greenHouse

Security ...

What are we talking about?

Carl Weber

GreenHouse Software & Consulting

greenHouse

Brief Intro

- 1978 start as an analyst with Tandem Germany
- 1979 first cryptographic program on \DUES
- 1985 specialization in SAFEGUARD & Security
- 1989 - 1993 successful evaluations (C2, F2/F7, Q3)
- 1994 start of GreenHouse Software & Consulting
- 31+ years on the best platform available

greenHouse

Agenda

- What are we talking about?
- Security policy
- Use of mechanisms
- Audit
- Security Review
- Summary

greenHouse

Motto...:

Security people have a good heart, but a sick mind ...

Good judgment comes from experience.
Experience comes from bad judgment.

greenHouse

The five A's from 1985

1. Authentication
2. Authorization
3. Auditing
4. Administration
5. Availability

greenHouse

What are we talking about?
View I

- Confidentiality
- Integrity
- Availability

greenHouse

What are we talking about?
View II

- People
- Environment
- System

greenHouse

What are we talking about? Reality

	Confidentiality	Integrity	Availability
Human	Clearance	Trust Social engineering	Illness Vacation Motivation
Environment	Access control	Bullet proof Bunker	Power Data comm lines
System	ACL/CL systems Encryption	Hard- and software ECC TMF Encryption	Error recovery DoS RDF

greenHouse

What are we talking about?
What we normally focus on

	Confidentiality	Integrity	Availability
Human	Clearance	Trust Social engineering	Illness Vacation Motivation
Environment	Access control	Bullet proof Bunker	Power Data comm lines
System	ACL/CL systems Encryption	Hard- and software ECC TMF Encryption	Error recovery DoS RDF

greenHouse

Security I

- Confidentiality
  - Identification
  - Authentication
  - Authorization
  - Auditing
  - Administration
  - Object re-use

greenHouse

Security I

- Integrity
  - Hardware
  - Software
  - Employees

greenHouse

Security I

- Availability
  - Error Recovery
  - Guarantee of functionality
  - Denial of Service

greenHouse

Security II

- People
  - Clearance
  - Engagement
  - Trust
  - Company Policy
  - Social Engineering

greenHouse

Security II

- Environment
  - Air conditioning
  - Computer room
  - Access control
  - Modem/Switch room
  - Silo

greenHouse

Security II-a

- System
  - ON system security (e.g. ACLs)
  - OFF system security (e.g. cryptography)
  - Electro magnetic radiation (temptest)
  - Availability (online maintenance)
  - Data integrity (ECC, Parity)
  - DoS
  - Covert channel

greenHouse

Security II-b

- System
  - Robust applications (error handling)
  - Functionality (software design)

Person related aspects

- Education of ALL employees including management
  - why security!
  - description of goal
- Hiring the RIGHT people
- Proper people management

Person related aspects

- Clearance
- Trust
- Motivation
- Environment for
  - normal daily work
  - disaster case

greenHouse

Person related aspects

- Leakage of insider information
  - possible?
  - what if?
- Accessing sensitive information
  - paper/CD/DVD shredder
  - secure paper container
  - locked offices and desks
  - is your PC a Personal or Public C?

greenHouse

Person related aspects

- Roles within the company
  - Management
  - Auditing
  - Operations
  - Backups
- Possible personal restrictions
  - shift
  - standby

Person related aspects

- Possible restrictions by law
  - liability
- Escalation procedures
- Shared Secrets (4-eye principle)
- Social Engineering

greenHouse

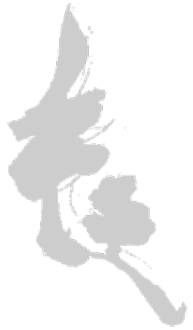
Environment

- Building requirements
  - bunker?
  - in basement, or highest floor?
  - room without windows?
- Access control (man traps?) for IN and OUT
- Separation of persons
- Air conditioning
  e.g. inlet not at ground level

greenHouse

Environment

- Entrance not below high water level
- No water pipes in compute room
- Fire alarm and extinguish systems
- Closed shop operation
- Separation of system and peripherals
  - printer and paper
  - tape silo
  - disk farms (mirrored disks)



greenHouse

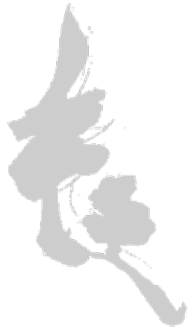
Environment

- Power
  - two separate inlets, UPS
  - emergency generator
- Communication
  - modem/switch room
  - two separate providers/inlets
  - installation of satellite dish
  - micro wave/laser

greenHouse

ON System Security

- TCP (trusted computing base)
  - what's that?
  - connections to
- Reference Monitor Concept
- National security criteria
  - TCSEC (Orange Book, Rainbow series)
  - ITSEC (harmonized criteria)



greenHouse

ON System Security

- Authentication
  - by knowledge, e.g. PIN, static password
  - by possession, e.g. chip card, token
  - by biometrics, e.g. finger print, retina, typing characteristic, voice, hand writing etc.
  - mixed systems with two of the above

greenHouse

ON System Security

- Authorization
  - ACL systems, e.g. SAFEGUARD
  - CL systems, e.g. command level control
  - access methods for read, write, re-write, write to EOF only, execute, purge, own, create etc.

greenHouse

ON System Security

- Auditing
  - conservation of evidence
  - security breach
  - hardware as well as software events

- Labeling/Classification (B level security)

greenHouse

ON System Security

- Object re-use
  - magnetic storage, such as tape and disk
  - optical storage such as CD and DVD
  - data on externa media, such as USB stick
  - main memory

greenHouse

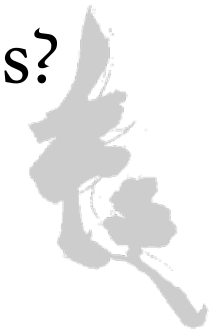
ON System Security

- Command level security
- Configuration control
- Software/Application release and control
  - Source and object control
  - Quality assurance
  - Separation of production from test and development

greenHouse

ON System Security

- What is needed to run the system?
- What is NOT needed to run the system?
- Do I have everything in place?
- Trusted Facility Manual (TFM) and
  The Secure Site Manual (TSSM)
- How to make use of security within applications?



greenHouse

ON System Security

- Worms
- Viruses
- Trojan Horses (*)
- Time Bombs (*)

(*) can be found on Tandem systems!

greenHouse

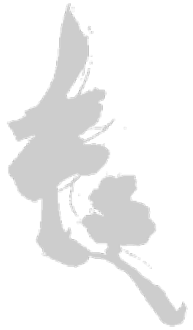
OFF System Security

- TCP/IP with
  - TELNET
  - FTP
  - Finger, Ping, Echo
- Dial-in
  - authentication

greenHouse

OFF System Security

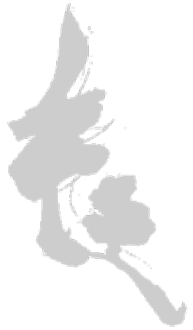
- MAC – Message Authentication Code
  - digital signature, e.g. used in EFT/POS
- SWID
  - digital signature for software distribution
- PIN – Personal Identification Number
- TAN – Transaction Number



greenHouse

OFF System Security

- Cryptography
  - symmetric algorithms (DES, IDEA)
  - asymmetric algorithm (public key, e.g. RSA)
  - shared secrets (n of m)
  - e.g. PGP, TrueCrype, PasswordSafe, etc.
- Key distribution
- Standards from ANSII, ECMA, ISO etc.



greenHouse

OFF System Security

- How to store, and how to destroy tapes?
- Printouts
  - who distributes them
  - elimination when no longer needed
- E-Mail
  - PGP
- WLAN
  - SSID suppression and link encryption
- USB Stick

greenHouse

Electro magnetic radiation

- Tempest system (computer in a fridge)
  - prevents compromising emission
- Anti EMP (secure against neutrons)
  - no damaging irradiation
- Special cables
  - fiber in a tube

Electro magnetic radiation

- Radiation free displays
- Secure placement of displays
  - screens not visible by others

greenHouse

Information radiation

- Covert channels
  - Resource usage
- Communication without a direct path
  - changing the priority
  - watching the EOF
- Guessing based on available facts

greenHouse

Availability & Integrity

- Online maintenance
- Redundancy of critical hardware
  - Securing the data high ways in the hardware by parity, CRC, ECC, CPU (voting logic), even connectors
- Redundancy of critical processes
  - Tolerating ‘Heisenbugs’

greenHouse

Availability & Integrity (physical)

- Disaster Recovery
- Risk analysis
- Application analysis and –evaluation
- Alternate power and communication lines
- Procedures and cook books with regular test runs
- Executive buy in (to justify the costs)
- System wide backups and storage
- Availability and security of personnel

greenHouse

Availability & Integrity (logical)

- Audits
- Before and After images
- Process Pairs (I love Tandem ...)
- Checksums (e.g. the good old type U files)
- Hash (e.g. MD5)
- Message Authentication Code (MAC)

greenHouse

Error Handling

- Error detection
- Error recovery
- Robust applications
- Calling DEBUG, STOP and ABEND
- Error messages and description
  (do NOT use ‘well known’ error numbers)

greenHouse

Denial of Service

- Controlling system resources
  - disk space
  - CPU usage (% load, which CPU)
  - Communication lines
- Controlling applications
  - Blocking by intentional wrong input
  - parallel usage/users
  - Deadlock

greenHouse

Software Design

- Functionality
- Robust code
- Optimal usage of system specialties
- Following (company) standards
- Easy to maintain and change
- Documented
- Security attributes

greenHouse

Possible attacks (internal)

- By Error
- Defective programs (inadequate QA)
- Defective handling (inadequate user prompting)

greenHouse

Possible attacks (internal)

- By Intention
- Defective programs (virus, time bomb)
- Wanton wrong handling
- Spying
- Sabotage and demolition
- Social engineering

greenHouse

Possible attacks (external)

- Force Majeure
  - Fire
  - Water
  - Earth quakes
- By hackers
  - Bit napping
  - Manipulation
  - Reiteration
  - Repudiation

greenHouse

Possible attacks (external)

- By slobs
  - Demolition
  - Fire
- DoS by FTP (!)
- Social Engineering

greenHouse

Security Policy

No policy – No security!

Weak policy: Please don't damage the system

Strong policy: Need to know

greenHouse

Security Policy

- A good Security Policy is a one pager

  which is the base for

- Platform specific guidelines

- Has to be backed by the board

greenHouse

Introducing Security

- Appoint a security administrator
- Appoint accountability for installing new software
- Define QA
- Install Object and Source version control

greenHouse

Introducing Security

- Make use of available tools (GUARDIAN and SAFEGUARD) and functions (PATHWAY) BEFORE new products are introduced

greenHouse

Security Audit

- Auditors have to be independent from system staff, and report directly to the board of directors
- Audits are created by applications as well!
- Check audits on a regular basis
- Have tested escalation procedures in place

greenHouse

Security Review

- Check employees (only in military?)
- Check environment
- Check implementation and usage of security tools and procedures
- Do it on a regular basis!

greenHouse

Recapitulation

- Security is top priority and the responsibility of the CEO
- No security policy – no security
- No education – no acceptance
- No individualization – no security
- First use available tools and functions
- The presence of security tools does NOT make the system more secure

greenHouse

Recapitulation

- Separate operating, and security administration
- Auditing has to be IT independent
- Accreditation of application by owner
- Checking of used mechanisms by evaluation of ALL audits
- Close (new) security holes immediately

greenHouse

Recapitulation

- Be aware of the ‘p.ss.d o.f’ in-house expert
- Understand security as method to
  - enforce and keep a clean system
  - mechanism to reduce and prevent errors

  and not as
  - barrier
  - controlling instance

greenHouse

Recapitulation

- Run an audit on a regular basis, e.g. every 2 years
- Make use of auditors, who KNOW the hardware and software they have to audit
- No GePEx (general purpose expert) please!

- Feel insecure!

greenHouse

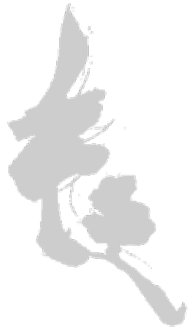
Recapitulation (Tandem GUARDIAN)

- Use all GUARDIAN features
- One user – one ID – one password
- Prevent the use of SUPER.SUPER
- Don’t make use of group managers
- Set the default security as strict as possible
- Restrict the use of remote passwords
- Secure $SYSTEM.SYS*.* as tight as possible
- Clear CIIN

greenHouse

Recapitulation (Tandem SAFEGUARD)

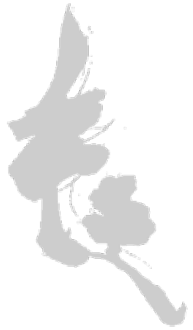
- Use all GUARDIAN features
- Introduce ALL administrative items in SAFEGUARD - e.g. OBJECTTYPE
- Before introducing/changing attributes, know what the change will do
- Make use of SAFGUARD when GUAARDIAN is insufficient
- Check ALL audit files



greenHouse

Recapitulation (Tandem subsystems)

- Keep an eye on
  - SCF
  - TACL
  - SQLCI
  - SAFECOM – they all support a RUN command
- Secure all CSTM files to “OOOO”
- Set the PATHWAY security attributes
- Use SUPER.SUPER in controlled and homeopathic dosage



greenHouse

Hope we now know what we are talking about ...

greenHouse

Questions?