

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

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

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
- Bildschirmschoner
- Mobil-Angebote
- WAP-Dienste
- Newsletter
- RSS-Angebot
- Nachrichtenbanner
- Sidebar

PlayStation Network: Hacker klauen 77 Millionen Kundendaten

Sony sperrt Online-Dienste - Racheakt aus der Szene?

Gigantischer Datenklau. Hacker haben Passwörter, Adressen und möglicherweise auch Kreditkarten-Nummern von 77 Millionen Sony-Kunden gestohlen. Betroffen ist vor allem das PlayStation Network. Ist der Angriff eine Racheaktion aus der Hacker-Szene?

Drucken | Versenden | 27.04.2011

börsenkurs

SONY
Kurs
19,91 ↓
Datum/Zeit
27.04. 09:30:06
Vortag Änderung
20,35 -2,19%

Börse: XETRA
Kurs ID nicht verzögert
Indizes: realtime

Charts und weitere Informationen
Quelle: Teledata / Innovative Software

Daten-Klau bei Sony: Hacker haben Informationen von Millionen Nutzern der Online-Dienste PlayStation Network und des Video- und Musikservices Qriocity erbeutet. Der japanische Elektronik-Riese hatte nach dem Hacker-Angriff vor einer Woche den Stecker gezogen und die Dienste abgeschaltet.

Passwörter ausgespäht

Eine unbekannte Person habe sich Zugang zu persönlichen Daten wie Name, Adresse, E-Mail oder Geburtsdatum verschafft, schrieb Sony in Firmenblogs weltweit und informierte die Betroffenen. Auch Logins und Passwörter seien nach derzeitigem Kenntnisstand ausgespäht worden, möglicherweise auch die Liste der Käufe.

ZDFmediathek

- Video iPhone speichert Positionsdaten
- Video Weiter viele Mängel beim Datenschutz
- Video "Digitaler Radiergummi"

zur ZDFmediathek

Links

- Thema Daten in Gefahr

Kundenkarten: Datenstriptease beim Wäscheaufkäuf
Was wir beim Einkaufen per Kundenkarte über uns verraten

Der Spion, der in der Kleidung steckt
Neue Technologien bringen neue Probleme für den Datenschutz

Wo Datenjäger im Alltag lauern
Gewinnspiele, Online-Shops und weitere Fallen - ein Überblick

Interaktiver Krimi

- Sendung Wer rettet Dina Foxx?

E-MAIL UND VERSCHLÜSSELUNG

E-Mail

PGP

- ⊙ 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

PGP

- ⊙ 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

E-Mail

PGP

- ⊙ 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

E-Mail

PGP

- ⊙ 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

E-Mail

PGP

- ⊙ Alles gute Gründe E-Mails zu verschlüsseln.
Aber -

**Warum macht das
niemand ?**

E-MAIL UND VERSCHLÜSSELUNG

E-Mail

PGP

- ⊙ 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




Geschichte Profil Freeware Produkte Shrinkware

Pi-Systemprogrammierungs-GmbH



Teichstraße 39E
63225 Langen
tel: 06103-71254
tagsüber: 0171-850 7132
Email: info@pi-sysprog.de

 for a version in english click here

„What can happen when you put your CICS on the web“

Martin Trübner

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

The screenshot shows a web browser window titled "J-51 Abatement History Menu - SeaMonkey". The address bar displays the URL "https://webapps.nyc.gov:8084/cics/cwbs/dfhwbttta/abht". The browser's search bar contains "Suchen". The page content is organized into a sidebar with navigation links: HOME, PROPERTY, PARKING & VEHICLES, BUSINESS TAXES, OTHER SERVICES, FORMS & PUBLICATIONS, ABOUT FINANCE, and CONTACT FINANCE. The main content area is titled "J-51 Benefit History Request Screen" and includes a "Disclaimer" link. Below the title, it prompts the user to "Please enter all fields:" and provides input fields for "Borough:" (a dropdown menu), "Block:" (a text box), "Lot:" (a text box), and "Tax Year:" (a dropdown menu set to "2010/2011"). There are "Reset" and "Tax Year Summary" buttons, and a "SEARCH" button at the bottom left. Below the form, there is a "J-51 Explanation" section with text describing the program, a "J-51 Program Information" link, and a "Disclaimer" section with four numbered points. At the bottom, there is contact information for the Exemptions Section - J51 and a copyright notice for 2005 The City of New York.

J-51 Benefit History Request Screen [Disclaimer](#)

PROPERTY [J-51 Explanation](#)

PARKING & VEHICLES Please enter all fields:

BUSINESS TAXES Borough:

OTHER SERVICES Block:

FORMS & PUBLICATIONS Lot:

ABOUT FINANCE Tax Year:

CONTACT FINANCE

J-51 Explanation

The J-51 benefit program of the City of New York is a tax incentive for the renovation of multiple unit residential buildings. The Department of Housing, Preservation and Development (HPD) administers the program and handles all applications for it. The Department of Finance applies the HPD approved benefits to real property assessed value and taxes.

The program includes two benefits, both based on the certified cost of building alteration. (1) The J-51 Exemption reduces the taxable assessed value, which is the basis for calculating Real Estate Taxes. (2) The J-51 Abatement reduces the actual tax that has been charged against a property.

[J-51 Program Information](#)

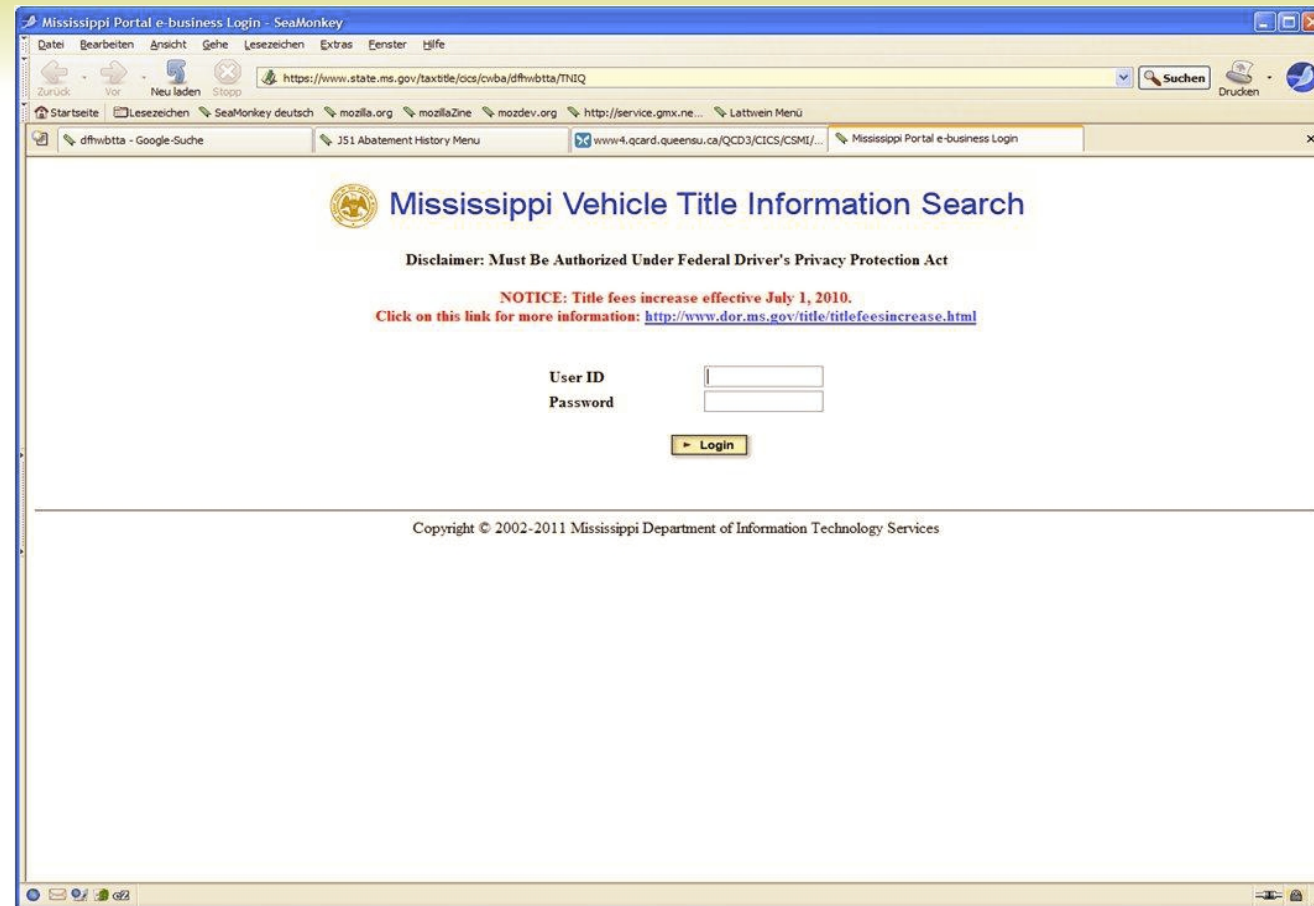
Disclaimer

1. The J-51 Benefit History is for informational purposes only. It contains information that may be currently under review. The information shown may not show data that has been added or changed in the last 7 days. Recent changes shown may not yet have affected billing.
2. The Department of Finance records are updated regularly. If you believe there are any inaccuracies as to the information contained on these pages or if you need updated information, please contact the Department of Finance.
3. You may not be entitled to the credits appearing on these pages. To verify entitlement please contact the Department of Finance.
4. To reach the Department of Finance J51 Abatement Unit write to:

Exemptions Section - J51
P.O.Box 3120
Church Street Station
New York, NY 10007-3120

Copyright 2005 The City of New York [Contact Us](#) | [FAQs](#) | [Privacy Statement](#) | [Site Map](#)

WWW.STATE.MS.GOV



QUEEN UNIVERSITY CA

ASQ - Queen's University - SeaMonkey

https://www.asq.queensu.ca/asq1/cics/csm/dfhwbtta/aw01

Suchen Drucken

Starthome Lesezeichen SeaMonkey deutsch mozilla.org mozillaZine mozdev.org http://service.gmx.ne... Lattwein Menü

dfhwbtta - Google-Suche JS1 Abatement History Menu www4.qcard.queensu.ca/QCD3/C... Mississippi Portal e-business Login NYC Property Search NYC ASQ - Queen's University

Queens UNIVERSITY

Sign off

ASQ Sign-On
**** PLEASE ENTER YOUR REFERENCE NUMBER OR STUDENT NUMBER ****

For OUAC Applicants
Please enter your OUAC reference number. This number can be found on your copy of your application or on the OUAC acknowledgement/amendment form.

OUAC Reference Number:
 Please enter the full 2010 at the beginning of your OUAC Reference number. (2010*****) Please enter the final digit (11th) as a zero.

Enter your date of birth, following the format below. If you have not included your date of birth on your OUAC application, you should amend your application using the Amendment/Verification Form that was sent to you. Otherwise you will not be able to access ASQ. After entering your Reference Number and date of birth please click the PROCEED button to continue.

Date of Birth: (yyyy mm dd)

For Current Queen's Students
Student Number: Enter your student number and date of birth (following the instructions above). Click PROCEED to enter.

Your PSE
The PSE is required by all first-year, full-time undergraduate programs and Education programs.

March Break Open House
Experience Queen's!
March 18, 19, 2010

English Requirements
The language of instruction at Queen's is English. Click to learn more about our requirements.

©2007 Queen's University
Admission Services - Office of the University Registrar
Gordon Hall
Queen's University
Kingston, Ontario, Canada
K7L 3N6
admission@queensu.ca

NEW ORLEANS: ACCOUNTS.SWBNO.ORG:8010

Online Payment System - Sewerage and Water Board of New Orleans - SeaMonkey

https://accounts.swbno.org/dics/cvba/dfhwbtta/wa37

Sewerage and Water Board of New Orleans

Customer Service

HOME > Customer Service >> View & Pay Your Bill Online >>> Find Account Number >>>

Payment Locations

View & Pay Bill Online

Customer Information

Close an Account

Report a Leak/Problem

Ask a Question

Change Mailing Address

Sanitation

Contact Us

What do you want to do?

What do you want to know?

Search the Site

Find Account Number

In an effort to make your information more secure, we have disabled the online Find Account Number feature. To find your account number, please retrieve a recent water bill and locate your account number in one of the two locations outlined on the sample bill below.

Sewerage and Water Board of New Orleans

423 Sibley Joseph St.
New Orleans, LA 70145-4307
529-2637 • TDD 529-2499
www.swbno.org

Amount Due \$ 129.94

Amount Due \$ 129.94

Late Payment \$ 141.58

PAST DUE BALANCE

Service For: 1111 ALABAMA STREET Account 115468-02-0

Reading Date	Reading (100)	Bill Type	Meter Usage (100 gal)	Number of Days Usage	Ave Usage/Day (100 gal)
THIS BILL 06/01/07	4,800	R	198.0	22	9.00
Last Bill 04/09/07	4,602	E	0.0	40	0.00
Last Year 09/30/06	4,093	E	0.0	98	0.00

Meter: 8/8" Class

A292815 8/8" RESIDENTIAL

Previous Bill	(-) Payments Thru 05/09/07	(+) Adjustments	(+) Late Fees	(-) Balance Forward
0.00	0.00	0.00	0.00	000.00

Sewerage and Water Board

WATER USAGE \$9.91 / 1000 GAL 45.74

WATER SERVICE CHARGE 3.50

CITY SALES TAX 2.905

SEWER VOLUME CHARGE \$4.04 / 1000 GAL 67.87

SEWER SERVICE CHARGE 11.60

25.0% of the above sewer charges provides funding to comply with the Federal Consent Decree between the SWB and the Environmental Protection Agency.

City of New Orleans

CITY SANITATION CHARGE .00

MUNICIPALITY OF ANCHORAGE

SeaMonkey

http://property.muni.org/oc/cvba/dfwbtt/TX:IP+0907602121000XXXXXXXXXXXXXXXXXXXXIMAGWORD2009

MUNICIPALITY OF ANCHORAGE

Home Residents Businesses Government Visitors Departments Public Safety

Departments > Finance > Property Taxes > New Search > results

Account Key: 076-021-21-000 Tax Year: 2009

Name: WEAVER SHELBY C

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

632 W. 6th Avenue Anchorage, Alaska 99501
PO Box 196650 Anchorage, Alaska 99519

STATE OF NEVADA

The screenshot shows a web browser window titled "UI Internet Claims Logon Screen - SeaMonkey". The address bar displays the URL "https://inccp.nvdetr.org/cics/cwba/dfhwbttb/euls". The browser's menu bar includes "Datei", "Bearbeiten", "Ansicht", "Gehe", "Lesezeichen", "Extras", "Fenster", and "Hilfe". The browser's toolbar contains navigation buttons (Zurück, Vor, Neu laden, Stopp) and a search bar with the text "Suchen". The browser's address bar shows several open tabs, including "dfhwbttb - Goo...", "J51 Abatement...", "www-4.qcard.q...", "Mississippi Port...", "ASQ - Queen's ...", "accounts.swbn...", "http://.RD2009", "Ask a question ...", "12300_Old_Gle...", "Cics 88 414 | A...", and "UI Internet Cl...".

The main content area of the browser displays the "State of Nevada" logo and the text "Department of Employment, Training & Rehabilitation" and "Nevada Internet Claims". Below this, the heading "UI Login" is displayed with a key icon. The login form consists of the following fields and buttons:

- Social Security Number:** A field with a hyphen and a box for each digit.
- Personal Identification Number (PIN):** A field with a "Help" button.
- Security Verification:** A field with a "Reload Image" button.
- Buttons:** "Exit", "Back", "Print", and "LOGIN".
- Link:** "Forgot Your PIN or Need a new PIN? Click to get a new PIN".

UND WIE SICHER SIND UNSERE STANDARD ANWENDUNGEN

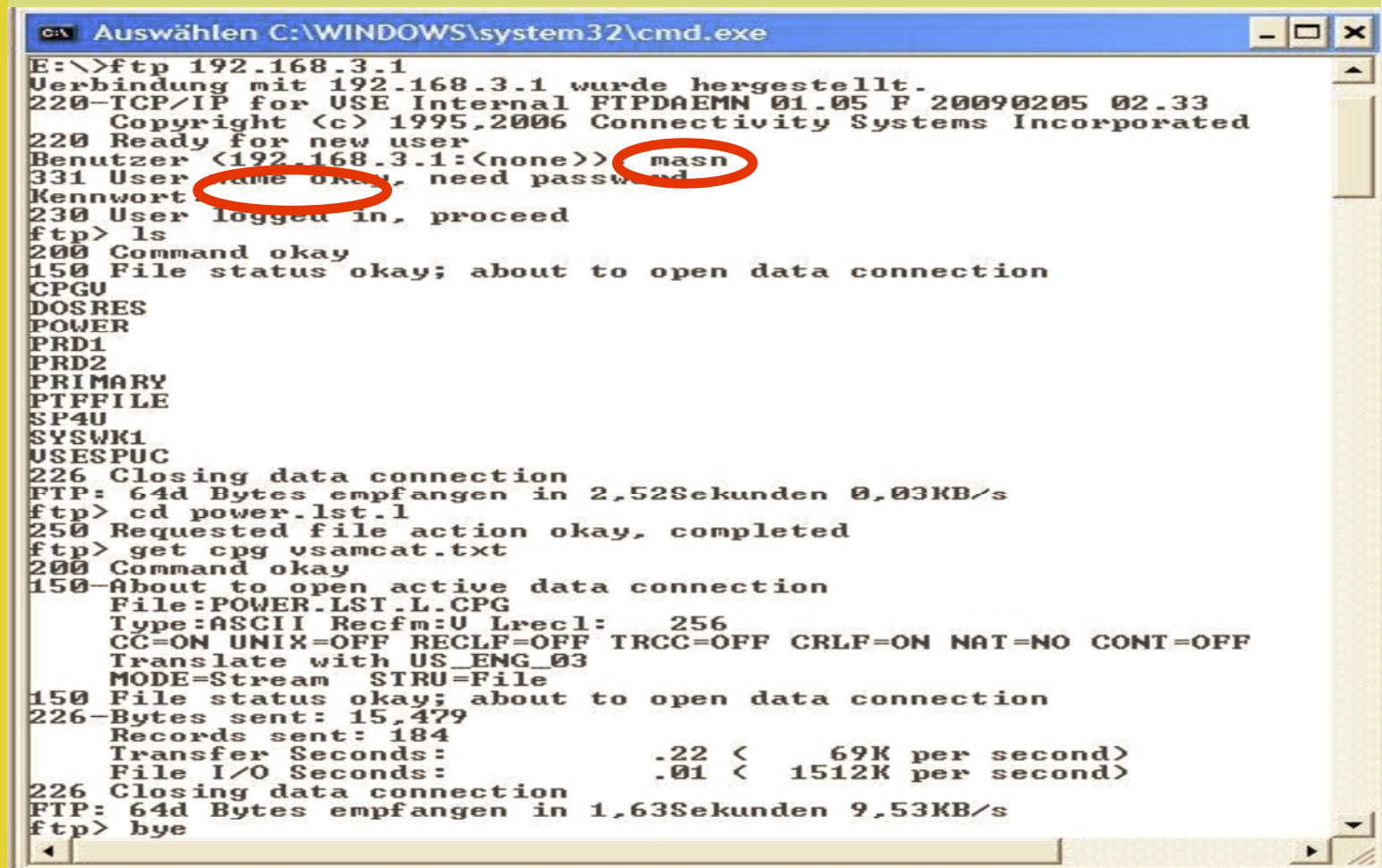
- ⊙ Auch Inhouse Anwendungen sind nicht sicher!
- ⊙ Sei es CICS Sign-ON über Telnet
- ⊙ FTP von oder zum z/VSE
- ⊙ Email im zVSE versendet

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 normalerweise 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“).

Command Fenster
mit FTP zum
z/VSE.
TCPIP 1.5.F



```
E:\>ftp 192.168.3.1
Verbindung mit 192.168.3.1 wurde hergestellt.
220-TCP/IP for USE Internal FTPDAEMN 01.05 F 20090205 02.33
    Copyright (c) 1995,2006 Connectivity Systems Incorporated
220 Ready for new user
Benutzer (192.168.3.1:(none)) masn
331 User name okay, need password
Kennwort
230 User logged in, proceed
ftp> ls
200 Command okay
150 File status okay; about to open data connection
CPGU
DOSRES
POWER
PRD1
PRD2
PRIMARY
PTFFILE
SP4U
SYSWK1
USESPUC
226 Closing data connection
FTP: 64d Bytes empfangen in 2,52Sekunden 0,03KB/s
ftp> cd power.lst.l
250 Requested file action okay, completed
ftp> get cpg vsamcat.txt
200 Command okay
150-About to open active data connection
File:POWER.LST.L.CPG
Type:ASCII Recfm:U Lrecl: 256
CC=ON UNIX=OFF RECLF=OFF TRCC=OFF CRLF=ON NAT=NO CONT=OFF
MODE=Stream SIRU=File
150 File status okay; about to open data connection
226-Bytes sent: 15,479
Records sent: 184
Transfer Seconds: .22 ( 69K per second)
File I/O Seconds: .01 ( 1512K per second)
226 Closing data connection
FTP: 64d Bytes empfangen in 1,63Sekunden 9,53KB/s
ftp> bye
```


FTP DAEMON RESPONSE

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

Wireshark capture showing FTP daemon response. The packet list shows a sequence of packets from 192.168.197.40 to 192.168.3.1. Packet 16 is expanded to show the FTP response '220 Ready for new user'.

No.	Time	Source	Destination	Protocol	Info
9	4.515284	192.168.197.40	192.168.3.1	TCP	17566 > ftp [ACK] Seq=1 Ack=1 win=65535 [TCP CHECKSUM INCORRECT
10	4.521980	192.168.3.1	192.168.197.40	FTP	Response: 220-TCP/IP for VSE Internal FTPDAEMN 01.05 F 20090205
11	4.531205	192.168.3.1	192.168.197.40	TCP	htuilsrv > 16603 [PSH, ACK] Seq=1 Ack=1 win=65534 Len=106
12	4.653894	192.168.197.40	192.168.3.1	TCP	17566 > ftp [ACK] Seq=1 Ack=62 win=65474 [TCP CHECKSUM INCORREC
13	4.653904	192.168.197.40	192.168.3.1	TCP	16603 > htuilsrv [ACK] Seq=1 Ack=107 win=65429 [TCP CHECKSUM IN
14	4.658183	192.168.3.1	192.168.197.40	FTP	Response: Copyright (c) 1995,2006 Connectivity Systems Inco
15	4.855059	192.168.197.40	192.168.3.1	TCP	17566 > ftp [ACK] Seq=1 Ack=125 win=65411 [TCP CHECKSUM INCORRE
16	4.858520	192.168.3.1	192.168.197.40	FTP	Response: 220 Ready for new user

Expanded packet 16 details:

- Frame 16 (78 bytes on wire, 78 bytes captured)
- Ethernet II, Src: Broadcom_3d:41:5d (00:10:18:3d:41:5d), Dst: 00:22:19:23:05:5a (00:22:19:23:05:5a)
- Internet Protocol, Src: 192.168.3.1 (192.168.3.1), Dst: 192.168.197.40 (192.168.197.40)
- Transmission Control Protocol, Src Port: ftp (21), Dst Port: 17566 (17566), Seq: 125, Ack: 1, Len: 24
- File Transfer Protocol (FTP)
 - 220 Ready for new user\r\n
 - Response code: Service ready for new user (220)
 - Response arg: Ready for new user

Hex dump of packet 16:

```

0000 0000 0000 00 22 19 23 05 5a 00 10 18 3d 41 5d 08 00 45 00  .".#.Z... [=A]..E.
0010 0010 0010 00 40 73 cc 00 00 fd 06 00 71 c0 a8 03 01 c0 a8  .@s..... .q.....
0020 0020 c5 28 00 15 44 9e 60 2f 11 b2 22 ea 05 e2 50 18  .(.D.\/ .."...P.
0030 0030 ff fe 51 98 00 00 32 32 30 20 52 65 61 64 79 20  ..Q...22 0 Ready
0040 0040 66 6f 72 20 6e 65 77 20 75 73 65 72 0d 0a  for new user..
0050 0050
0060 0060
0070 0070
  
```

FTP USER MASN

Userid und
Passwort im
Klartext !

(Untitled) - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: (ip.addr eq 192.168.3.1 and ip.addr eq 192.168.197.40) Expression... Clear Apply

No. -	Time	Source	Destination	Protocol	Info
9	4.953591	192.168.3.1	192.168.197.40	FTP	Response: 220 Ready for new user
10	5.168833	192.168.197.40	192.168.3.1	TCP	16693 > ftp [ACK] Seq=1 Ack=149 win=65535
14	8.834804	192.168.197.40	192.168.3.1	FTP	Request: USER masn
15	8.839620	192.168.3.1	192.168.197.40	TCP	ftp > 16693 [ACK] Seq=149 Ack=12 win=65535
16	8.840910	192.168.3.1	192.168.197.40	FTP	Response: 331 User name okay, need password
25	9.106232	192.168.197.40	192.168.3.1	TCP	16693 > ftp [ACK] Seq=12 Ack=184 win=65535
38	12.866749	192.168.197.40	192.168.3.1	FTP	Request: PASS geheim
39	12.874149	192.168.3.1	192.168.197.40	TCP	ftp > 16693 [ACK] Seq=184 Ack=25 win=65535
40	12.875698	192.168.3.1	192.168.197.40	FTP	Response: 230 User logged in, proceed

Frame 40 (83 bytes on wire, 83 bytes captured)

- Ethernet II, Src: Broadcom_3d:41:5d (00:10:18:3d:41:5d), Dst: 00:22:19:23:05:5a (00:22:19:23:05:5a)
- Internet Protocol, Src: 192.168.3.1 (192.168.3.1), Dst: 192.168.197.40 (192.168.197.40)
- Transmission Control Protocol, Src Port: ftp (21), Dst Port: 16693 (16693), Seq: 184, Ack: 25, Len: 29
- File Transfer Protocol (FTP)

```

0000  00 22 19 23 05 5a 00 10 18 3d 41 5d 08 00 45 00  .".#.Z... [=A]..E.
0010  00 45 d9 b9 00 00 fd 06 9a 7e c0 a8 03 01 c0 a8  .E..... ~.....
0020  c5 28 00 15 41 35 40 43 dd 7b cb ac 51 0e 50 18  .(..A5@C .{..Q.P.
0030  ff fe 29 08 00 00 32 33 30 20 55 73 65 72 20 6c  ..)...23 0 User 1
0040  6f 67 67 65 64 20 69 6e 2c 20 70 72 6f 63 65 65  ogged in , procee
0050  64 0d 0a                                          d..
  
```

File: "C:\DOKUME~1\Maassen2\LOKALE~1\Temp\etherXXXa05488" 40 KB 00:01:29 Packets: 247 Displayed: 63 Marked: 0 Dropped: 0

FTP FOLLOW TCP STREAM

FTP LS Data

```
220-TCP/IP for VSE Internal FTPDAEMN 01.05 F 20090205 02.33
  Copyright (c) 1995,2006 Connectivity Systems Incorporated
220 Ready for new user
USER masn
331 User name okay, need password
PASS geheim
230 User logged in, proceed
PORT 192,168,197,40,65,55
200 Command okay
NLST
150 File status okay; about to open data connection
226 closing data connection
CWD power.lst.1
250 Requested file action okay, completed
PORT 192,168,197,40,65,58
200 Command okay
RETR cpg
150-About to open active data connection
  File:POWER.LST.L.CPG
  Type:ASCII Recfm:V Lrecl: 256
  CC=ON UNIX=OFF RECLF=OFF TRCC=OFF CRLF=ON NAT=NO CONT=OFF
  Translate with US_ENG_03
  MODE=Stream STRU=File
150 File status okay; about to open data connection
226-Bytes sent: 15,479
  Records sent: 184
  Transfer Seconds: .22 ( 69K per second)
  File I/O Seconds: .01 ( 1512K per second)
226 Closing data connection
QUIT
221 FTPDaemn closing control connection
```

PASSWORT SCHUTZ

Passwörter

Was ein sicheres Passwort ist:

Wa\$ 31n 51ch3r3\$ Pa5\$w0r7 157

Wa\$ 31n 51ch3r3\$ Pa5\$w0r7 157

Wa\$ 31n 51ch3r3\$ Pa5\$w0r7 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 ?

```
Sitzung B - [24 x 80]
Datei Bearbeiten Anzeige Kommunikation Aktionen Fenster Hilfe
Signon to CICS APPLID CICSTEST

VSE/ESA CICS2

Type your userid and password, then press ENTER:

  Userid . . . . masn
  Password . . . .
  Groupid . . . .
  Language . . . .

  New Password . . . .

DFHCE3520 Please type your userid.
F3=Exit

MA b 11/032
Verbindung zum fernen Server/Host 192.168.3.1 aufgebaut über LU/Pool LATNT202 und Anschluss 5023. \\PSEVER\\Lexmark Optra Lxi EIN LPT1:
```


CESN USER/PASSWORD

Nicht falls man
EBCDIC Hex lesen
kann !

Geht aber auch
im Klartext . . .

The screenshot shows a 'Follow TCP Stream' window. The 'Stream Content' field displays a hex string: `..... 'A&CESN..... '<'..ZMASN.<9GEHEIM... ..' cqtf.....!'...$v....."...`. A red circle highlights the segment `'<'..ZMASN.<9GEHEIM...`. A callout box with a green arrow points to this segment, containing the text: **Hier steht die UserId und das Passwort !**

Below the stream content, the 'Find' button is active, and the 'EBCDIC' radio button is selected. The 'Data' field shows the hex dump: `0000 00 a0 f9 10 59 ea 00 22 18 23 05 5a 08 00 45 00`. A red circle highlights the hex sequence `d4 c1 e2 d5 11 4c f9 c7 c5 c8 c5 c9 d4 ff ef`.

A callout box at the bottom right of the hex dump contains the text: **d4 c1 e2 d5 = 'MASN' | c7 c5 c8 c5 c9 d4 = 'GEHEIM'**

EMAIL IM ZVSE TRACE

- ⊙ Wie bei IPTRACE dokumentiert, kann Email Traffic 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

```

Follow TCP Stream
Stream Content
UCAT220          C KSDS 2003.065      0 91%  1%  0%  0%  0% ** INDEX LEVELS > 2  98
TXTVSM. DATA   D   170  170  2048  64  0    21    0    0    5  1  23
VSAM. CATALOG. BASE. INDEX. RECORD  I     0    64    3  26592 1174405122 945 980 33

UMSATZ. ZWIBER. K2101      C ESDS 2001.061 2001.068 99%  0%  0%  0%  59% ** ZU GROSS > 50 %
TA1040D0. VSAMDSET. DFD01061. TB579439. TA1040D0 D  4080  4080  8192    0    90    1  13

VORLAUF. KARTE. UMSATZ     C ESDS 2001.059 2001.066 99%  0%  0%  0%  96% ** ZU GROSS > 50 %
T959E863. VSAMDSET. DFD01059. TB576DB0. T959E863 D  4080  4080  4096    0    24    1  13

VSE260. CPGWKL. TEMP      C KSDS 2007.222      0 98%                                ** NO. EXTENTS > 3
VSE260. CPGWKL. DATA. TEMP D   100  2040  2048  40  0   126   19636  10  23
VSE260. CPGWKL. INDEX. TEMP I     0  2553  2560  40    17    20  2  2 23

XXX. ZENTRAL. ARTIKEL. STAMM. KSDS  C KSDS 2006.072 1999.366 99%  0%  0%  0%  75% ** ZU GROSS > 50 %
XXX. ZENTRAL. ARTIKEL. STAMM. KSDS. .D. D   406  406  4096  7  0    12    100  1  23
XXX. ZENTRAL. ARTIKEL. STAMM. KSDS. .I. I     0  505  512  7  49    3  1  2 23

ZSART            C KSDS 1998.114      0 98%  0%  0%  0%  80% ** ZU GROSS > 50 %
ZSART. DATA    D   200  200  2048  7  0   126    94  1  23
ZSART. INDEX    I     0  1529  1536  7  26    1  1  1 23

CLUSTER - TOT      93.
EOJ CPG                                DATE 03/01/2011, CLOCK 12/34/22, DURATION 00/00/01
-----_C73CF06A4CD09000==_--
.
250 2.6.0 <C73CF06A4CD09000@LWSERVER03> Queued mail for delivery
QUIT
221 2.0.0 lattwein.de service closing transmission channel|

Find Save As Print Entire conversation (16763 bytes)
 ASCII  EBCDIC  Hex Dump  C Arrays  Raw

Help Close Filter Out This Stream
  
```


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

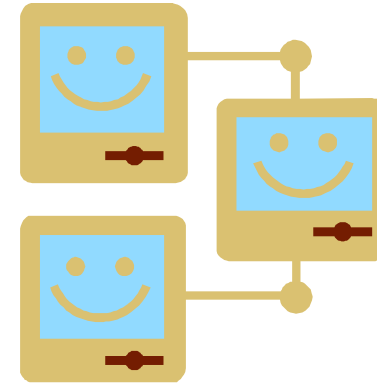
Gefahren in der IT – Ist Ihre Produktion sicher vor Angriffen?



TCP/IP Security

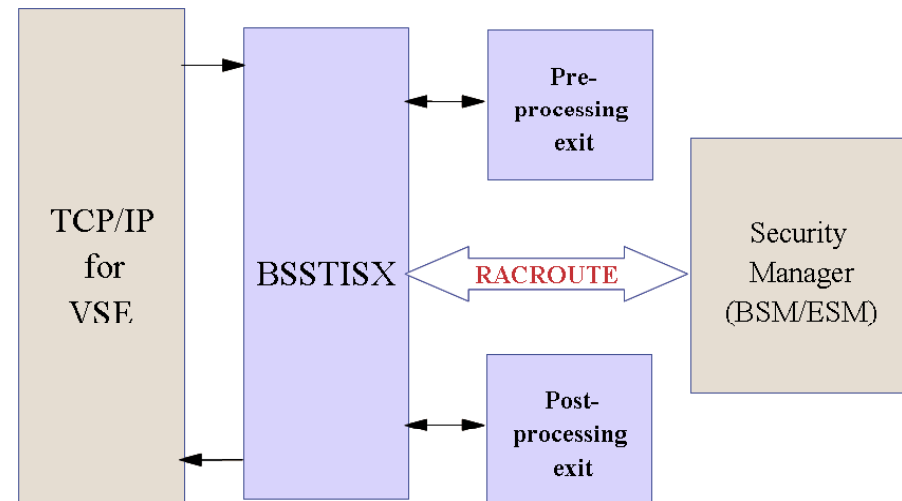
- **In general TCP/IP uses its own user id definitions**

- 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

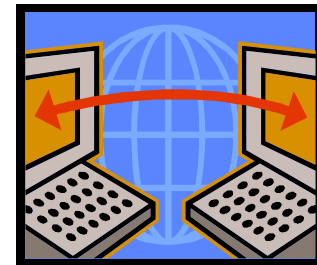


Cryptography and data encryption

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

Cryptography uses **Keys** and **Certificates**

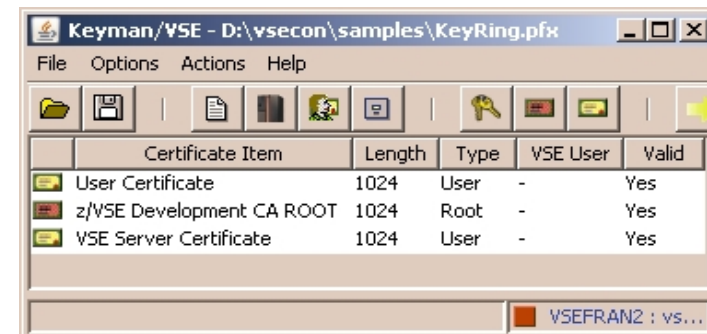
- **Key Management is not trivial**

- 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**

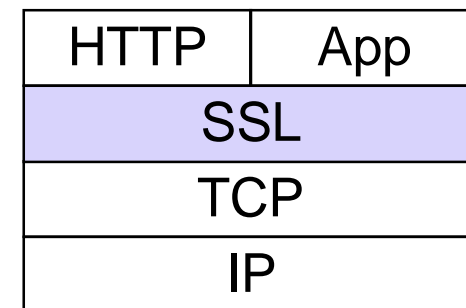
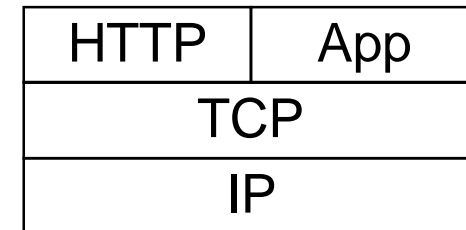
- Creation of RSA keys and digital certificates
- Upload of keys and certificates to VSE
- Creation of PKCS#12 keyring files (use with Java-based connector or import into a Web browser)
- Download from VSE Homepage

<http://www.ibm.com/systems/z/os/zvse/downloads/#vkeyman>

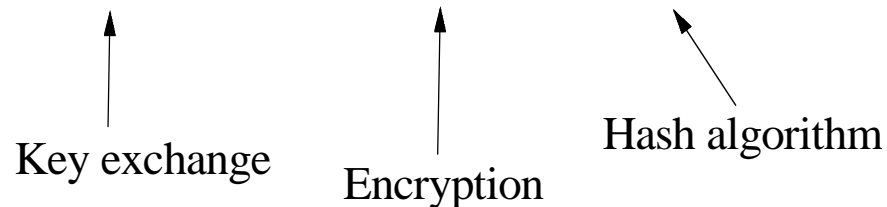


Secure Socket Layer – Encrypted data transfer over a network

- **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



SSL_RSA_WITH_DES_CBC_SHA

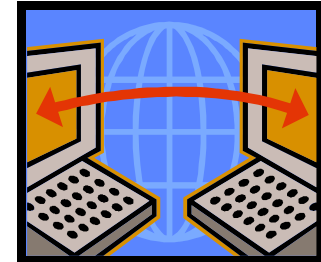


SecureFTP

- **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 TLS D:**

DEFINE TLS D, ID=TLS DTELNET,	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 TLS D 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](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	-	-	-

	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

by server



CEX2C = Crypto Express2/3 in coprocessor mode

CEX2A = Crypto Express2/3 in accelerator mode

See: <http://www.ibm.com/systems/z/security/cryptography.html>



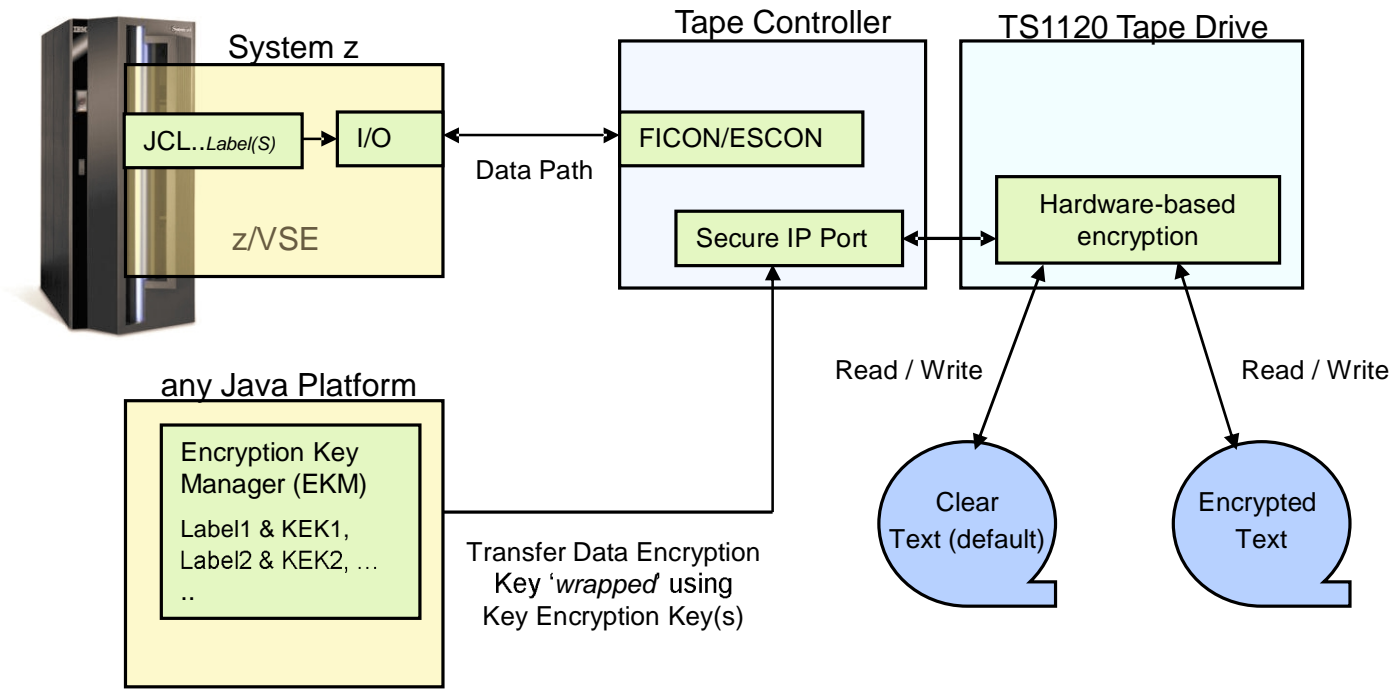
VSE Hardware Configuration

- **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



```

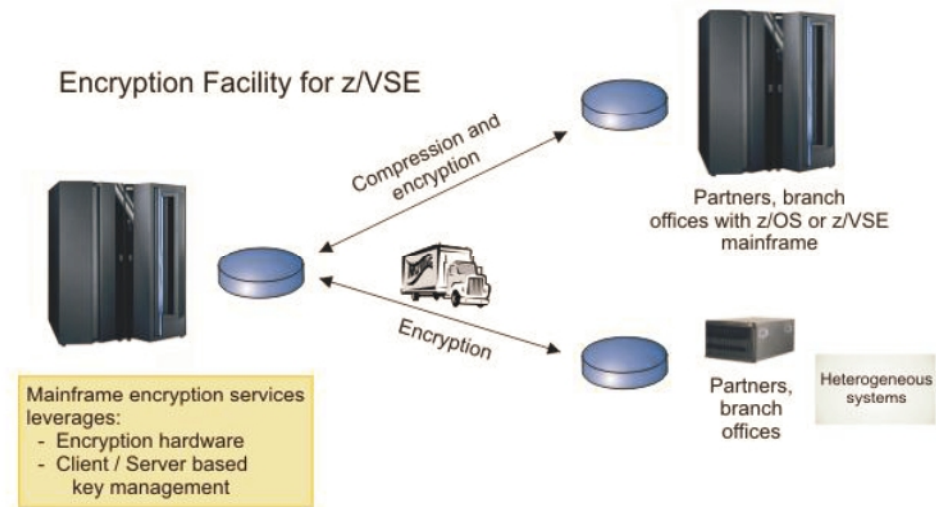
// JOB ENCRYPT
// ASSGN SYS005,480,03
// KEKL UNIT=480,KEKL1='MYKEKL1',KEM1=L,KEKL2='MYKEKL2',KEM2=L
// EXEC LIBR
  BACKUP LIB=PRD2 TAPE=SYS005
/*
/&
    
```

encryption mode (03=write)
 key label1 (name of the 1. KEK-key in EKM)
 encoding mechanism (L=Label, H=Hash)



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, described 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

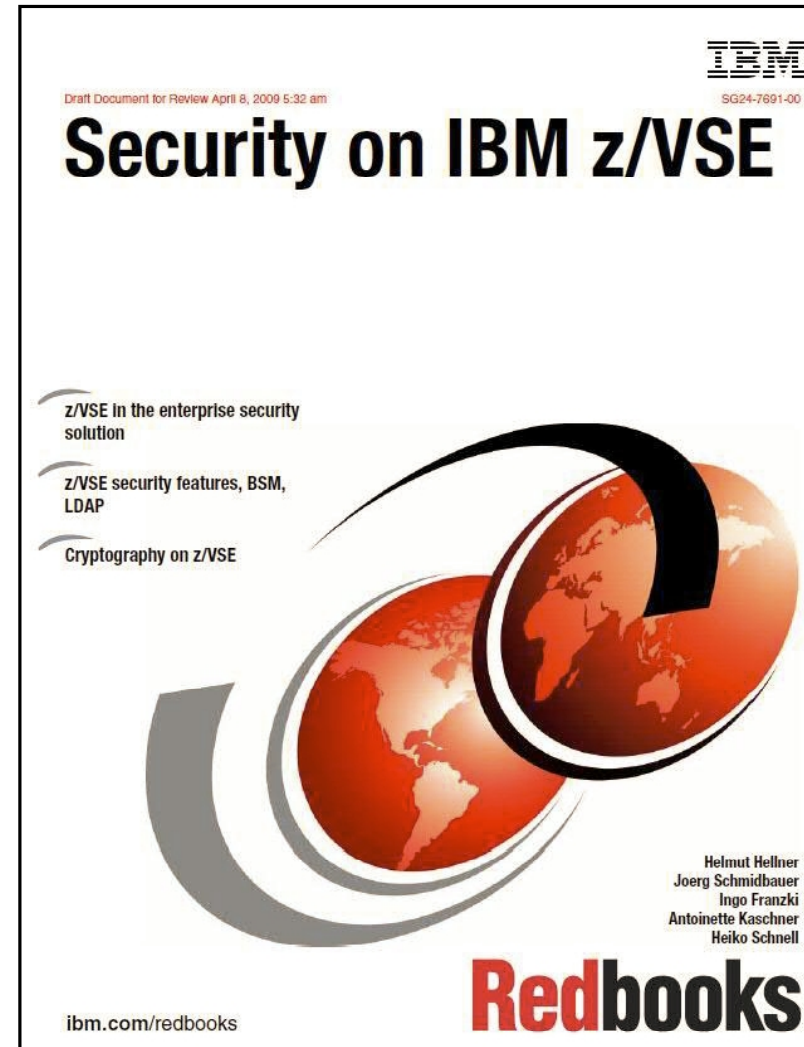
Available since October 20, 2009

<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

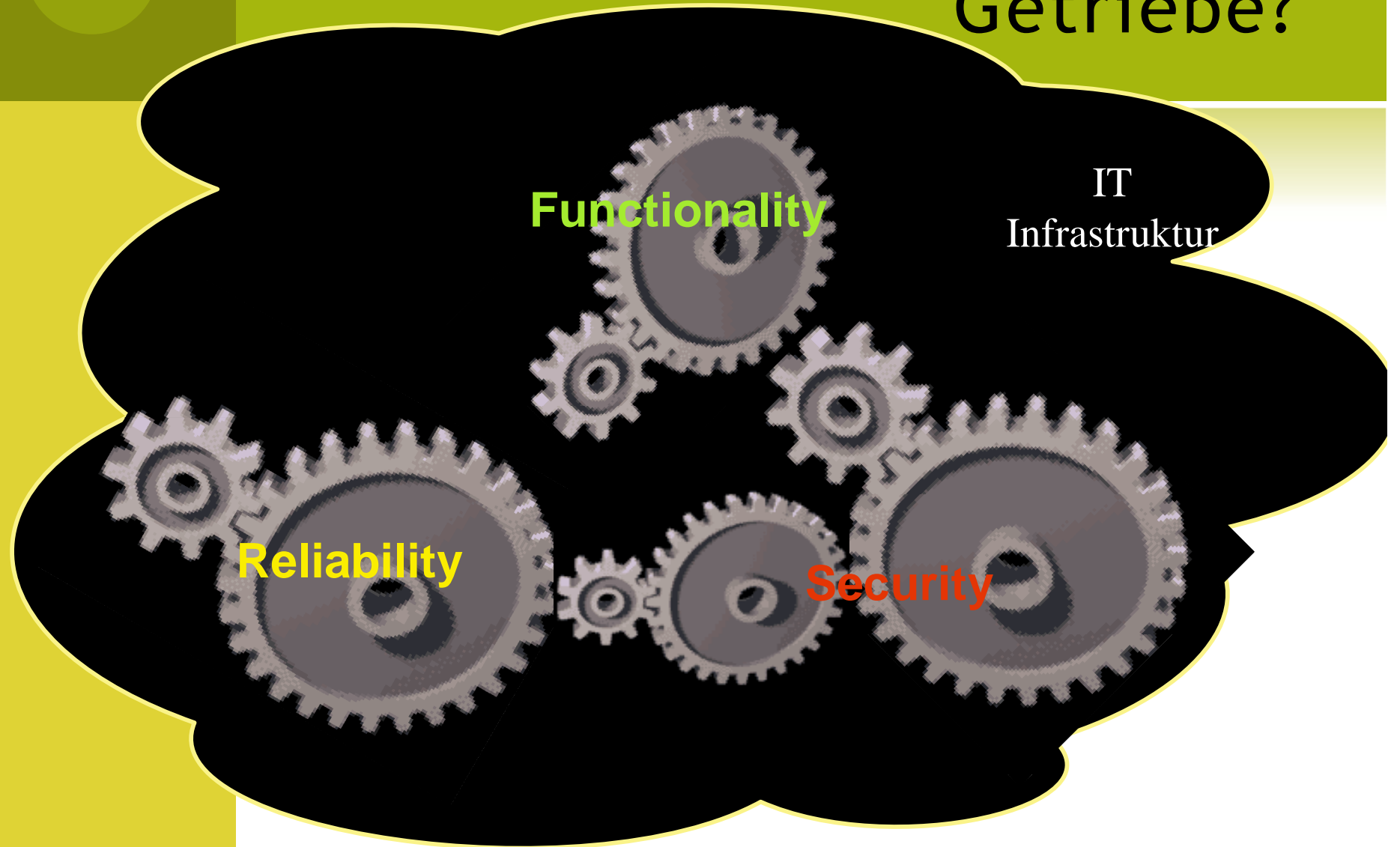


Questions ?



Fortsetzung Dr. Manfred Gnirss, IBM Security zVM

Sicherheit: Sand im Getriebe?



Functionality

IT
Infrastruktur

Reliability

Security

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

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

- ⊙ Muss abgesichert 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/atmastr.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/