Accreditation
2014-12-01

Susanne Frank
Information Security Consultant
susanne.frank@combitech.se
Agenda

- My background
- Basics of the Accreditation method
  - Standards
  - System Development Lifecycle
  - Step by step
- Why accreditation
- Difficulties
- Example – Smart phone
Customers

FÖRSVARSMAKTEN

FMV

SAAB

personal

business-oriented
Method, Swedish Armed Forces

- ISO/IEC 12207 Systems and software engineering — Software life cycle processes
- ISO/IEC 15288 Systems Engineering standard covering processes and life cycle stages
- DIT 04 Directives for the Swedish Armed Forces Information Technology
Method, Saab

ISO/IEC 12207

PROPS

ISO/IEC 15288

SAAB Accreditation Method
System Development Lifecycle

Phase out
Order
Specify
Systemize
Develop
Tests
Operation
Implementation

Security Objective
IT Security Architecture
Evaluation
Why accreditation?

- To ensure Information Security is handled in the system
- To do the right thing from the beginning - Information Security shall be a part of system development from the beginning to accomplish cost effectiveness
- It will be a better system in the end in the aspect of security, usability and technology
- Coordination of IT-systems in the organization
- Enhanced documentation of the system
- Record of approved applications and systems in the organization
- Standardized method in large organizations
- CC is used for products – Accreditation is used for systems
Priorities

Protect the critical information

Technique and organisation

Correct protection for correct information

Prepare for when something happens
Security Objective

A compilation of all security related requirements – independent of the source

- Identify and handle contrarious requirements
- Order requirements by shall and should
- Identify requirements by technical and administrative
Security Objective, Method

- Operational analysis
- Information analysis
- Threat and risk analysis
- Operational requirements
- Legal requirements
- Information requirements
- Threat requirements
The Security architecture is based on the security objective along with the design suggestion in order to describe how security shall be attained in the system.
Develop

Plan

Develop – what functions and solutions shall be implemented?

Test

Develop – how shall the functions be realized?

Test – validate desired functionality

Ensure that decided functions and solutions are implemented.

Handle modified requirements and conditions

- Plan – what functions and solutions shall be implemented?
- Develop – how shall the functions be realized?
- Test – validate desired functionality
Evaluation

Can be performed during different stages in the project. Several types, depending on requests.
Difficulties

- Project Management sees cost, not profit
- Information security is generally applied late or afterwards
- Documentation is inadequate - Security functions are rarely described thoroughly in system documentation
- “System of systems” depending on other systems or components being accredited already
- Contradictive security objectives
Example - Smart phone

Assessment/Evaluation

- Technical Evaluation/Penetration test
- Code review
- Validation and verification
Security Objective

- Operational analysis
- Information analysis
- Operational requirements
- Legal requirements
- Information requirements
- Threat and risk analysis
- Threat requirements
**Camera:**
I want to be able to take photos and store a lot of photos.

**SMS/MMS:**
I want to be able to send texts including pictures.

**WIFI:**
I want WIFI.

**E-mail:**
I want to be able to send both private and company e-mails.

**Contacts:**
I want both customers, family and friends in my contacts.

**Internet:**
I want to be able to connect to Internet.

**GPS:**
I want Facebook and google maps to know my position.

**APP:**
I want Facebook, Instagram, LinkedIn.

**Calendar:**
I want both my private calendar and work calendar.
The calendar shall synchronize automatically.
Security Objective

Operational analysis

Information analysis

Operational requirements

Legal requirements

Information requirements

Threat and risk analysis

Threat requirements
Photos:
Whiteboard from job meeting
Embarrassing photo from Saturday night party...

SMS/MMS:
Here is your password...
I’ll be away on a trip all of next week...

E-mail:
Log in information...
Tickets...

Calendar:
Away...

Contacts:
Customers
Family, friends

GPS
History
Location

Phone log:
Customers

Social media:
Family, friends
Pictures, status updates...

Internet:
Web history
Favorites

WIFI:
Net and password
Security Objective

- Operational analysis
- Information analysis
- Operational requirements
- Legal requirements
- Information requirements
- Threat and risk analysis
- Threat requirements
SMS/MMS:
Text in your name to customers/friends

E-mail
Send e-mails in your name

App
Control your online characters
Train-tickets
Spend money on online games
Settings on Spotify/Netflix/Skype

Phone
Call in your name

Social media:
Facebook posts/Instagram in your/the company’s name
Twitter in your/the company’s name
What differs a smart phone from a laptop?

- You often use it both for work and in your spare time
  - Different focus on protection
- Easier to carry
  - Easier to lose, easier to steal
  - More opportunities to surf on unprotected WiFi networks
  - Often left where people can use it unnoticed
- Many more and easy to get applications
- Children and friends use it for games, films and music
Suggested requirements

- Use password (not just the SIM-code)
- Encrypt the content, if possible
- Control app permissions
- Always use HTTPS
- Avoid unencrypted/unsecure networks
- Install updates
Suggested requirements

- No root or jailbreak
- Contact information outside of the locked content
- Backup
- No unknown chargers/cables
- Turn off interfaces that is not needed
- Be aware that photos may contain time and position
- Reset old mobile phones, in combination with encryption
Security functions

- Access control
  *(user name, password, certificates, etc.)*
- Logging of security related events
  *(change in time, decryption, log in, etc.)*
- Protection of stored information
  *(checksums, encryption, key handling, revocation, etc.)*
- Redundancy
- Intrusion detection/prevention
  *(firewalls, IDS/IPS, etc.)*
- Protection of information in transmission
  *(HTTPS, VPN, TLS, i.e. encryption)*
- Protection against malware
  *(virus, worms, trojans, etc.)*
Evaluation

Assessment/Evaluation

- Validation and verification
- Technical evaluation/Penetration tests
- Code review
- Accreditation