Day 2 – Oct 11th

- Introduction
- Concepts
- Risks and Threats
- Methods and standards
  - ISO2700x, OCTAVE, Ebios, Mehari,
- Tools
  - Nessus, nmap, ethereal, ntop, ...
- Hand-on Labs
Outline

• Introduction
• Concepts
• Risks and Threats
• Methods and standards
  • ISO2700x, OCTAVE, Ebios, Mehari,
• Tools
  • Nessus, nmap, ethereal, ntop, ...
• Hand-on Labs
Cartography of InfoSec

- Set of documentation, questionnaires and knowledge bases.
- Allow to measure existing practices and to compare to a reference guide of « good practices ».
- Identify important processes within organization and propose metrics in order to calculate impacts of potential losses (Risk Analysis).
Purpose of InfoSec Standards

- Protection of informational assets
- Sign (if not Proof) of Trust
- Potential Differentiator (from Competition)
- Profitability
- Respect of Legislation and Rules
- Public Image
Legislation

- Sarbanes-Oxley (USA)
- HIPAA – Heath Information Protection Assurance Act (USA)
- FOIA – Freedom Of Information Act (USA)
- Access to Information and Privacy Acts (Canada)
- Bale2 (EU)
- LCEN (FR)
Standards : Guide of Good Practices

● Define a set of **good practices** for Information Security, used as reference and able to insure third party with an acceptable and recognized level of security.

● Specify **requirements** for
  – Implementation
  – Operation
  – Improvement of documented ISMS (Information Security Management System)

● Specify **requirements** to implement security measures that are:
  – Adapted to the needs of the enterprise or organisation
  – Appropriate
  – Well Suited / Commensurate
Sprechen sich esperanto?

"Too many standards and methodologies IS confusing"
<table>
<thead>
<tr>
<th>Identification</th>
<th>Désignation</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>EBIOS</td>
<td>Méthode</td>
<td>DCSSI</td>
</tr>
<tr>
<td>MEHARI</td>
<td>Méthode</td>
<td>CLUSIF</td>
</tr>
<tr>
<td>OCTAVE</td>
<td>Méthode</td>
<td>CERT</td>
</tr>
<tr>
<td>PSSI</td>
<td>Guide méthodologique</td>
<td>DCSSI</td>
</tr>
<tr>
<td>TDBSSI</td>
<td>Guide méthodologique</td>
<td>DCSSI</td>
</tr>
<tr>
<td>PC2</td>
<td>Guide méthodologique</td>
<td>DCSSI</td>
</tr>
<tr>
<td>DSIS</td>
<td>Guide méthodologique</td>
<td>DCSSI</td>
</tr>
<tr>
<td>Memento DeP</td>
<td>Guide méthodologique</td>
<td>DCSSI</td>
</tr>
<tr>
<td>sp800-60</td>
<td>Guide méthodologique</td>
<td>NIST</td>
</tr>
<tr>
<td>PSC-SI</td>
<td>Guide de bonnes pratiques</td>
<td>GMSIH</td>
</tr>
<tr>
<td>PAU</td>
<td>Guide de bonnes pratiques</td>
<td>GMSIH</td>
</tr>
<tr>
<td>ITIL</td>
<td>Guides de bonne pratiques</td>
<td>ITSMF – BSI</td>
</tr>
<tr>
<td>Guide SMSI</td>
<td>Guide de bonnes pratiques</td>
<td>CNRS</td>
</tr>
<tr>
<td>CobIT</td>
<td>Guide de bonnes pratiques</td>
<td>ISACA - ITGI</td>
</tr>
<tr>
<td>ISF</td>
<td>Guide de bonnes pratiques</td>
<td>ISF</td>
</tr>
<tr>
<td>ITSEC</td>
<td>Norme d’exigences</td>
<td>DCSSI</td>
</tr>
<tr>
<td>ISO 15408</td>
<td>Norme d’exigences</td>
<td>DCSSI</td>
</tr>
<tr>
<td>EESSI</td>
<td>Normes d’exigences</td>
<td>MINEFI</td>
</tr>
<tr>
<td>NF Z 42-013</td>
<td>Normes d’exigences</td>
<td>AFNOR</td>
</tr>
<tr>
<td>21 CFR Part 11</td>
<td>Norme d’exigences</td>
<td>FDA</td>
</tr>
<tr>
<td>ISO 13335</td>
<td>Norme de bonnes pratiques</td>
<td>ISO</td>
</tr>
<tr>
<td>ISO 13569</td>
<td>Norme de bonnes pratiques</td>
<td>ISO</td>
</tr>
<tr>
<td>ISO 17799</td>
<td>Norme de bonnes pratiques</td>
<td>ISO</td>
</tr>
<tr>
<td>PRIS</td>
<td>Politique de référencement</td>
<td>DCSSI</td>
</tr>
<tr>
<td>sp800-45</td>
<td>Guide technique</td>
<td>NIST</td>
</tr>
<tr>
<td>PPnc004</td>
<td>Guide technique</td>
<td>DCSSI</td>
</tr>
</tbody>
</table>

- **DCSSI** :
  - [http://www.ssi.gouv.fr/fr/dcssi](http://www.ssi.gouv.fr/fr/dcssi)

- **CERT** :
  - [www.cert.org](http://www.cert.org)

- **NIST** :
  - [csrg.nist.gov](https://www.csrc.nist.gov)

- **CNRS** :
  - [www.sg.cnrs.fr/fsd](http://www.sg.cnrs.fr/fsd)

- **ISACA** :
  - [www.isaca.org](http://www.isaca.org)

- **ITIL** :
  - [www.itil.co.uk](http://www.itil.co.uk)

- **CLUSIF** :
  - [www.clusif.asso.fr](http://www.clusif.asso.fr)
ISO 27000 Standards

Covers:

- Risk Assessment
- Security policy - management direction
- Organization / Governance of InfoSec
- Asset management
- Human resources security
- Physical and environmental security
ISO 27000 Standards (cont.)

- Communications and operations management - management of technical security controls in systems and networks
- Access control
- Information systems acquisition, development and maintenance - building security into applications
- InfoSec incident management
ISO 27000 Standards (cont.)

- Business continuity management
- Compliance/conformance with policies, standards, laws and regulations
ISO 27000 Series

• ISO 27000
  – Glossary

• ISO 27001 (2005)
  – ISMS – Information Security Management System
  – certification standard against which organizations' ISMS may be certified
  – good practices in IT Security.
  – 2^{nd} part of BS7799.
ISO 270000 Series (2)

• ISO 27002 (ex-17799)
  – Code of practice
  – Security Measures
  – 1st part of BS7799.

• ISO 27003
  – Implementation Guide

• ISO 27004 (2007 ou 2008)
  – Measurement and metrics
ISO 270000 Series (3)

• ISO 27005 (2007)
  – Risk management / Risk analysis
  – 3rd part of BS7799

• ISO 27006 (2007)
  – Guideline for Auditing and Certification of ISMS

• ISO 27007
  – Continuity and Contingency Plan
Methods and ad-hoc standards

- Complexity of methods for risk analysis
- Hence ad-hoc methods and standards for specific environment
- As an example, Comité Français d'Organisation et de Normalisation Bancaire defined a profile of minimum set of protection to cover precise needs of banking sector.
Methods

• MEHARI
  – Méthode d'analyse de Risques based on ISO 2700x series. www.clusif.asso.fr
  – Derived from MARION and MELISSA

• EBIOS/PSSI
  – Methods and plans provided by the french government
    www.ssi.gouv.fr/fr/confiance/methodes.html
MEHARI

- MEthode Harmonisée d'Analyse de RIsques (MEHARI) - Commission Méthodes du CLUSIF (Club de la Sécurité des Systèmes d'Information Français)

- 6 factors for risks:
  - 3 for potentiality and 3 for impact;

- 6 types of security measures:
  - structural, dissuasive, prevent/protection, palliative and recovery.
MEHARI – Domains (1)

- Organization of ISMS
- Security Awareness and Education
- Physical Security of Sites
- Access Control to Sensitive Areas
- Protection against usual risks (fire, flooding, etc.)
- Network Architecture (Access Control, Filtering, containment, reliability)
- Confidentiality and integrity of communication
MEHARI – Domains (2)

- Access Control to Logical level (systems, apps and data)
- Data Security
- Operational Procedures
- Management of Information Support
- Rescue Plan
- Backup and Recovery Planning
- Maintenance
- Security of projects and development
- Incident Management
MEHARI

- Stakes & asset analysis - Classification
- Security services audit
- Identification of critical risks
- Risk situation analysis

Action plans based on the vulnerability audit
Action plans based on risk analysis
Project-based risk management
Action plans based on stakes analysis
Identification of a risk situation

Evaluation of natural exposure

Evaluation of dissuasive and preventive factors

Evaluation of Potentiality

Evaluation of intrinsic impact

Evaluation of protective, palliative and recuperative factors

Evaluation of impact reduction

Evaluation of impact

Global risk evaluation

Potential assistance: Malfunction value scale or prior classification

Decision on whether risk is acceptable

Figure 5: Risk situation analysis
OCTAVE

- From CERT
  http://www.CERT.org/octave/osig.html

- Operationally Critical Threat, Asset, and Vulnerability EvaluationSM (OCTAVE®)

- self-directed approach

- Required broad knowledge of business and security processes
FIPS 140-1

- Security Requirements for Security Modules
- Standard from US Department of Industry
- Mainly used to evaluate security equipment from anglo-saxon countries
- Barely used for software
FIPS 140-1 (Levels)

- **Level 1**: Minimum Level with basic security requirements
- **Level 2**: Includes constraints to resist to attack by using integrity checking and authentication for operators
- **Level 3**: Includes physicals requirements (detection of physical intrusion).
- **Level 4**: Adds stricter stronger requirements (armoured shelter, detection variation of pressure, d…).
ITSEC

- Relatively Old Standard (1991)
- Derived from the Orange Book (DOD)
- Define level of trust as well as methods to evaluate
- Interpretated differently from one country to another
- Most of the products have been evaluated in UK
- European Standard
Common Criteria

- Following ITSEC.
- Attempt to correct ITSEC weaknesses (discrepancy in evaluations)
- LARGE amount of documentation
- International recognition (not EU only)
- define classes of insurance (development, tests, vulnerabilities...).
- Global level is obtained by minimal level in each class.
Common Criteria (levels)

- EAL 1: functionally tested
- EAL 2: structurally tested
- EAL 3: methodically tested and evaluated
- EAL 4: methodically designed, tested and evaluated
- EAL 5: designed with semi-formal methods and tested
- EAL 6: design validated with semi-formal methods and tested
- EAL 7: design verified with semi-formal methods and tested
Maintenance of evaluation

■ Evolution of products
  – Technical evolution,
  – Functional evolution,
  – corrections.

■ Need to update evaluation periodically.
What is a Security Audit?
For what Purpose?
Information Security Audit

• Audit:
  • Risk Assessment
  • Assessment and evaluation of conformance with security policy and set of security rules.

• Reference: Set of rules defining organization, procedure and/or technics to ensure information security.
Why assessing Information Security?

- Evaluate and validate security practices (control, quality processes);
- Validate procedures to alert, react and handle incident or disaster;
- Detect “forgotten/ignored” stakes or weaknesses;
- Educate users, management, employees to Information Security and Risk Management.
Phases of the Audit

- Preparation
- Documentation Review
- Interviews, talks, visits
- Technical Investigation, Data Collection
- Data Analysis
- Synthesis and report writing
- Report Presentation
- Planning corrective actions
InfoSec Audit (1)

- "White Box"
  - audit in situ;
  - Access to buildings, organization, data, processes, documentation and procedures;
  - Access to people with interviews of managers and people in charge of operation.
InfoSec Audit (2)

• "Black Box"
  – Partial knowledge and/or access to the Information System (organization, documents procedures, sites, people);
  – Reveal/spot weaknesses:

• Ex: penetration testing.
Who can perform an audit?

- AUTHORIZED personal
  - Sysadmin, consultant, contractor
- Technical and Business Knowledge
- Excellent Communication Skills
- Certified (ex: ISO Lead Auditor)

Trained and Educated people
Limitations

- Based on interviews with declarations and claims that can be twisted (intentionally or not);
- Context and time dependent;
- Snapshot / view.
How to perform an Audit?
Where to start?

- Define the contract: daily job, mission, contract, order, ...
- Define the type of audit (host-based, network-based, 'white-box', 'black-box', penetration testing, ...)
- Define perimeter and schedule
- List people to be involved
How to perform an Audit?

- Define the type of Audit, Target, Perimeter
- Prepare the Tools
- Review Policies and Documentation
- Data Collection
- Analyse and Synthesis
- Writing the Report
- Presentation
- Planning Corrective Actions
Collect information

• Collect information on the target:
  • Documentation: policies, “chartes”, etc ...
  • Interview
  • Research: Google, Whois, DNS, department of commerce ...

*Goal: Identify systems, processes, applications, people, organizations as well as documents*
Cartography

- Detection of systems and services, cartography:
  - Locating and visiting sites and buildings (if possible)
  - Documentation
  - Asset Management Tools or Network Management
    - Ex: HP OpenView, Lan Manager, N-View
  - Network Topology: IP routing, SMTP...
  - Detection of ports/services
  - Identification of systems
Looking for Vulnerabilities

• Scan and exploitation of vulnerabilities:
  • Physical (garbage dumping, wires, access to resources)
  • Network (filtering policies, equipments)
  • Systems (patches, active services)
  • Applications
    • Web Server,
    • Database,
    • Mail Server,
    • Directory,
    • ...

• Take and Secure Position
• Progress
• Move Deeper and Deeper
Outline

• Introduction
• Concepts
• Risks and Threats
• Methods and standards
  • ISO2700x, OCTAVE, Ebios, Mehari,
• Tools
  • Nessus, nmap, ethereal, ntop, ...
• Hand-on Labs
The Toolbox
Prepare the Tools

- Safe, Trusted and Autonomous Platform for execution and storage of resulting data.
  - Dedicated laptop
  - USB or CD-based bootable (such as Knoppix/BackTrak)
- Retrieve, install and configure necessary tools.
- Eventually development.
- Get used and trained.
- Verify ALL tools used are untampered with.
Discovery Tools (1)

- Information: WhoIS, Dig, ...
- Topology
  - IP: Traceroute, Itrace, Tctrace, ...
  - SNMP: SNMPWalk
  - SMB: LinNeighborood, NBTscan
- Network or System Administration
  - HP-Openview, N-View
- Services:
  - Nmap
Discovery Tools (2)

- Wi-Fi
  - Kismet
- Bluetooth
  - BTScanner
- Google
Network Flow Analysis

- Wireshark / Ethereal
- Etherape
- Ntop
Testing Configuration

- HIDS – Host Based Intrusion Detection
  - MSAT – Microsoft Security Assessment Tool
  - Sara (Unix)
  - JASS (Solaris)
  - Bastille
  - Checkperms
  - Utilities from sysinternals.com
Vulnerabilities Scanners

- Nessus
- Auditor
- BlueSnarf
- Code Injection
- Sending Virus Samples
- XSS (Cross Site Scripting)
Restitution
Report

- Analysis and synthesis in report
- Achievement of audit
- Readable and adapted to audience
  - From executive summary to detailed annexes
- Adapted to the business objectives
- Definition of an action plan
Audience

- Executive
- Stockholders
- Managers
- Operational staff
- Technical staff (techno-geek)
Content

- Title, Introduction, legal
- Executive Summary
- Prioritized recommendations (with cost)
- Report (following the structure of MEHARI domains)
- Conclusion and detailed recommendations
- Annexes
So What?

- Definition of action plan for correction
  - Action
  - Who is the owner?
  - Who is involved/concerned?
  - When is it due?
  - How much?
- Require everyone's involvement
References – More readings

- 'TCP/IP Illustrated', Richard Stevens
- 'Network Security Assessment', McNab
- 'The TAO of Network Security Monitoring', Bejtlich
- 'IT Auditing', Davis/Schiller/Wheeler
Tutoring