greenHouse

Singe Sign-On

ON

the system

VNUG 04. September 2013

Carl Weber

greenHouse

Before we get serious …

… a short recap of VNUG 2011

greenHouse

Reminders from last VNUG!

Peace, Love

and

Understanding

Reminders from last VNUG!

Reminders from last VNUG!

Why do cars have brakes?

To slow down?

Why do cars have brakes?

To drive fast!

The better the brakes, the faster you can drive!

What is security for?

To disable and prevent?

What is security for?

To enable and enforce!

The better the security system, the more you can do!

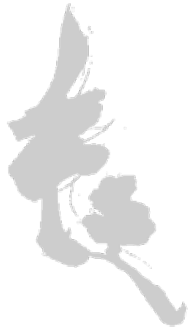
This is your Tandem system!

Or do you treat it like this?

Aspects of security

… just a few …

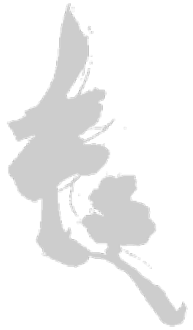
Action	Negative	Positive
Security	Protects (no access)	Enables (access allowed)
Auditing	Controls (depends on the auditor)	Conservation of evidence (it wasn‘t me)
Authentication	… always these logons	No foreigners on the system
Authorization	Prevents (no access)	Allows (except foreigners)
Single Sign-On	Only **ONE** authentication for „n“ Systemen	Just **ONE** authentication for „n“ Systemen



Single Sign-On

- Single Sign ON - what is it?
  ONE secure central authentication for multiple systems and platforms.

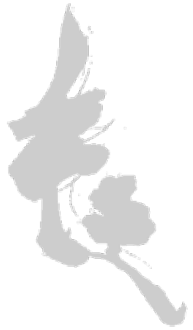
- Sounds perfect – **BUT** is not real life!
  How many ID‘s are used by your system stuff to operate the Tandem system?
  - perform a sysgen and system cold load
  - start/manage/stop an application
  - do a system wide backup
  - get to VPROC
  - etc.



Single Sign-On

- The problem: When you logon to a functional user with a password, you can logon ‚from scratch', loosing all user related attributes, making auditing obsolete.

- The need to know many different password is annoying and leads to complications, e.g. when passwords have to be changed on a regular basis.



Single Sign-On – two views

- From the outside (off the system)
  e.g. products from competitors

- From the inside (on the system)
  ... and here GreenHouse helps:
  - FTPSERV-E Secure Tandem FTP Server
  - MyLogin OFF System SSO für die Tandem
  - SECOM Command Level Security and ID hopping (this presentation)
  - SFTP Secure Tandem FTP Client
  - VILib Secure logon to Visual Inspect Library
  - XDBCLib Secure logon to NSM/Web and MXDM

Single Sign-On

What you think you have

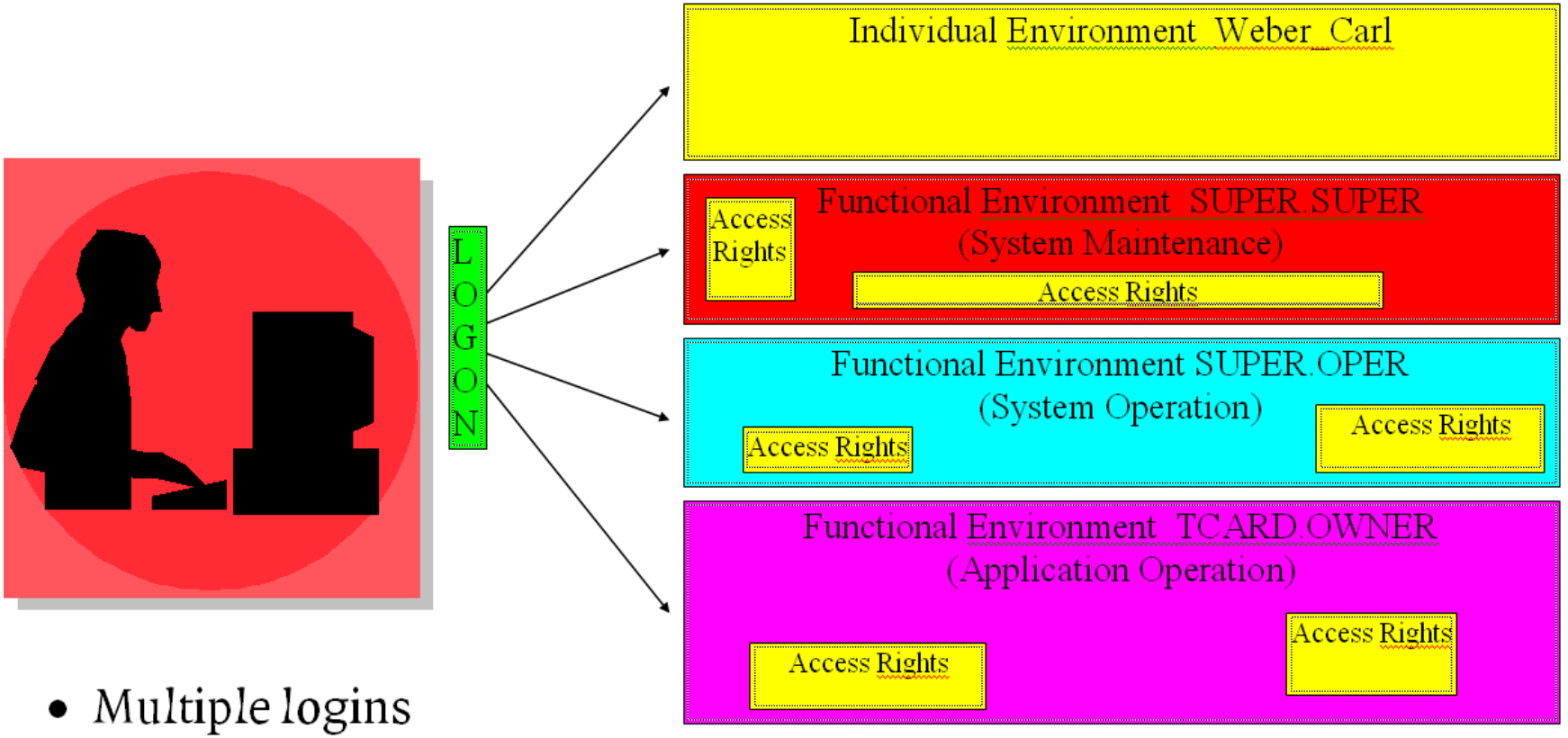
One logon grants access to all user related resources.

LOGON

Users Environment			
Object 1	Object 2	...	Object n
Diskfile	Program		Process
Access Right	Access Right		Access Right
- Read	- Execute		- Read
- Write			- Write
- Purge			- Start
			- Stop

Single Sign-On

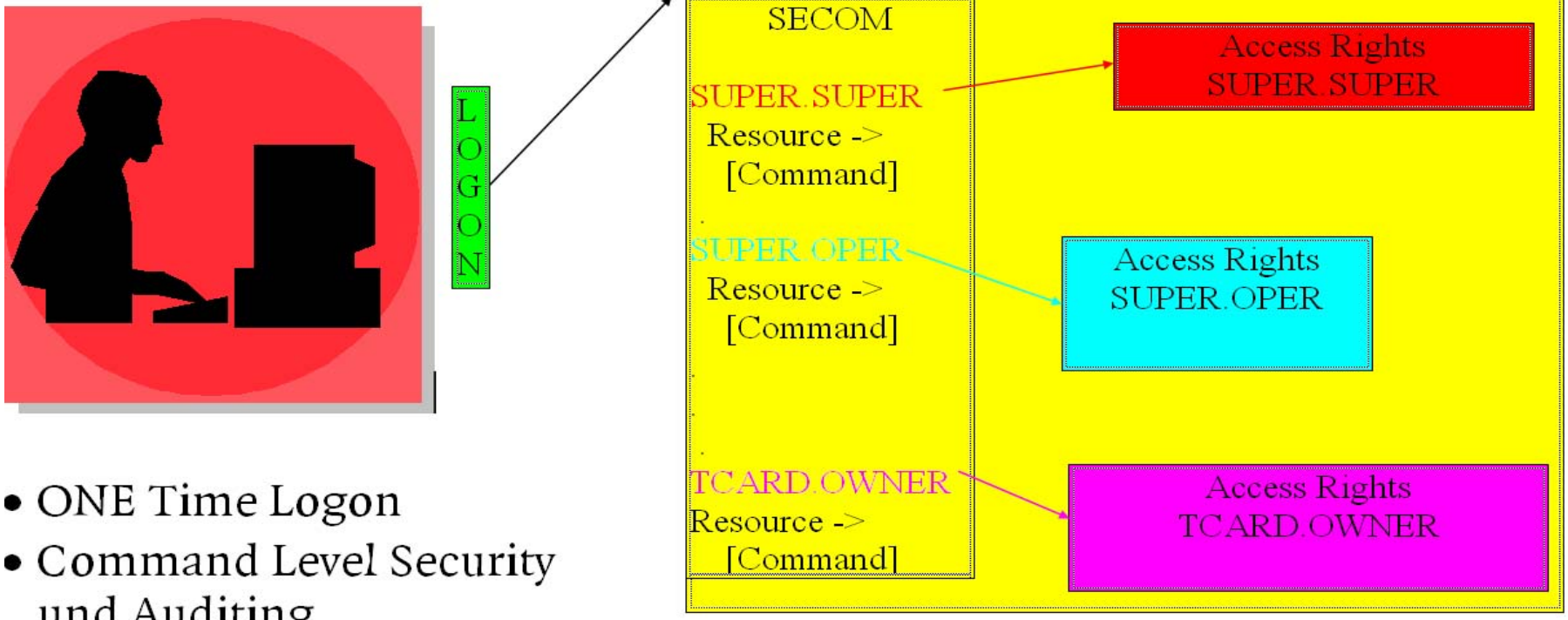
What you really have



- Multiple logins
- No meaningful auditing
- No separation of users and functions

Single Sign-On

What you need



- ONE Time Logon
- Command Level Security und Auditing
- Individualized system access

greenHouse

Single Sign-On
Requirements

- Has to run on a cold loaded system.
  - NO subsystem necessary, such as TMF, SQL, PATHWAY etc.
  - just a ‘naked’ system with a TACL only

- Individual logon to an individual, non PRIV ID.
  (users of SUPER-group do have to many hard coded rights)

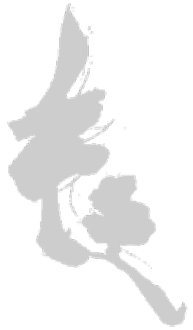
- Access to all IDs required to manage/develop/operate the system WITHOUT any re-logon!

Single Sign-On
Control of functional users

- Control and inspection of ALL functional users in GUARDIAN as well as OSS
  - SUPER.SUPER (255,255)
  - SUPER.xxx (255,xxx)
  - xxx.MANAGER (xxx,255)
  - Application owner (xxx,yyy)

Single Sign-On
Control of functional users

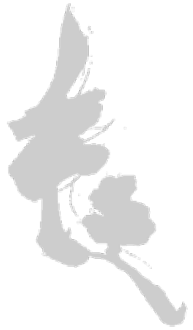
- Support of Alias user specific access rights
- Support of user groups
  - SECOM user groups
  - File Sharing Groups
- Support of command groups
  - EMERGENCY
  - application management
  - etc.



greenHouse

Single Sign-On
Control of functional users

- Command and Subcommand Level Security
  - e.g: FUP INFO xxx,DETAIL is OK, while
    FUP INFOxxx,STAT is NOT
  - device start in SCF is OK, device stop or alter is not
  - access to a SUPER.SUPER TACL is OK,
    while changing the SUPER.SUPER password is not



greenHouse

Single Sign-On
Action control

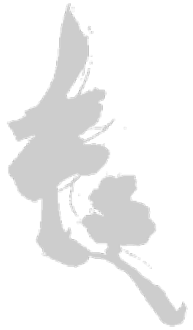
- Controlled access
  - Programs (FUP, SCF, SQLCI etc.)
  - OBEY-Files und TACL-Macros
- Controlled input to programs and macros
  - Command/Sub-Command Level Security
- Controlled access to action streams
  - system cold start/stop, application start, etc.

... and all this with pre-defined access IDs WITHOUT the need to know any (additional) password.

Single Sign-On
Auditing

- Log of all activities (logging)
  - who did what at what time from where und why

- Key stroke recording (tracing)
  - Interactive use of
    GUARDIAN (TACL, FUP, SCF etc.)
    OSS (osh & Co.)
  - Block mode use of
    GUARDIAN resources (EDIT, TEDIT, PATHWAY etc.)
    OSS resources (bash, vi etc.)



Single Sign-On

What you need

Controlled programmatical and transparent resource execution from any ID with any ID

greenHouse

Single Sign-On ON the System

SSO-OS mit

SECOM

Secure Command Manager

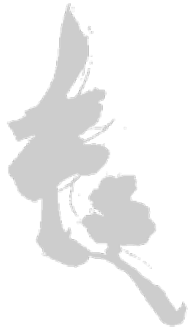
SSO-OS

SECOM versus SAFEGUARD

- SAFEGUARD
  Access rights are attached to the object
  = ACL (Access Control List) System (z.B. RAC-F)
  = insufficient granularity (no time, no access place etc.)

- SECOM
  Access rights are attached to the user (subject)
  = CL (Capability List) System (e.g. Top Secret)
  = much more granularity (time, place of origin etc.)

Both systems complement each other!



greenHouse

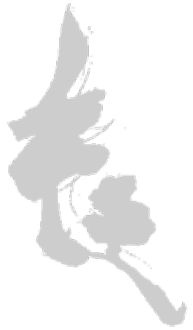
SSO-OS

History

- Developed since 1990, when I still was with Tandem Germany, based on:

  - **MPWD** (Modem Port Watch Dog)
    Challenge/Response Authentisierung & Tracing
  - **GivePW** (Give Password)
    Password generation
  - **FUNCTRAC** (Function Tracer)
    ID-Switching und Tracing

  in close cooperation with RABO Bank, Holland



SSO-OS

Standard Tandem Utilities

- Do have a predefined number of commands, which are executed with the ID of the utility user,
  z.B. FUP, SCF, SQLCI usw.
- The users interaction is NOT controlled.
- SUPER-users often do have exclusive rights.
- Roll concept not feasible.
- Inadequate audit.

SSO-OS

SECOM commands

- SECOM allows the configuration of commands:

  - command name of up to 32 bytes
  - generic commands
    (different behavior based on time and date)
  - command groups
    (z.B. EMERGENCY, APPLICATION-MGMT usw.)

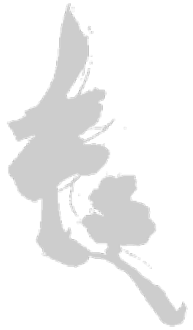
SSO-OS

SECOM command resources

- SECOM allows the configuration of commands:

  - ANY resource
    (TACL, FUP, SCF, usw.)
  - ANY ID to execute the resource
    GUARDIAN- as well as Alias-User
    (even non existing GUARDIAN-ID)

  - OBEY-File and TACL-macro support
  - Execution of grouped commands
    (z.B. system cold start, application start/restart/stop etc.)



SSO-OS

SECOM command attributes

- SECOM allows the configuration of commands:

  - command control (user input)
    (Sub-/Command level security)
  - unlimited number of users
    (GUARDIAN as well as Alias users)
  - Generic User support
    (SECOM users)
  - SECOM user groups
    (up to three levels)
  - File Sharing Groups

  Group support allows an easy implementation of the roll concept!

SSO-OS

SECOM command security

- SECOM allows the configuration of commands:

  - additional global/individual Authentisierung
    = users password
    = Challenge/Response
    = multi eye principle with remote authorization (Android APP)
  - Restriction by time and place of origin (IP address)

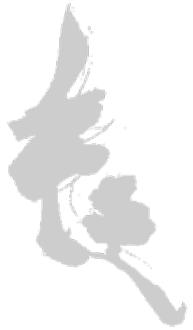
SSO-OS

SECOM command attributes

- SECOM resource attributes are:

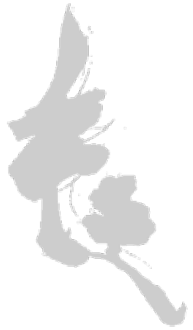
  - automatic load balancing
  - Inactivity Timeout
  - Aktions-Log
  - Optional EMS Message Generation
  - GUARDIAN- und OSS-Tracing
  - Online help and documentation

  - and much more ...



SSO-OS
Administration

- SECMAN (interactive interface)
- PATHWAY-application (the good old PATHWAY ...)
- SECWin-GUI (C++ GUI, PC basierend, optional)
- iWAMS-SECOM (Browser basierend, optional)
- Central administration of commands of all EXPAND reachable SECOM environments.
  (RABO ~ 30 Systeme, ING ~ 30 Systeme, Six ..., etc.)

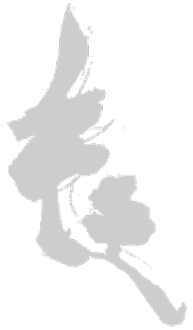


SSO-OS

SECOM Usage

- Interactive from TACL (normal case)
  e.g. SECOM SUPERTACL
- As INLINE process
- As ‘initial command interpreter (ICI)‘ from TELNET or SAFEGUARD (Swiss Police [EJPD])
- In OBEY files
- In TACL Macros
- In NetBatch

- Block Mode Interface SECOMCI (NO PATHWAY!)



SSO-OS

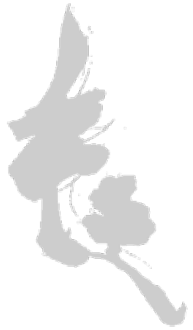
Live Demo

- VPN zu \GINKGO (NS1002, H06.26)

- SECOM PATHWAY Administration
- SECWin GUI
- iWAMS-SECOM (Browser basierendes GUI)

- Start EMSDIST

- SECOM – SUPERTACL
- SECOM – CHKFUP
- SECOMCI – SUPERTACL
- SECOMCI – CHKFUP



SSO-OS

Current status

- Still not mature – we always implement new features – mostly on ideas by customers (e.g. File Sharing Groups)
- Oriented on our customser needs – not (only) our ideas.
- Customer requested features will be implemented in a timly manner – without costs – when it is a generally interesting feature..
- Comes with a bunch of helpful tools.
  (Passwortsplitter, Im-/Export from commands etc.)

SSO-OS

Conclusion and in Short

Simple to understand

Simple to manage

Simple to use

Simply good!

SSO-OS

Questions?

Comments?
Ideas for new features?

SSO-OS

Thank you for your time and attention.

Please visit me on our booth for further questions, and a demo.