Digital Forensic Investigations
COS783
Digital Forensic Standardisation efforts

Prof HS Venter
hventer@cs.up.ac.za
Copyright © HS Venter (2015)

Content

• Standardisation bodies – ISO, NIST, other
• Standardisation process
• Standards (other than ISO 27043)
The ISO process

- Proposal
- Study period (SP) for 6 or 12 months
- Working Draft (WD) 1 to n
- Committee Draft (CD) 1 to n
- Draft International Standard (DIS)
- Final Draft International Standard (FDIS)
- International Standard (IS), i.e. published
- Each of the above = at least 6 months, handled at international meetings
The ISO process

• In each 6-month period between meetings
  – Draft standard goes out for comment
    • WD: Expert level
    • CD: Committee level
    • DIS: SC27 level
    • FDIS: World level (publicly available)
  – Comments collected by NB
  – DoC: Comments discussed at meeting: accepted, not accepted, accepted with modification
  – DoC worked into doc by editor(s)
  – Another round starts from the top

The ISO structure

• ISO root
  – Sub committee level
    • Working group level
• SC27 – Information security – security techniques
  – WG1 to WG5
The ISO structure

ISO/IEC JTC 1/SC 27: Information technology - Security techniques
Chair: 
Vice-Chair: 
Working Group 1: Information Security Management Systems
Convener: 
Working Group 2: Cryptography and security mechanisms
Convener: 
Working Group 3: Security evaluation criteria
Convener: 
Working Group 4: Security controls and services
Convener: 
Working Group 5: Identity management & privacy technologies
Convener: 
Working Group 6: To be formed...
Convener:

Evolving Structure

Assessment

WG 3
“Security Evaluation Criteria”

WG 1
“Information Security Management Systems”

WG 4
“Security Controls & Services”

WG 2
“Cryptography & Security Mechanisms”

Guidelines

Techniques

Product
System
Environment
Process

WG 5
“Ideity management & privacy technologies”
ISO/IEC 27000 Family of Standards

- 27000
- 27001
- 27002
- 27003
- 27004
- 27005
- 27006
- 27007...
- 27050

Applicability to other standards
WG4 related standards

• ISO/IEC 27035: Information security incident management
• ISO/IEC 27035 Part 1: Principles of incident management (DIS)
• ISO/IEC 27035 Part 2: Guidelines to plan and prepare for incident response (DIS)
• ISO/IEC 27035 Part 3: Guidelines for incident response operations (TS)

• ISO/IEC 27037: Guidelines for identification, collection, acquisition, and preservation of digital evidence (IS-2012)
• ISO/IEC 27038: Specification for digital redaction (IS 2014)
• ISO/IEC 27040: Storage security (IS 2015)
• ISO/IEC 27041: Guidance on assuring the suitability and adequacy of incident investigation methods (FDIS)
WG4 related standards

- ISO/IEC 27042: Guidelines for the analysis and interpretation of digital evidence (FDIS)
- ISO/IEC 27043: Incident investigation principles and processes (IS 2015)
- ISO/IEC 27044: Guidelines for Security Information and Event Management (SIEM) (SP)
- ISO/IEC 27050: Electronic discovery (WD3)
- ISO/IEC 30121: Governance of digital forensic risk framework (IS 2014)

ISO/IEC 27037

- Guidelines for identification, collection, acquisition, and preservation of digital evidence
- Published in 2012
ISO/IEC 27037 Content

5 Overview
5.1 Context for collecting digital evidence
5.2 Principles of digital evidence
5.3 Requirements for digital evidence handling
  5.3.1 General
  5.3.2 Auditability
  5.3.3 Repeatability
  5.3.4 Reproducibility
  5.3.5 Justifiability
5.4 Digital evidence handling processes
  5.4.1 Overview
  5.4.2 Identification
  5.4.3 Collection
  5.4.4 Acquisition
  5.4.5 Preservation

6 Key components of identification, collection, acquisition and preservation of digital evidence
  6.1 Chain of custody
  6.2 Precautions at the site of incident
  6.3 Roles and responsibilities
  6.4 Competency
  6.5 Use reasonable care
  6.6 Documentation
  6.7 Briefing
  6.8 Prioritizing collection and acquisition
  6.9 Preservation of potential digital evidence
ISO/IEC 27037 Content

7 Instances of identification, collection, acquisition and preservation

7.1 Computers, peripheral devices and digital storage media
   7.1.1 Identification
   7.1.2 Collection
   7.1.3 Acquisition
   7.1.4 Preservation

7.2 Networked devices
   7.2.1 Identification
   7.2.2 Collection, acquisition and preservation

7.3 CCTV collection, acquisition and preservation

Conclusion

• ISO/IEC 27043 is an ‘umbrella standard’
• 27043 covers width
• 27037, 27035, 27040, 27041, 27042, 27050 (and the others) cover depth
• ISO/IEC 17025: General requirements for the competence of testing and calibration laboratories, might eventually become outdated
• Additional standardisation possibilities