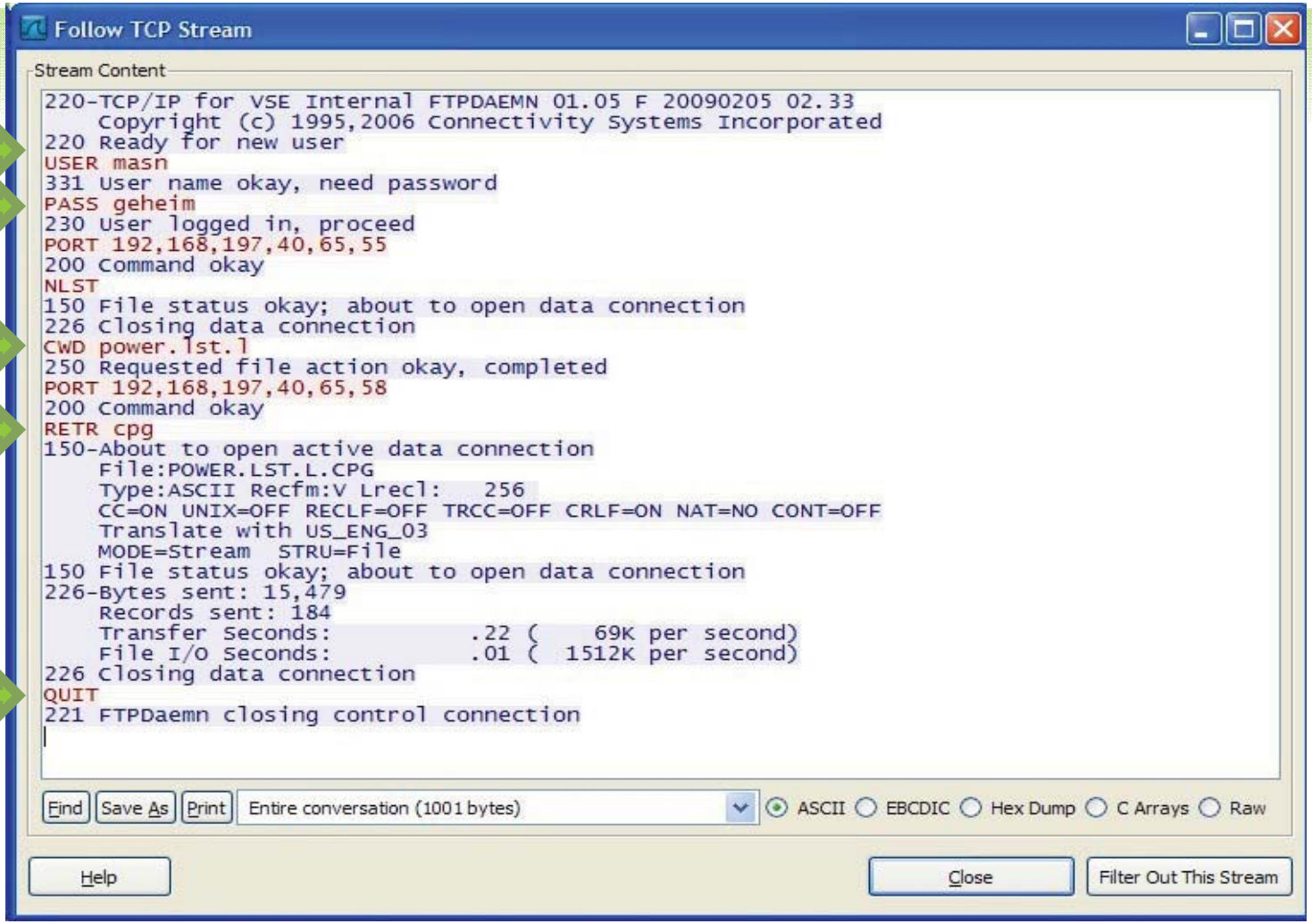
User

PASS

CWD

RETR

QUIT



# Password Protection



What‘s a secure password:

What‘s a secure password: 1_don‘t know_it!

*What‘s a secure password: 1_don‘t know_it!*

In z/VSE passwords are usually limited to 8 bytes, by using LDAP sign-on the password can be up to 64 bytes.

Usually passwords are entered in Uppercase and the contents are characters, digits and special characters.

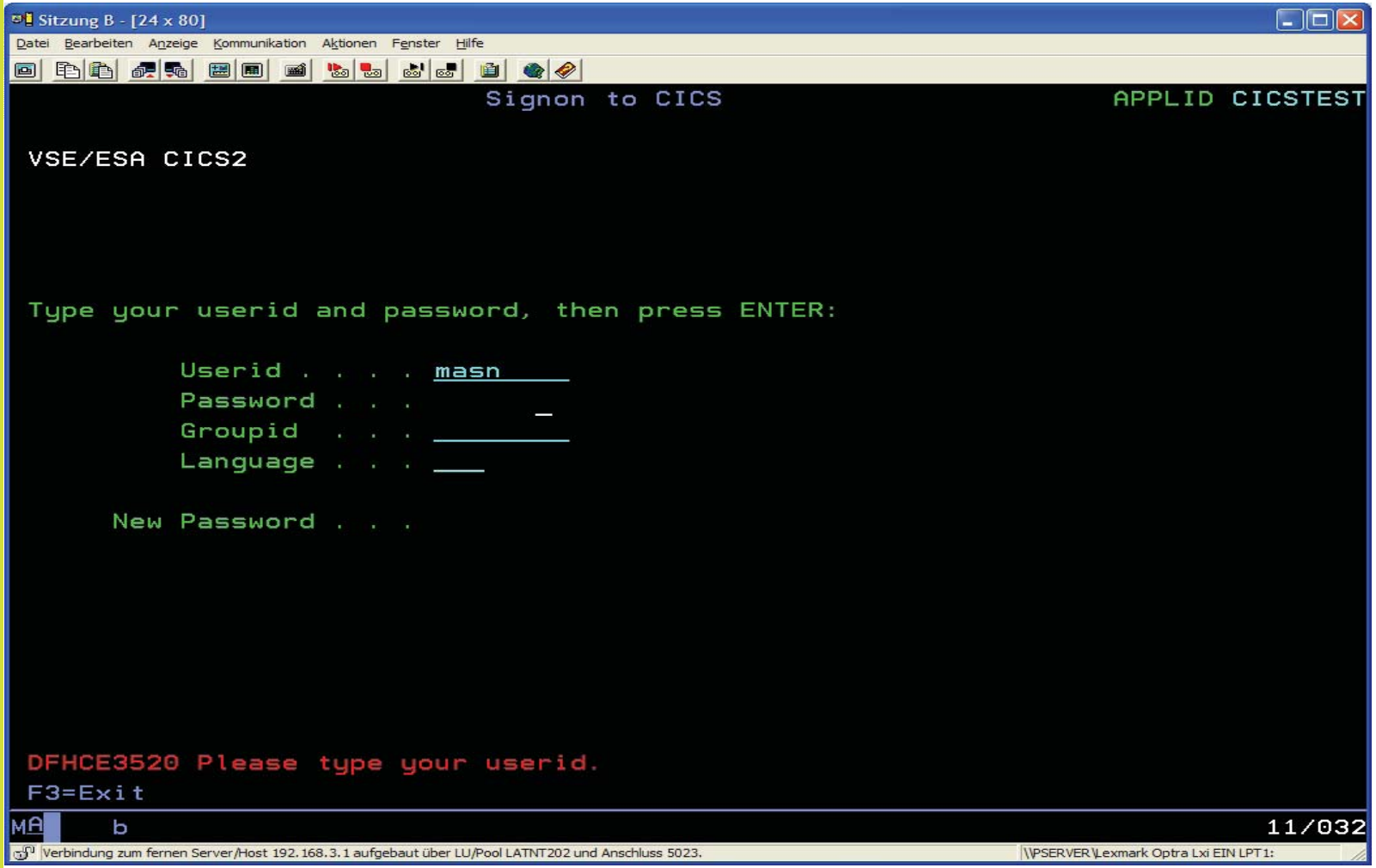
Are they secret and secure ?

# CESN DATA

CESN:

Sign On to CICS

Everything is secret- it's not displayed on a 3270 terminal?



# CESN USER/PASSWORD

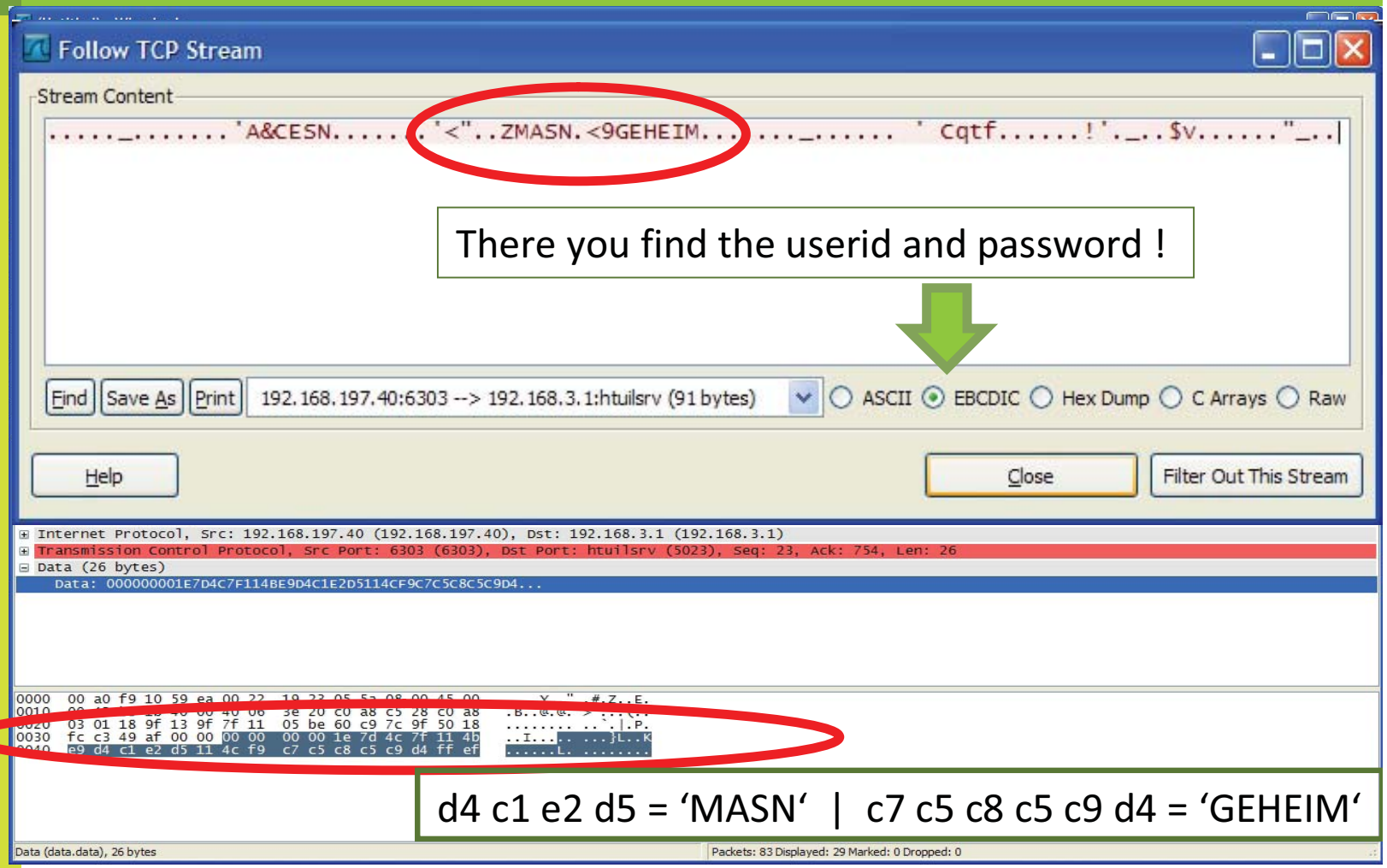
But if you can read

EBCDIC Data in Hex !

It can also be

converted to

ASCII . . .



# E-Mail in z/VSE Trace

- IP Trace tool describes how you can start TCP/IP traces, Dump them and transfer the traces to another platform, using Wireshark and viewing even E-Mail traffic.

This text is from the HTML documentation: ~/doc/ipTraceTool.html

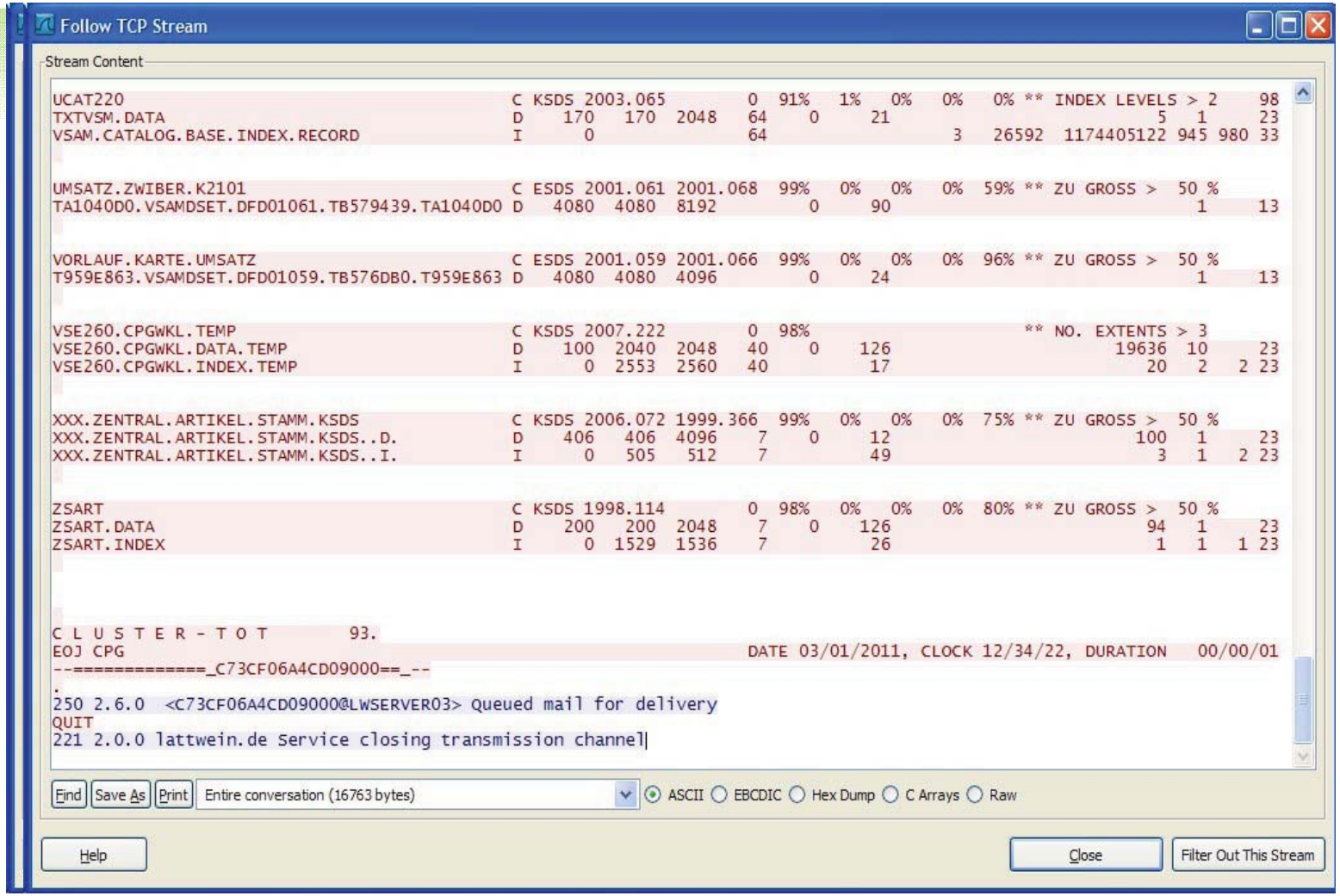
**How to take a trace**
Enter the following commands on your VSE console:

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 - no encryption

Email with attachments
From z/VSE



# CICS Transaction dump

Name

Password

In a CICS Transaction Dump

CICS transaction dumps may have userids and passwords, which can easiliy be read.

Because of this, check if you can trust the people, who get a transaction or system dump.

```
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
```

This is a dump containing terminal input data. But the same information May be found in a common area or in temporary storage.

# CICS Transaction dump

Positive:

When using CEDF

the password is

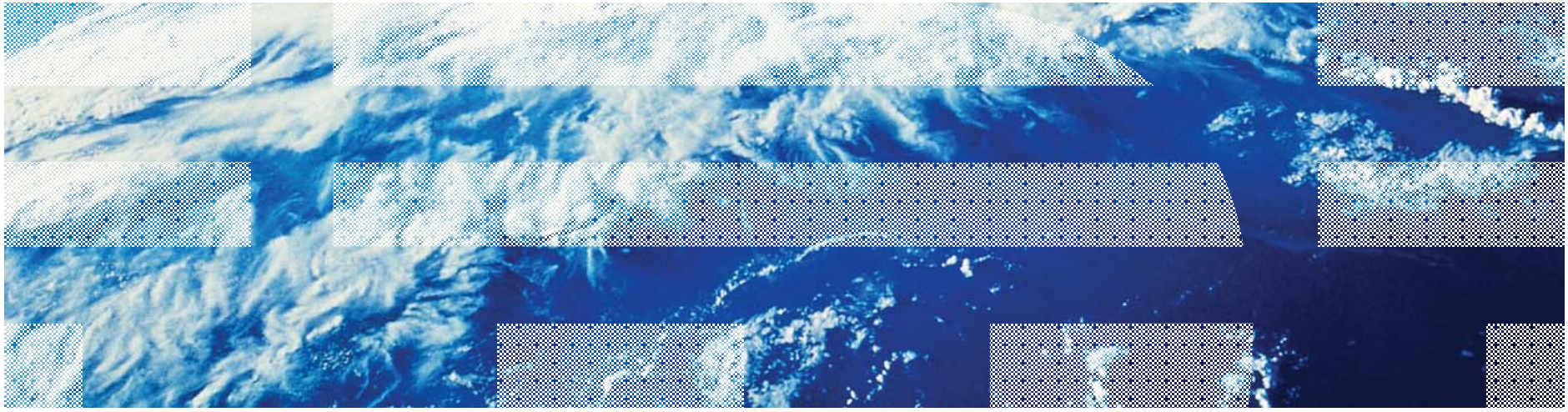
suppressed !

- When using CEDF, the password is suppressed in the EXEC CICS SIGNON command.
- When processing an EXEC CICS SIGNON command, CEDF ***suppresses*** display of the ***password*** value to reduce the risk of accidental disclosure.

**Passwords are not suppressed if stored in a EIB storage, terminal storage, file storage, user storage, TD storage . . . .**

# IS03 Production Security for Linux on System z, z/VM and z/VSE

Heinz Peter Maassen, Lattwein
Ingo Franzki, IBM
Dr. Manfred Gnirss, IBM



# Trademarks

**The following are trademarks of the International Business Machines Corporation in the United States, other countries, or both.**

Not all common law marks used by IBM are listed on this page. Failure of a mark to appear does not mean that IBM does not use the mark nor does it mean that the product is not actively marketed or is not significant within its relevant market.

Those trademarks followed by ® are registered trademarks of IBM in the United States; all others are trademarks or common law marks of IBM in the United States.

For a complete list of IBM Trademarks, see www.ibm.com/legal/copytrade.shtml:

*, AS/400®, e business(logo)®, DBE, ESCO, eServer, FICON, IBM®, IBM (logo)®, iSeries®, MVS, OS/390®, pSeries®, RS/6000®, S/30, VM/ESA®, VSE/ESA, WebSphere®, xSeries®, z/OS®, zSeries®, z/VM®, System i, System i5, System p, System p5, System x, System z, System z9®, BladeCenter®

**The following are trademarks or registered trademarks of other companies.**

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
UNIX is a registered trademark of The Open Group in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

* All other products may be trademarks or registered trademarks of their respective companies.

**Notes**:
Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

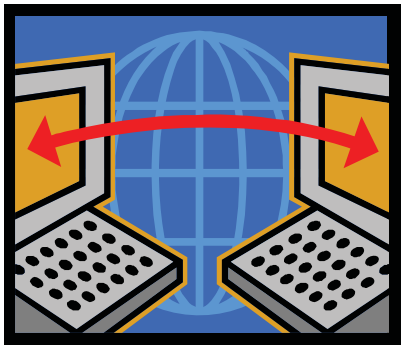
Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

# Why secure VSE ?

- **Prevent unauthorized access to VSE and data**
  - Keep secret data secret
  - Data modification by unauthorized users

- **Prevent users from damaging the VSE system (maybe by accident)**
  - Deletion of members or entries
  - Submission of jobs

- **Prevent unauthorized remote access to VSE**
  - Today most computers are part of a network
  - Theoretically every system in the network could connect to your VSE system
  - FTP allows to access production data
    - VSAM
    - POWER entries (listings)



# CICS Security

- **CICS sign on is performed using**
  - Native CICS TS sign on (CESN)
  - VSE/Interactive Interface sign on (IEGM)
  - Private sign on programs based on CICS SIGNON
- **Grant access to CICS ressources**
  - Per individual user
  - Per group
- **Every transaction runs under the context of a user-id**
  - If no user is signed on, it runs under the default user
    - DFHSIT: DFLTUSER=CICSUSER
- **CICSUSER is predefined after base install:**
  - Type 3 (ICCF is not allowed)
  - Is in GROUP01, GROUP60-GROUP64
    - GROUP01 and GROUP60 is required by Interactive Interface
- **Actions to perform after installation**
  - Do not allow this user to use critical transactions
  - Adjust groups this user is belonging to

| Transaction | Description |
|---|---|
| USER | Display Activity Dialog, send Message to all users |
| CEMT | Master terminal |
| CEDA | Resource definition online |
| CEDB | Like CEDA, but no INSTALL possible |
| CEDC | Like CEDA, but read only |
| CECI | Command level interpreter |
| CEDF/CEDX | Execution diagnoistic facility |
| CETR | Trace control |
| CESN/CESF | Sign on/sign off |
| DITT | Online Ditto |
| others ? | |

# Batch Security

- **When you have batch security active (SYS SEC=YES), all your jobs need to specify a user-ID and password**
  - Either using the // ID statement within the job
  - or in the * $$ JOB card

- **ID statement or * $$ JOB specifies user id and password for a job**

```
* $$ JOB JNM=MYJOB,...,SEC=(user,password)
```

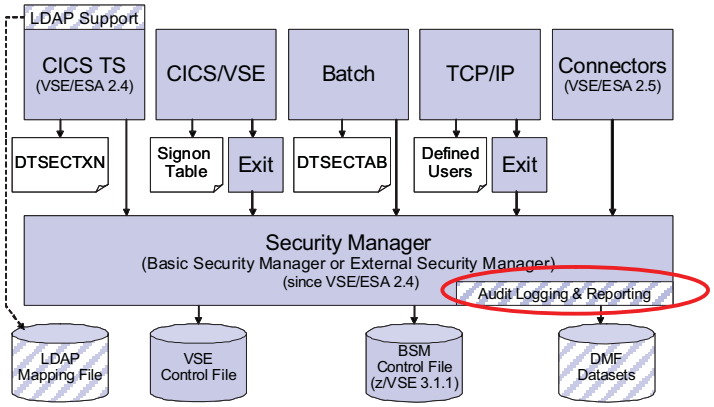
or

```
// ID USER=user,PWD=password
```

- **User id and password are verified against**
  - DTSECTAB
  - Security Manager (RACROUTE)
- **Subsystems (LIBR, VSAM, ...) uses this user id to verify access rights against DTSECTAB**
- **When you submit jobs from the ICCF library**
  - The submitted job automatically inherits the user-ID and password from the submitting user
  - No need to specify a // ID statement or user-ID in the * $$ JOB card
- **Inheritance only works if batch security is active at the time you do the submit**
  - Jobs that have been submitted prior to activating batch security do not have any inherited security information, you may have to re-submit those jobs

# Audit-Logging and Reporting

- **All access attempts to protected resources can be logged**
  - Allowed access as well as disallowed access
- **Possible attacks can be detected**
  - E.g. multiple logon attempts with invalid password
  - Who did when access which resource
- **Analysis can be done using a reporting tool**
  - Summary report
  - Detailed report of all access attempts
- **New with z/VSE 4.2:**
  - Logging of important BSTADMIN commands
- **New since z/VSE V4.3:**
  - Audit-Logging of DTSECTAB resources
- **To activate logging for a specific resource, you need to specify the AUDIT option (using BSTADMIN) on the resource profile:**




**AUDIT(*audit-level, access-level*)** ← New with z/VSE 4.2

**audit-level:**

**ALL:** All authorized accesses and detected unauthorized access attempts should be logged.
**FAILURES:** All detected unauthorized access attempts should be logged (the Default).
**SUCCESS:** All access attempts that were authorized should be logged.
**NONE: N**o logging should be done.

**access-level:**

**ALTER:** Logs ALTER access-level attempts only.
**READ:** Logs access attempts at any level. READ is the default value if the access-level is omitted.
**UPDATE:** Logs access attempts at the UPDATE and ALTER level.

# New since z/VSE V4.3: Protect JCL operands


- **You can use BSM security to protect operands of specific JCL statements.**
  - For example, you can protect the PERM operand of the ASSGN and LIBDEF statements.

- **IBM provides five resource profiles of class FACILITY that are used for JCL statement checking:**
  - IBMVSE.JCL.ASSGN.**PERM**
  - IBMVSE.JCL.LIBDEF.**PERM**
  - IBMVSE.JCL.LIBDROP.**PERM**
  - IBMVSE.JCL.OPTION.**PARSTD**
  - IBMVSE.JCL.OPTION.**STDLABEL**

- **To perform JCL statement checking:**
  - JCL security must be enabled (SYS SEC=YES,**JCL**)
  - The minimum access right for Universal Access or user-IDs/groups must be READ

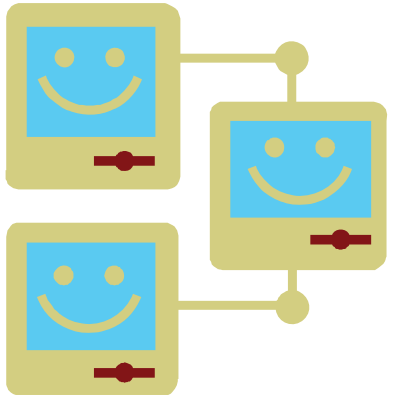
# New since z/VSE V4.3: Protect WebSphere MQ resources

- **The Basic Security Manager supports the following resource classes that are used by WebSphere MQ for z/VSE Version 3 onwards:**
  - MQADMIN – Administrative type functions
  - MQCMDS – Command security
  - MQCONN – Connection security
  - MQQUEUE – Queue resource security
  - MQNLIST – Namelist resource security


- **All resources (BSM profile names) used by WebSphere MQ are prefixed with the name of the subsystem that they are to be used by.**
  - For example, if queue manager with SSID **MQV1** has a queue called **QUEUE_FOR_LOST_CARD_LIST**, the appropriate profile would be defined to the ESM or BSM in class MQQUEUE as:
    - **MQV1.QUEUE_FOR_LOST_CARD_LIST**

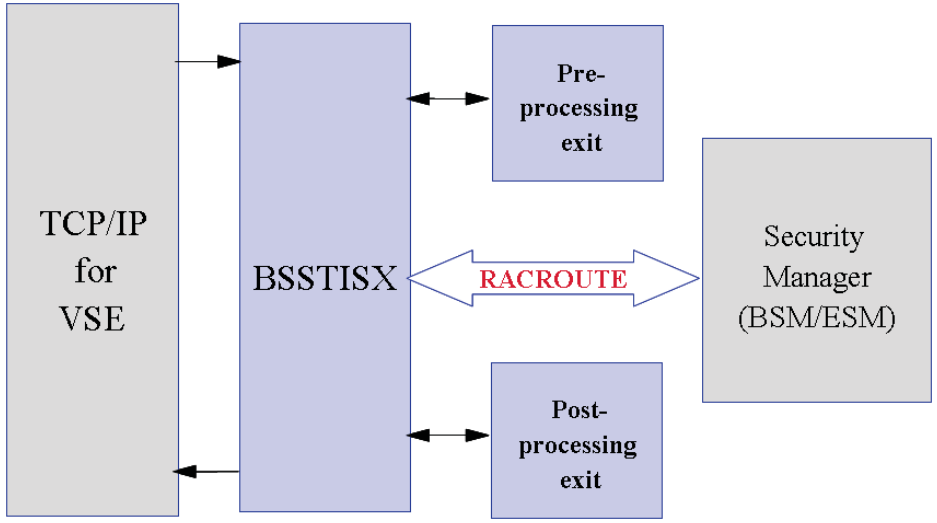
- **For details, please see manual "WebSphere MQ for z/VSE System Management Guide" - GC34-6981-02 (revision 02)**

# TCP/IP Security



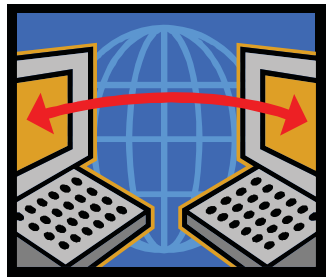
- **In general TCP/IP uses its own user id definitions**
  - Readable in initialization member (IPINITxx.L)
    - **`DEFINE USER,ID=user,PASSWORD=pwd`**
  - Duplicate user definitions

- **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:



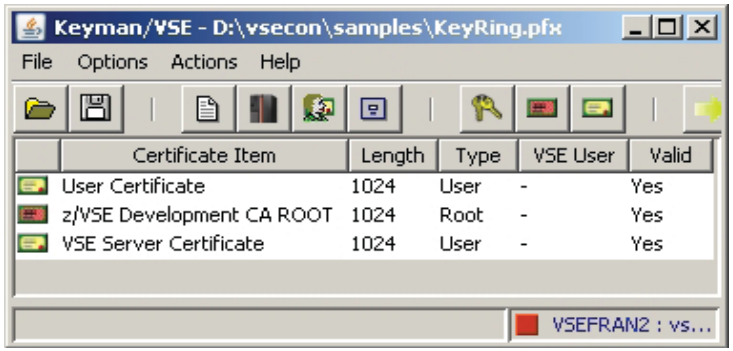
- **Encryption of data transmitted over network connections**
  - SSL, HTTPS
  - SecureFTP, Secure Telnet

- **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

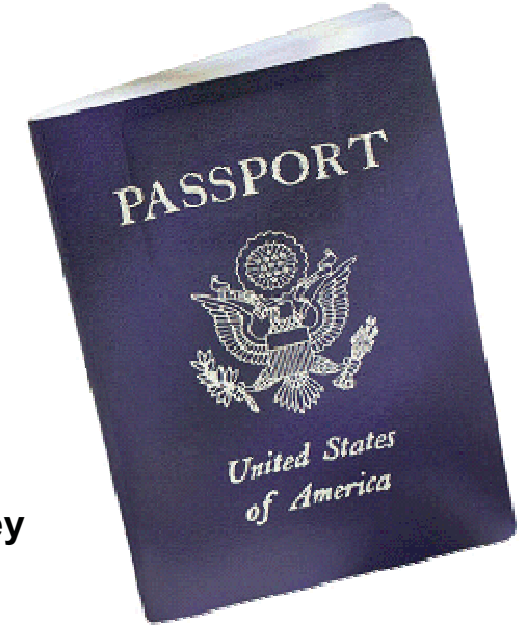
- **Key Management is not trivial**
  - Key must often be kept secure for a very long time
  - You must be able to associate the encrypted data with the corresponding key(s)
  - Encrypted data and the corresponding key(s) must be strictly separated




- **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

# Certificates

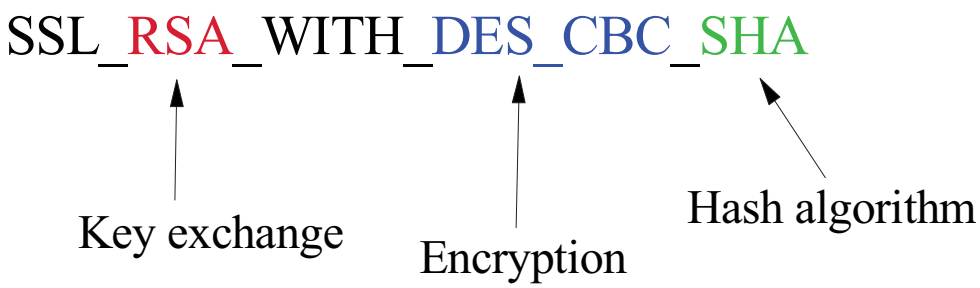
- **A certificate contains the following items**
  - The subject (name of the person)
  - The subject's public key
  - Period of validity
  - The issuer
  - Issuers signature

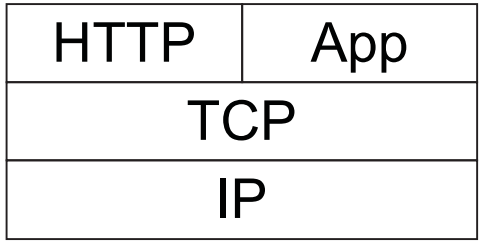


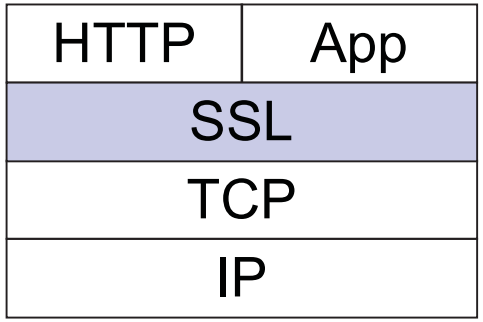

- **The issuer "signs" the certificate by encrypting a hash of the certificate content with his private key**
- **Everyone can check the sign by decrypting it with the issuers public key**
- **For production purposes, certificates are usually issued by a well known and trusted Certificate Authorities (CA)**
  - For example Thawte, VeriSign, etc.
  - Usually this cost money
- **For in-house use (Intranet), you can have your own Company-wide Certificate Authority**
  - Certificates are trusted inside your company, but not outside
- **For test purposes you can use self-signed Certificates (you are your own Certificate Authority)**
  - Nobody trusts these Certificates (except you)

# Secure Socket Layer – Encrypted data transfer over a network

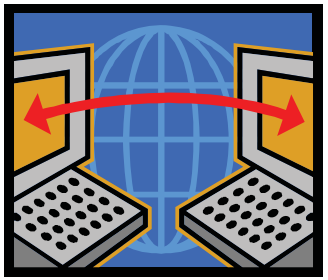
- **SSL provides a communication channel with message integrity, authentication, and confidentiality**
- **SSL is a widely used protocol**
  - Secure HTTP (HTTPS) is used very often in the Internet
- **SSL uses a TCP connection to transfer encrypted messages**
  - Uses asymmetric cryptography for session 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 5.1 | 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 | Yes | - |
| CEX2C | Yes | Yes | Yes | Yes | Yes | - | - |
| CPACF | Yes | Yes | Yes | Yes | Yes | - | - |
| CEX2A | Yes | Yes | Yes | Yes | Yes | - | - |
| PCIXCC | Yes | Yes | Yes | Yes | - | - | - |

by server

| | prior z800 | z800 | z900 | z890 | z990 | z9 | z10 | z196 | z114 |
|---|---|---|---|---|---|---|---|---|---|
| PCICA | - | Yes | Yes | Yes | Yes | - | - | - | - |
| PCIXCC | - | - | - | Yes | Yes | - | - | - | - |
| CEX2/3C | - | - | - | Yes | Yes | Yes | Yes | Yes | Yes |
| CPACF | - | - | - | Yes | Yes | Yes | Yes | Yes | Yes |
| CEX2/3A | - | - | - | - | - | Yes | 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.
```

# z/VSE V4.3 – Crypto Express3 and AP queue interrupt support

- **Support for AP-interrupts is a new function of IBM System z10 and IBM zEnterprise 196**
- **A hardware interrupt is issued when a response is ready for de-queueing from a card.**
  - Removes the need for the formerly used polling mechanism
  - User can switch between polling and interrupts (default: polling)
  - Using interrupts increase throughput for certain workloads without increasing CPU load
- **Not available under z/VM!**
- **Supported cards are:**
  - Crypto Express2 and
  - Crypto Express3

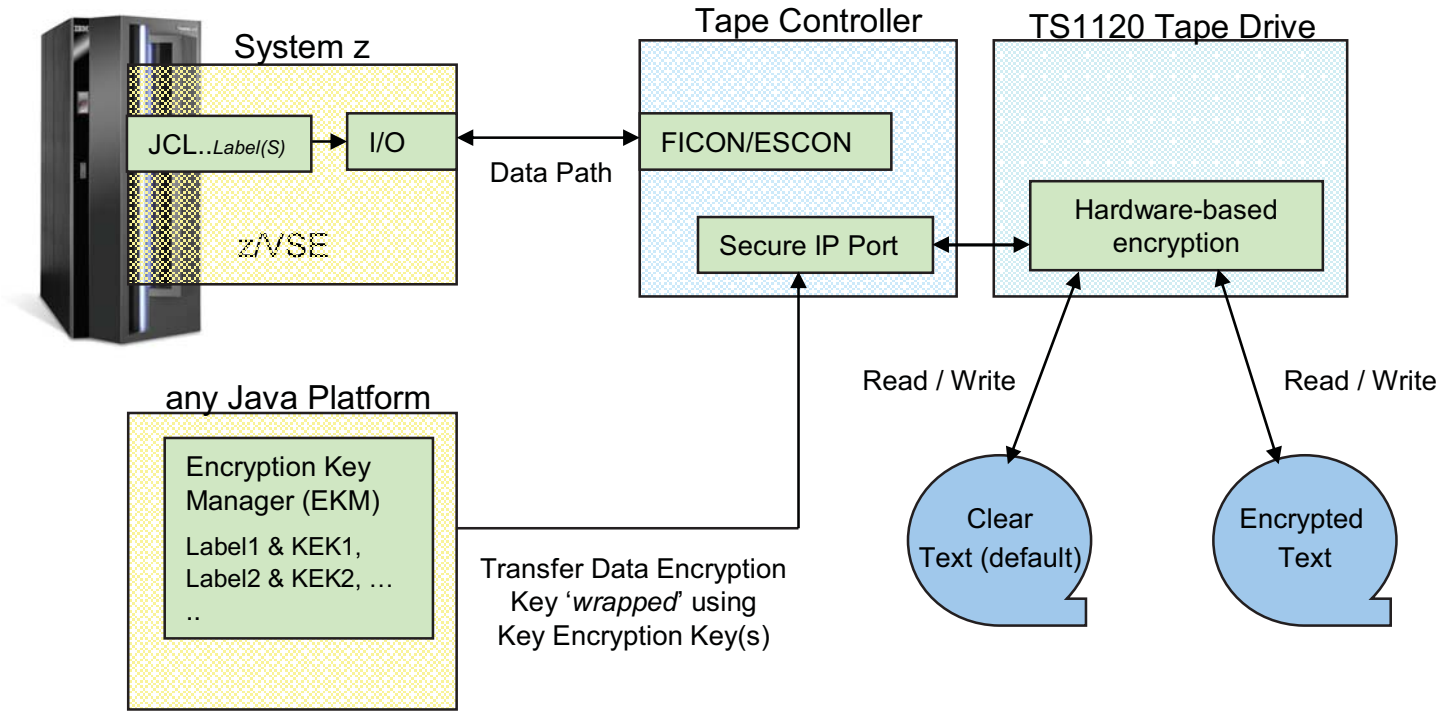
- **The VSE crypto device driver provides new commands:**
  - APEAI, enable AP interrupts for all APs
  - APDAI, disable AP interrupts for all APs

# IBM Tape Encryption – TS1120 & TS1130

- The IBM System Storage TS1120/TS1130 Tape Drive has been enhanced to provide drive based data encryption
- A key management component supports the generation and communication of encryption keys for the tape drives across the enterprise.
- Support is available for z/VSE:
  - *z/VSE V4.2:* *GA*
  - *z/VSE V4.1:* *DY46682 (UD53141 and UD53142)*
  - *z/VM:* *VM64062 (UM32012)*
  - *DITTO:* *PK44172 - With this APAR, DITTO/ESA for VSE supports tape encryption interactively and via standard VSE JCL in BATCH mode*

- Considerations when encrypting tapes:
  - A tape can either contain encrypted data or unencrypted data
  - If you encrypt the first file on the tape, all subsequent files will also be encrypted using the same key
    - Important for multi file tapes
  - If you send an encrypted tape to a business partner, the other side will also require a TS1120 or TS1130 to be able to read the tape

# IBM Tape Encryption – TS1120 & TS1130




encryption mode (03=write)

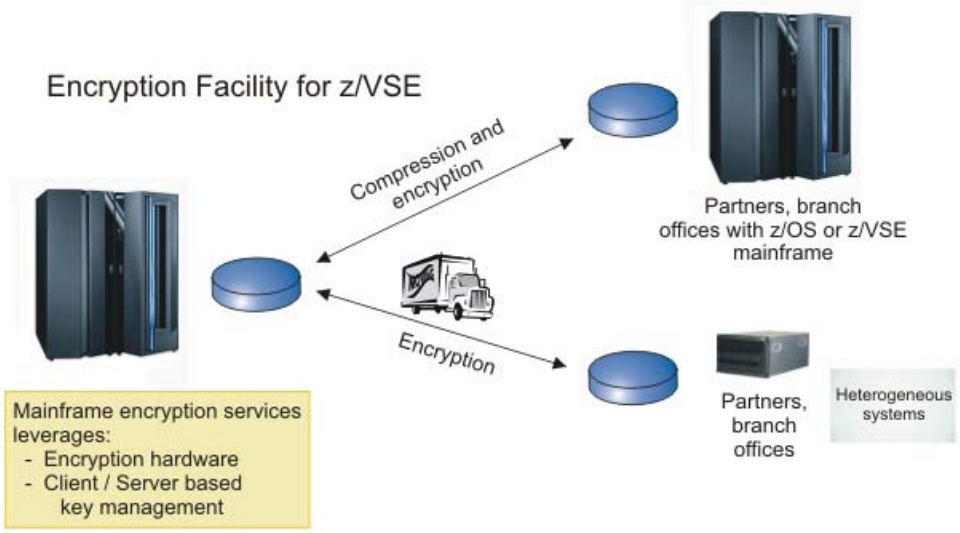
```
// JOB ENCRYPT
// ASSGN SYS005,480,03
// KEKL UNIT=480,KEKL1='MYKEKL1',KEM1=L,KEKL2='MYKEKL2',KEM2=L
// EXEC LIBR
  BACKUP LIB=PRD2 TAPE=SYS005
/*
/&
```

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

# Encryption Facility for z/VSE

## Differences between Encryption Facility V1.1 and V1.2 OpenPGP:

| | **EF for z/VSE V1.1** | **EF for z/VSE V1.2 OpenPGP** |
|---|---|---|
| **Encrypted data format** | System z format | OpenPGP format |
| **Compatibility with** | EF for z/OS V.1.1, EF for z/OS Java client | Any OpenPGP implementations, like GnuPG, EF for z/OS V1.2 OpenPGP |
| **Symmetric Algorithms** | TDES and AES-128 | DES, TDES, AES-128, 192, 256 |
| **Hash algorithms** | SHA1 | MD5, SHA1, 224, 256, 384, 512 |
| **Compression** | System z provided compression (hardware accelerated) | ZIP, ZLIB based compression (software) |
| **RSA key lengths** | 512, 1024, 2048 | 1024, 2048 |
| **Data integrity** | None | MDC |
| **Public key format** | x.509 certificates | PGP certificates |
| **Signatures** | None | RSA signatures |

# Encryption Facility for z/VSE - Customer value

- **No special tape hardware requirements (e.g. TS1120)**
  - But exploits IBM crypto hardware (crypto cards and CPACF)
- **Host-based utility, no additional client/server workstations**

- **Easy to use**
  - No special setup necessary for password-based encryption
- **Supports all VSE data formats: single files and complete tape backups (LIBR, IDCAMS, POWER, etc.)**
- **Supports even proprietary vendor backup formats**
- **Encrypted datasets and tapes can easily be exchanged between business partners even on non z platforms**
  - Password-based
  - Public-key based

# New technical articles on VSE homepage

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

**How to setup hardware crypto and SSL 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: November 2010
Joerg Schmidbauer, IBM

How to setup SSL with CICS Web Support (PDF, 1.7MB)
Updated: November 2010
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, 1.2MB)
Updated: November 2010
Joerg Schmidbauer, IBM

How to setup and use Keyman/VSE (PDF, 650KB)
New: November 2010
Joerg Schmidbauer, IBM

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

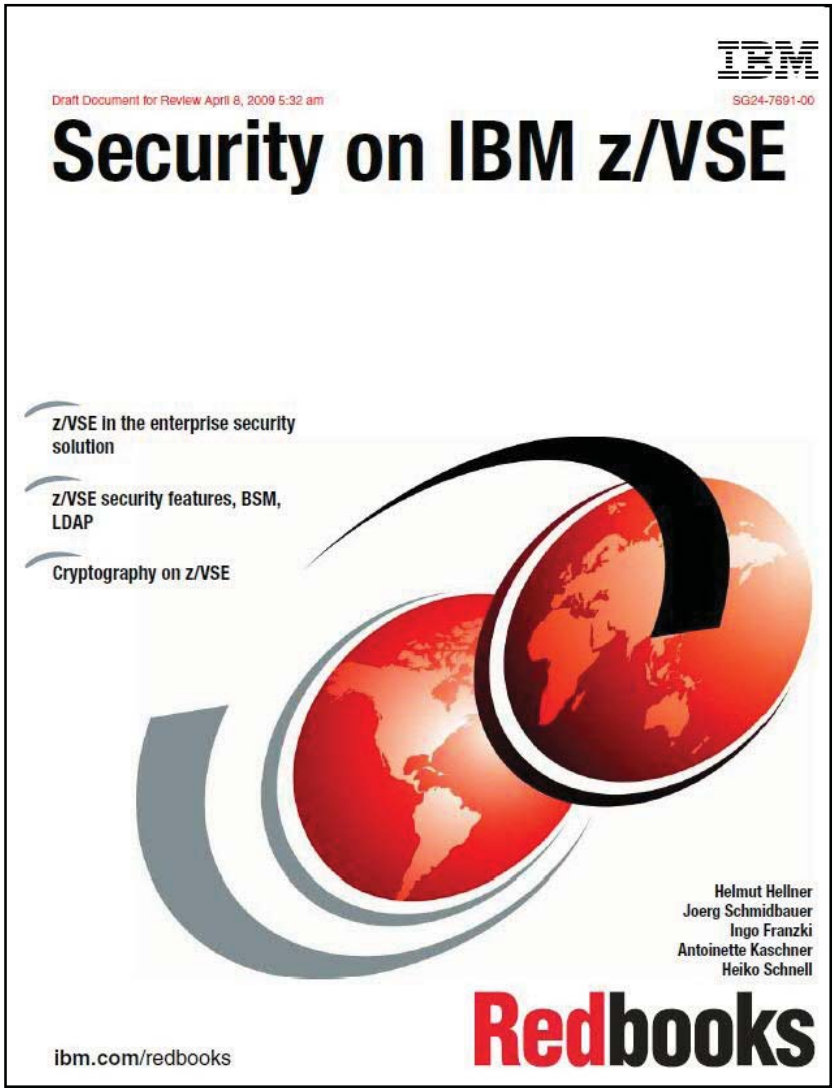
# New Redbook: Security on IBM z/VSE - SG24-7691

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

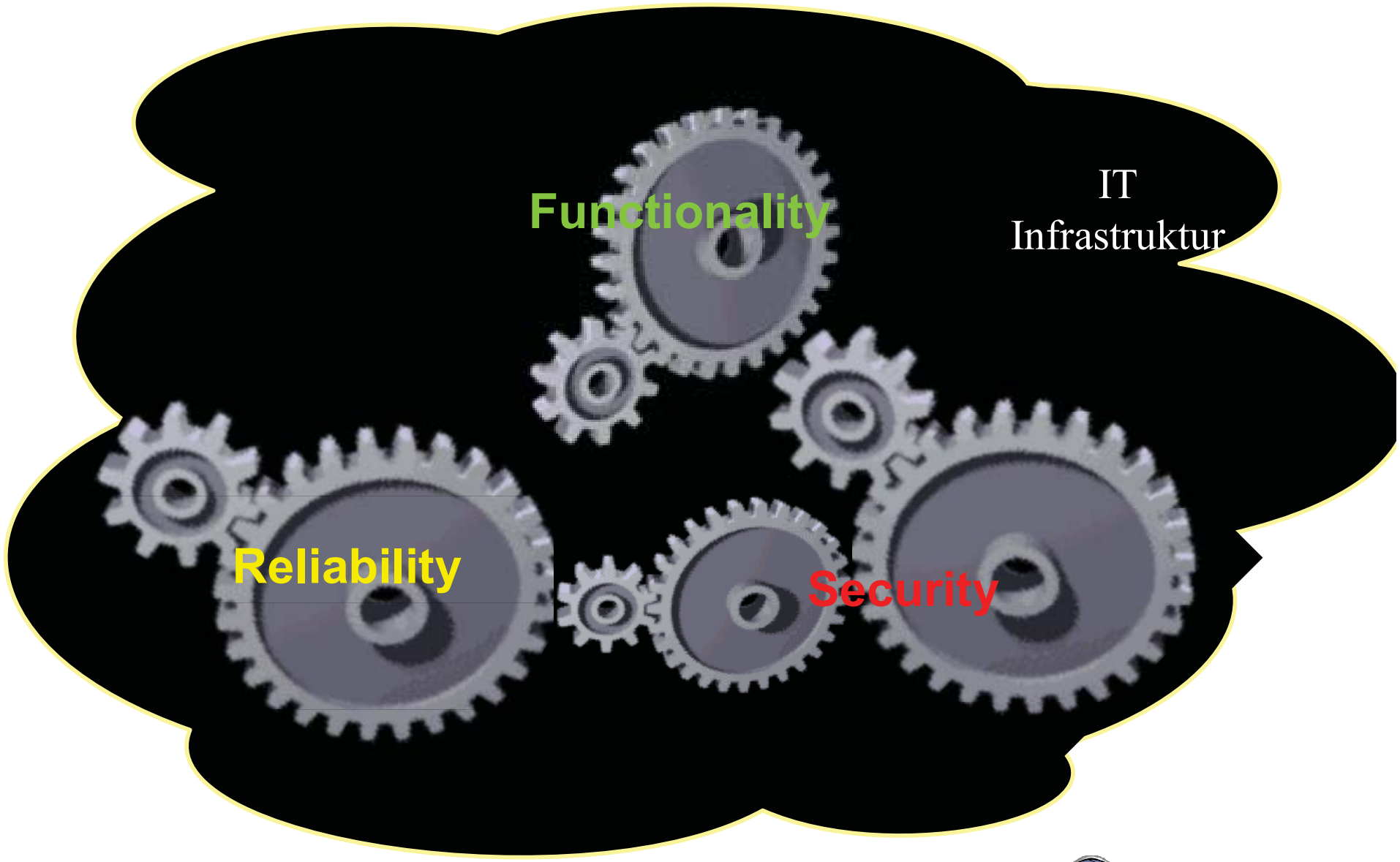


# Related Documentation

- New RedBook: Security on IBM z/VSE - SG24-7691
  - http://www.redbooks.ibm.com/redpieces/abstracts/sg247691.html
- IBM System z cryptography for highly secure transactions
  - http://www.ibm.com/systems/z/security/cryptography.html
- VSE Security Homepage
  - http://www.ibm.com/systems/z/os/zvse/documentation/security.html
- IBM Manuals
  - z/VSE Planning
  - z/VSE Administration
  - OS/390 Security Server External Security Interface (RACROUTE) Macro Reference (GC28-1922)
  - OS/390 Security Server (RACF) Data Areas (SY27-2640)
  - z/VSE e-business Connectors, User's Guide
  - CICS Enhancements Guide, GC34-5763

# Questions ?

# Security: Nothing is for free

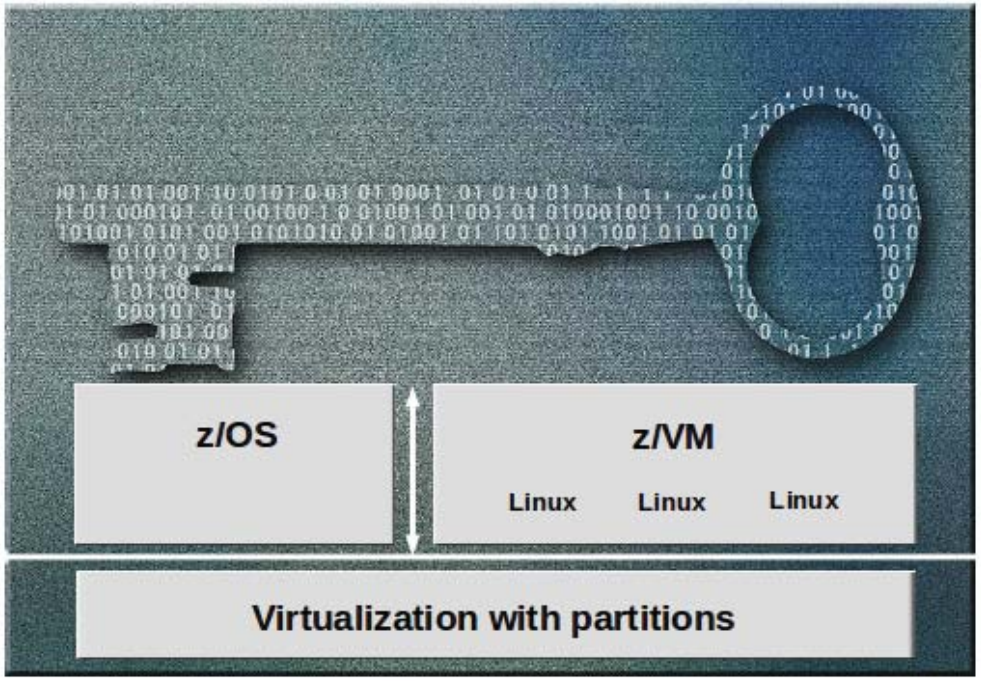


# Certification of mainframe products and components

## Physical infrastructure – System z security assessed

**Security Server: RACF, LDAP, Firewall - Encryption - Public Key Infrastructures - Certificate Authority**

The Common Criteria program developed by NIST and NSA establishes an organizational and technical framework to evaluate the trustworthiness of IT Products and protection profiles




### z/VM

- **Common Criteria** EAL4+ with CAPP and LSPP
  - **z/VM 5.3 + RACF**

### Linux on System z

- **Common Criteria** EAL4+ with CAPP and LSPP for SUSE and RedHat distribution

### z/OS

- **Common Criteria** EAL4+ with CAPP and LSPP
  - z/OS 1.10 + RACF
- **IdenTrust™** certification for z/OS PKI Services

### System z EC and other System z servers

- **Common Criteria EAL5** with specific Target of Evaluation
  - **Logical partitions**
- FIPS 140-2 level 4
  - Crypto Express 2 as coprocessor

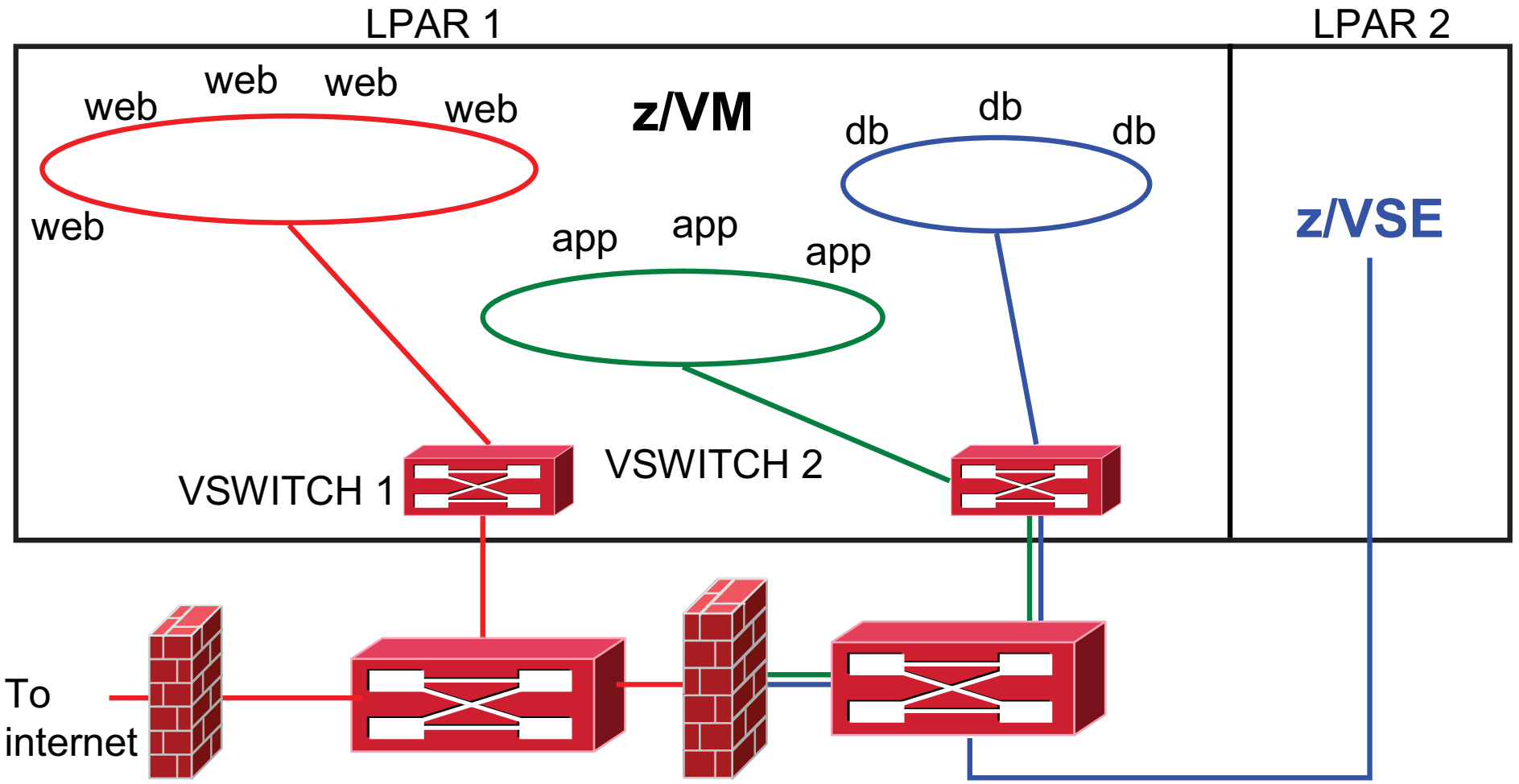
See: www.**ibm.com**/security/standards/st_evaluations.shtml

# z/VM

z/VM as platform for applications, or as hypervisor for z/VSE, Linux, or z/OS:

- Must be protected
- Access (system, networks., passwords)
  - Avoid things like user maint with pwd maint !
  - Rights and privilege classes: be careful
- Multiple Seurity Zones within one z/VM can be realised in a secure manner.
  - Take care of various aspects for administration and organisation
- RACF

# Multi-zone Network with VSWITCH (red zone physical isolation)




With 2 VSWITCHes, 3 VLANs, and a multi-domain firewall

# Open Source Software (Linux): No Security by Obscurity

- Philosophy
- Open Source ? < - > Closed Source ?
  - Algorithms
  - Implementation
  -
- Trust, guaranty and Service?
- Control (Audit-capability)

And a “Security Policy” is mandatory

# Linux for System z

- Linux as a server itself is not more secure or less secure if it is running on System z. Linux = Linux.

- Linux needs to be hardened
  - Follow standards
  - SELinux, AppArmor, . . .

- Linux for System z can use HW Crypto support

# Security – (most) important ascpects

Customers and Users have responsibilities.

- 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

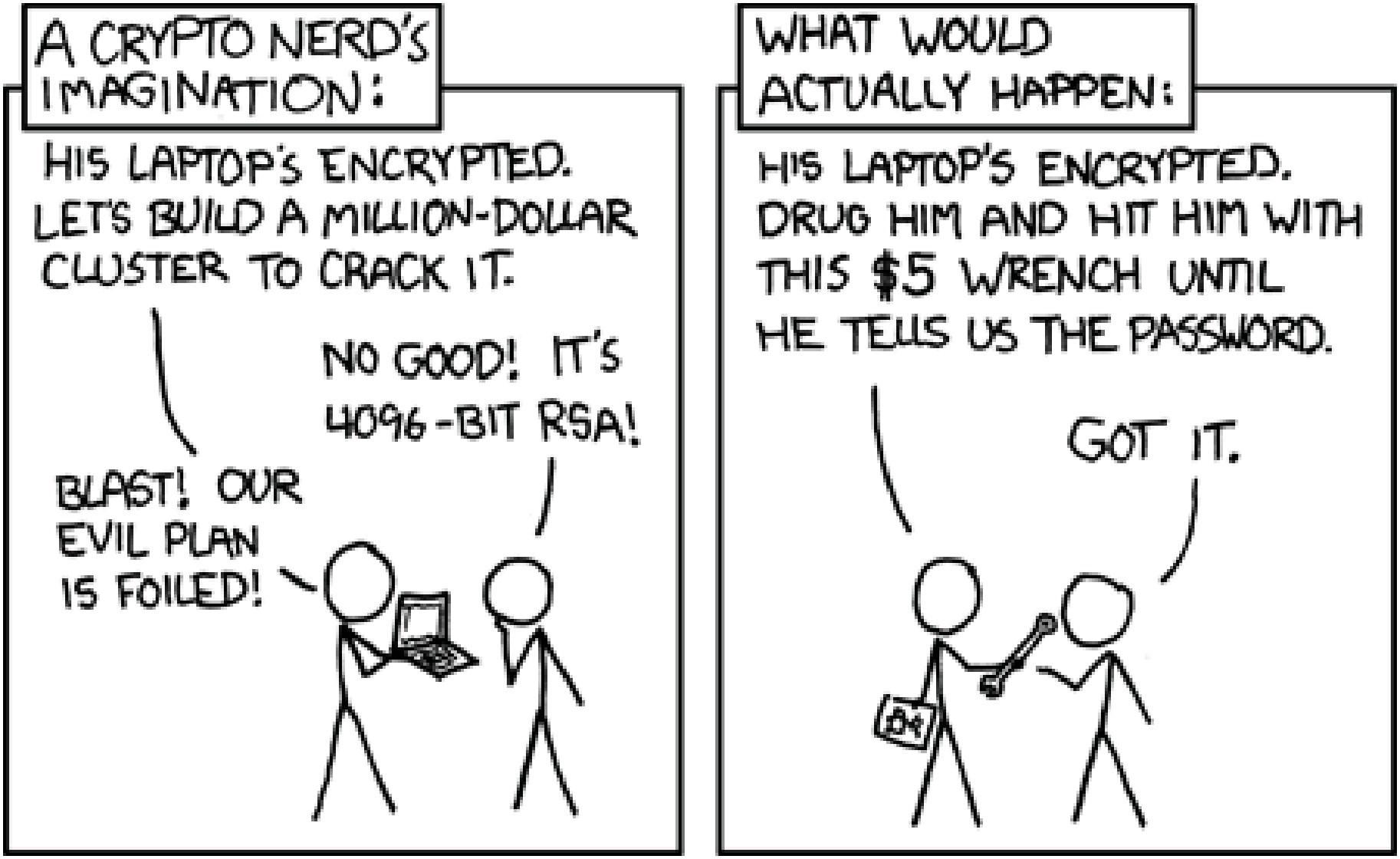
# Security – Hardening of a Linux servers

Customers and Users have responsibilities.

Here are some Selected HOWTO - aspects

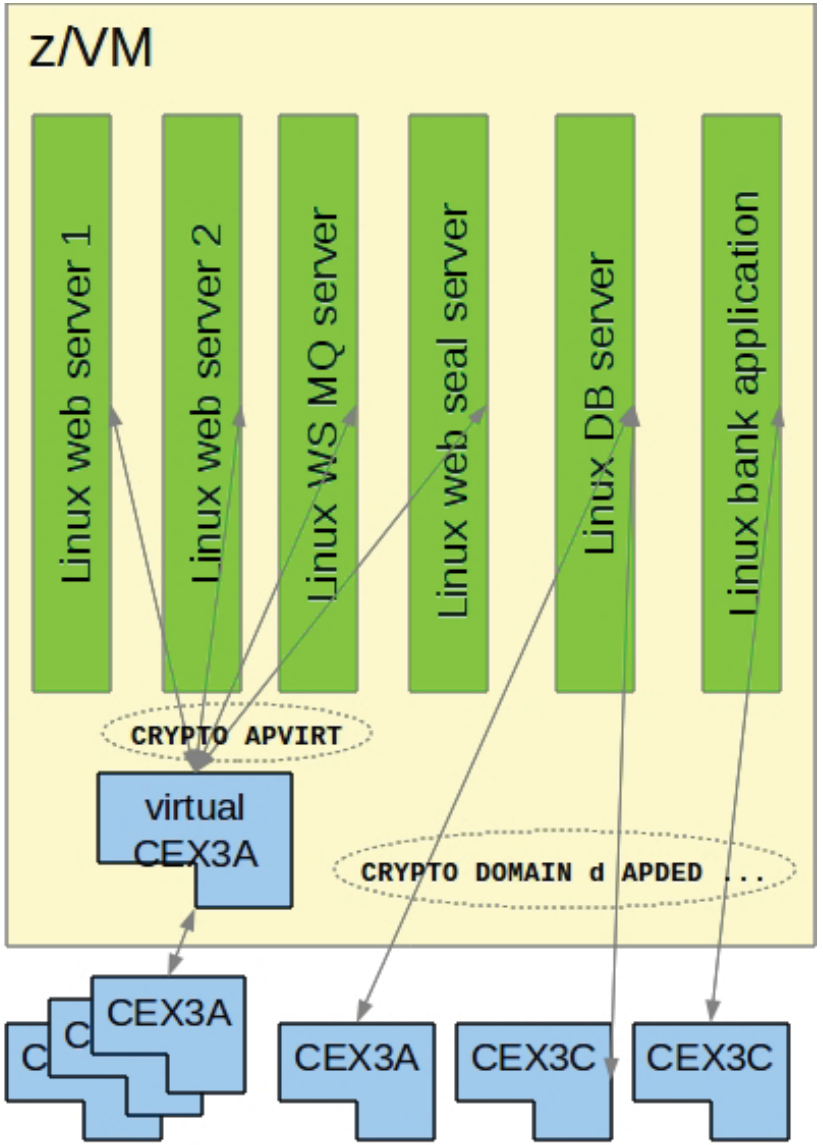
- Patch/upgrade strategy
- Set UID/Set GID programs
- Limit privileged accounts – superuser
- Password policy
- Unused services/ports – turn them off
- Insecure services – use secure version
- Intelligent and secure logging – "over-applied/under-utilized"
- Secure configuration
- Applications security – 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,……..

# Your system is as secure as its weakest link

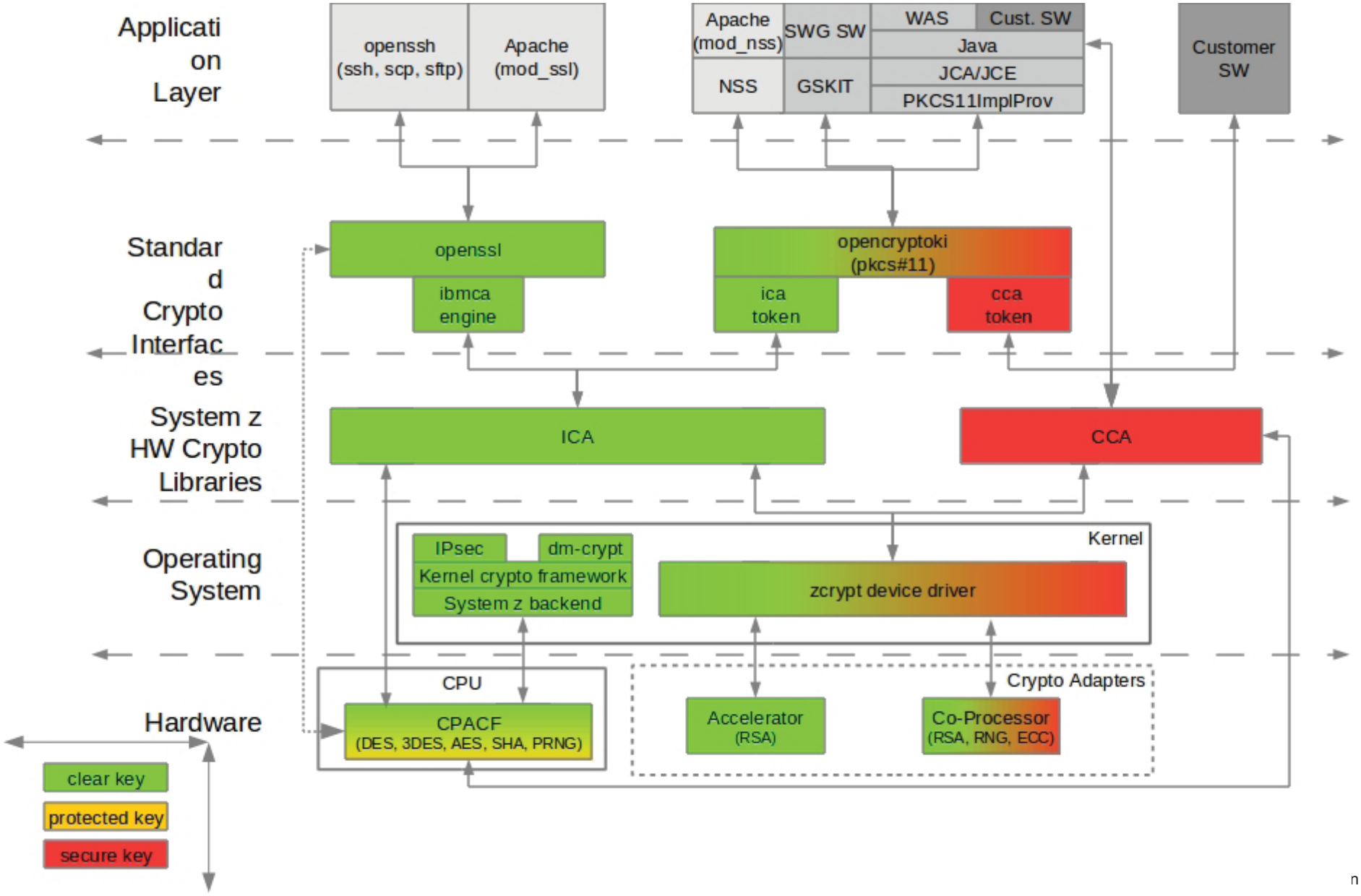


# z/VM Crypto Guest Support

- A guest may have
  - either dedicated adapters
    - `CRYPTO DOMAIN d APDED a1 a2 ...`
  - or shared adapters
    - `CRYPTO APVIRT`
- Shared adapters
  - are of a single type
    - uses only highest priority type
    - priority:
  - CEX3A > CEX2A > CEX3C > CEX2C
  - should only be used for clear key operations
  - Support for 4k RSA keys requires APAR VM64829 before z/VM 6.2
- Checking Crypto Configuration
  - show status of crypto facilities
    - `Q CRYPTO [ APqs [Users] ]`
  - show status of crypto facilities of guest
    - `Q V CRYPTO`



# Linux on System z Crypto Stack

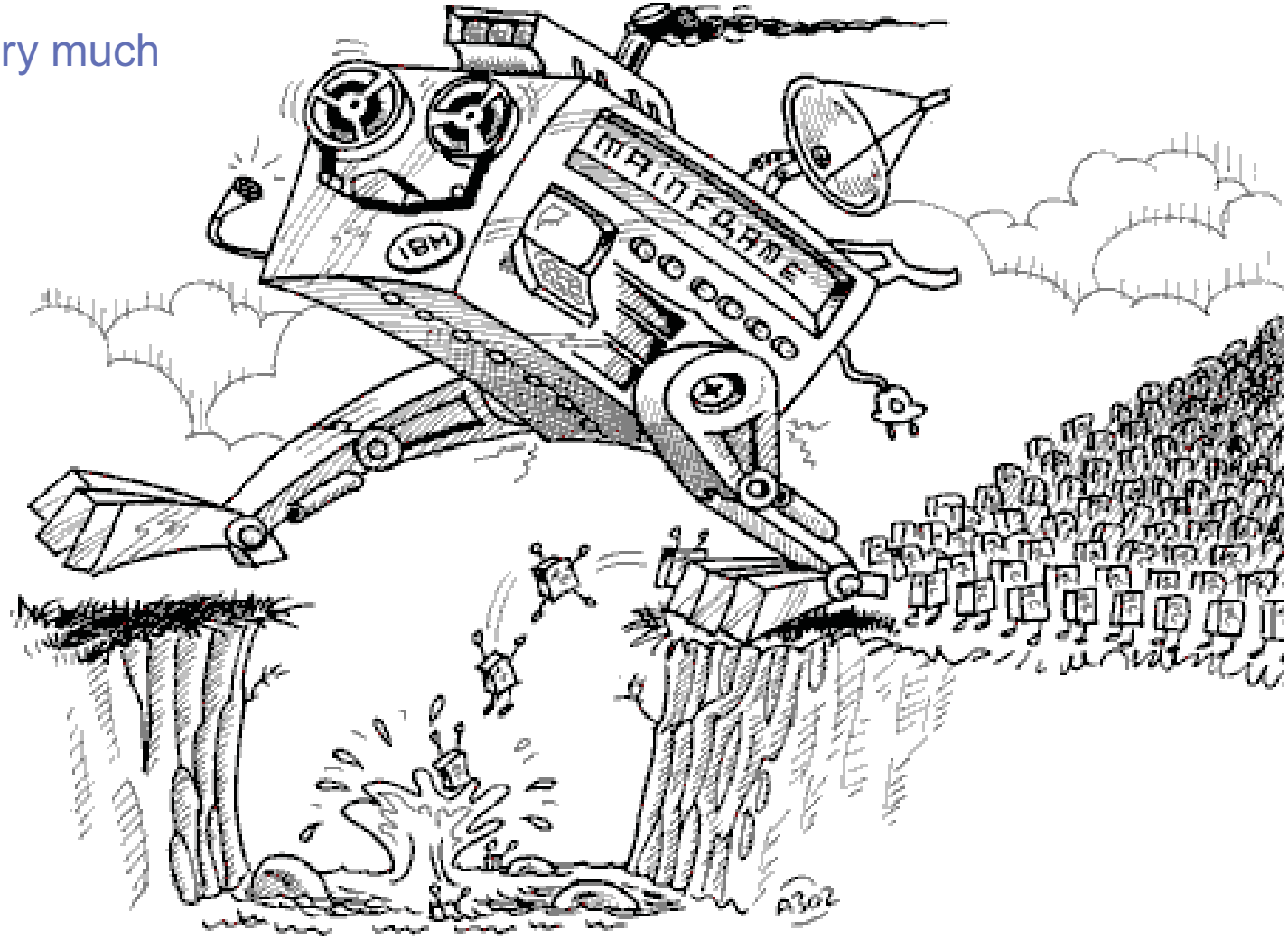


# Security – More aspects

- The importance of passwords
- User authentication in Linux
- Pluggable Authentication Modules
- Centralized LDAP Server
- OpenSSH
- Logging and remote logging
- Auditing

# Summary: Stepping forward with a secure environment

Thank you very much



# Questions ?

# Reference Information

- Security zones on z/VM presentation
  - http://www.VM.ibm.com/devpages/altmarka/present.html
- z/VM Security resources
  - http://www.VM.ibm.com/security
- z/VM Secure Configuration Guide
  - http://publibz.boulder.ibm.com/epubs/pdf/hcss0c00.pdf
- System z Security
  - http://www.ibm.com/systems/z/advantages/security/
- z/VM Home Page
  - http://www.VM.ibm.com