ISO/IEC JTC 1/SC 27
IT Security Techniques

Walter Fumy, SC 27 Chair
Krystyna Passia, SC 27 Secretariat

2012 JTC 1 Plenary, Jeju
Agenda

Executive summary
Recent publications
New projects
Structure & resources
Needs
Outreach
Outlook
Lessons learned
What is new

between October 2011 and September 2012

22 International Standards and Technical Reports published (total number of pages: 964, CHF 3.166)

17 new projects approved
(total number of projects: 170)

3 additional P-members (total 49)
(total number of O-members: 17)

24 internal liaisons
29 external liaisons
Programme of Work

Security and privacy

Information security and privacy governance

Information security management system (ISMS) requirements

Management system methods and processes

Security and privacy controls and services (including application and sector specific – Cloud, Privacy, Telecoms, Energy, Identity management), codes of practice, frameworks

Cryptographic and security mechanisms and technologies

Certification and auditing requirements and methods

Security, Evaluation, Testing, Processes, Methods and Specification

Economics of information security and privacy
Publications (I)

Cryptographic mechanisms & technologies

- **ISO/IEC 9797-3**: Message Authentication Codes (MACs)  
  - *Part 3*: Mechanisms using a universal hash-function
- **ISO/IEC 11770-5**: Key management  
  - *Part 5*: Group key management
- **ISO/IEC 18031**: Random bit generation
- **ISO/IEC 18033-4**: Encryption algorithms  
  - *Part 4*: Stream ciphers
- **ISO/IEC 29150**: Signcryption
- **ISO/IEC 29192**: Lightweight cryptography  
  - *Part 1*: General  
  - *Part 2*: Block ciphers  
  - *Part 3*: Stream ciphers
Information security management system (ISMS) requirements

ISO/IEC 27006: Requirements for bodies providing audit and certification of information security management systems (2nd edition)
ISO/IEC 27007: Guidelines for information security management systems guidelines auditing
ISO/IEC TR 27008: Guidelines for auditors on information security controls.
ISO/IEC 27010: Information security management for inter-sector and inter-organizational communications
ISO/IEC 24760-1: A framework for identity management
– Part 1: Terminology and concepts
ISO/IEC 27032: Guidelines for cybersecurity
ISO/IEC 27033-2: Network security – Part 2: Guidelines for the design
and implementation of network security
ISO/IEC 27034-1: Application security
– Part 1: Overview and concepts
ISO/IEC 27037: Guidelines for identification, collection, acquisition and
preservation of digital evidence
ISO/IEC 29100: Privacy framework
ISO/IEC TR 29149: Best practices for the provision and use of time-
stamping services
Publications (IV)

Security Evaluation Methods

ISO/IEC 19790: Security requirements for cryptographic modules (2nd ed)
ISO/IEC TR 20004: Refining software vulnerability analysis under ISO/IEC 15408 and ISO/IEC 18045
ISO/IEC 29128: Verification of cryptographic protocols
Approved New Projects (I)

ISO/IEC 18367: Cryptographic algorithms and security mechanisms conformance testing
ISO/IEC 18370: Blind digital signatures
  – Part 1: General
  – Part 2: Discrete logarithm based mechanisms
ISO/IEC 27018: Code of practice for data protection controls for public cloud computing services
Revision of ISO/IEC 27035: Information security incident management
  – Part 1: Principles of incident management
  – Part 2: Guidelines for incident response readiness
  – Part 3: Guidelines for incident response operations
Approved New Projects (II)

ISO/IEC 27036-5: Information security for supplier relationships – Part 5: Guidelines for security of Cloud services
ISO/IEC 27041: Guidance on assuring suitability and adequacy of investigation methods
ISO/IEC 27042: Guidelines for the analysis and interpretation of digital evidence
ISO/IEC 27043: Investigation principles and processes
ISO/IEC 27044: Security information and event management (SIEM)
ISO/IEC 29003: Identity proofing
ISO/IEC 29134: Privacy impact assessment – Methodology
ITU-T X.bhsm | ISO/IEC 17922: Telebiometric authentication framework using biometric hardware security module
## Resources – SC 27 Delegates 2011 & 2012

<table>
<thead>
<tr>
<th></th>
<th>Singapore</th>
<th>Nairobi</th>
<th>Stockholm</th>
<th>Rome</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plenary</td>
<td>65</td>
<td>-</td>
<td>61</td>
<td>-</td>
</tr>
<tr>
<td>WG 1</td>
<td>87</td>
<td>71*</td>
<td>120</td>
<td></td>
</tr>
<tr>
<td>WG 2</td>
<td>50</td>
<td>39</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>WG 3</td>
<td>39</td>
<td>34*</td>
<td>40</td>
<td></td>
</tr>
<tr>
<td>WG 4</td>
<td>27</td>
<td>25</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td>WG 5</td>
<td>55</td>
<td>40*</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td>WGs total</td>
<td>258</td>
<td>209</td>
<td>320</td>
<td></td>
</tr>
</tbody>
</table>

* including virtual delegates

not yet available

2012 JTC 1 Plenary - Jeju
Needs (I)

Ad hoc on “Modus Operandi”

Motivation & Goals

- further improve the efficiency of SC 27 and its WGs
- define the right balance between WG autonomy and coordination at SC 27 level
- make optimal use of the relevant ISO processes and tools available
- increase the overall quality of deliverables
Needs (II)

PAS Process

In view of recent experiences, SC 27 requests to further refine and improve the PAS maintenance process.

In particular, SC 27 requests JTC 1 to remove assignment of projects from the SC 27 Programme of Work, for which the maintenance remains with the PAS submitter.
Outreach

Press releases and articles, e.g. for ISO Focus, IEC e-tech magazine, ISO Journal, and ISO Management Systems

SC 27 mgt and experts frequently present the work of SC 27 at conferences and workshops around the world, e.g.

Digital Security Summit, Riyadh 2012
ETSI Security Workshop 2013

http://www.jtc1sc27.din.de/en
2012/2013

Again 10+ deliverables expected

Next SC 27 meetings

April 22-30, 2013 (WG and Plenary) France

Oct 2013 (WG) Korea
The times they are a-changing

Migration of human activities from a physical, person-to-person contact into an electronic world

This transformation offers the potential of
increasing efficiency and accuracy
improving the user experience

Key concern: negative effects on security & privacy
security aspects regularly named as major issue

Key solution element
increase level of trust associated with identities in cyberspace
## ISO/IEC 15408 „Common Criteria“

Certified Products by Assurance Level and Certification Date

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>EAL1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>22</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>5</td>
<td>34</td>
<td></td>
</tr>
<tr>
<td>EAL1+</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>17</td>
<td>2</td>
<td>2</td>
<td>6</td>
<td>2</td>
<td>0</td>
<td>30</td>
</tr>
<tr>
<td>EAL2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>4</td>
<td>13</td>
<td>53</td>
<td>29</td>
<td>16</td>
<td>6</td>
<td>12</td>
<td>1</td>
<td>136</td>
</tr>
<tr>
<td>EAL2+</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>40</td>
<td>21</td>
<td>28</td>
<td>21</td>
<td>38</td>
<td>25</td>
<td>177</td>
</tr>
<tr>
<td>EAL3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>5</td>
<td>7</td>
<td>53</td>
<td>21</td>
<td>35</td>
<td>35</td>
<td>32</td>
<td>17</td>
<td>211</td>
</tr>
<tr>
<td>EAL3+</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>4</td>
<td>48</td>
<td>17</td>
<td>25</td>
<td>22</td>
<td>36</td>
<td>25</td>
<td>180</td>
</tr>
<tr>
<td>EAL4</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>59</td>
<td>6</td>
<td>11</td>
<td>6</td>
<td>6</td>
<td>1</td>
<td>96</td>
</tr>
<tr>
<td>EAL4+</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>6</td>
<td>3</td>
<td>165</td>
<td>75</td>
<td>90</td>
<td>67</td>
<td>77</td>
<td>52</td>
<td>543</td>
</tr>
<tr>
<td>EAL5</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>3</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>11</td>
</tr>
<tr>
<td>EAL5+</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>51</td>
<td>28</td>
<td>31</td>
<td>38</td>
<td>27</td>
<td>8</td>
<td>183</td>
</tr>
<tr>
<td>EAL6</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>EAL6+</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>EAL7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>EAL7+</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td><strong>Totals</strong></td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>3</td>
<td>10</td>
<td>18</td>
<td>30</td>
<td>514</td>
<td>206</td>
<td>244</td>
<td>205</td>
<td>233</td>
<td>137</td>
<td>1613</td>
</tr>
</tbody>
</table>

Source: http://www.commoncriteriaportal.org/products/stats/
Lessons Learned

“On the Internet, nobody knows you’re a dog.”
“eBusiness (eGovernment, ... ) will not evolve without appropriate security solutions.”
“Secure systems are 10% about security technology and 90% about organization.”
“Trust is good – control is better.”
“Standards connect the world.”
Any Questions?

contact:
Walter.Fumy@bdr.de
Krystyna.Passia@din.de