Modern trends in the regulatory framework of the information security compliance assessment in Russia based on Common Criteria

Alexander Barabanov, Alexey Markov
Agenda

- Brief overview
- Current status of the Russian IT Security Certification Scheme
- Steps Toward Common Criteria Approach
- Final Remarks
Brief Overview: Historical Perspective

Establishment of Russian IT Security Certification Scheme

1995

Mandatory requirements for firewall and access control systems

1997

Mandatory requirements for source code analysis

1999

Guidance based on CC v.2.1

2003

Mandatory requirements for antiviruses (based on CC)

2012

Mandatory requirements for IPS/IDS (based on CC)

2013

Mandatory requirements for trusted boot loader (based on CC)

2014

Mandatory requirements for removable storage protection (based on CC)
Brief Overview: Historical Perspective

Orange Book Approach

Common Criteria Approach

1995

2012
Brief Overview:
Who Takes Part in the Certification Process?

[Diagram showing the process involving Sponsor (Vendor, Developer), FSTEC of Russia, Accredited Certification Body, and Accredited Evaluation Laboratory.]
Brief Overview: Typical Timeline

Typical Certification Time is 6 Months. 210 Days is Length of Pregnancy of Brown Bear.
Brief Overview: Typical Timeline

Obtaining FSTEC ID
- Normally 1 month

Evaluation provided by Laboratory
- 3-4 months

Certification by Certification Body
- 1 month and more – there may be delays:
  - for solutions that will be used for protection of classified information;
  - if a state-owned Certification authority was chosen by FSTEC

Obtaining a certificate from FSTEC of Russia
- Normally 1 month
Brief Overview: Accredited Evaluation Laboratories
Brief Overview: Accredited Certification Bodies
Brief Overview: Classical Major Approaches to Evaluation

Functional testing (black box) VS Structured testing (glass box) - Source code review
Brief Overview: Classical Major Approaches to Evaluation

Evaluation of the security functionality

- Black box testing to ensure that TOE works as it should

Evaluation for the absence of non-declared functions

- Testing of source code for the absence of software vulnerabilities
Current Status of the Russian Scheme: Products

![Bar chart showing the evaluation of products from 2003 to 2014. The evaluation peaks in 2011.]
Current Status of the Russian Scheme: Certified Products by Types (1)

- Firewall: 35%
- Embedded Access Control: 17%
- Access Control Systems: 15%
- Software: 13%
- Operating System: 5%
- Network System: 5%
- Vulnerability Assessment: 3%
- Antivirus System: 3%
- DBMS IPS/IDS: 2%

2011-2014 Evaluation Timeline
Current Status of the Russian Scheme: Certified Products by Types (2)
Current Status of the Russian Scheme: Russian vs. Non-Russian Developers

Targets of Evaluation
Current Status of the Russian Scheme: Russian vs. Non-Russian Developers
Current status of the Russian Scheme: Non-Russian Developers (1)
Current Status of the Russian Scheme: Non-Russian Developers (2)

Cisco 58%

Other 14%

Microsoft 7%

Juniper 6%

Oracle 5%

Symantec 3%

IBM 3%

Check Point 2%

McAfee 1%

Siemens 1%

2011-2014 Evaluation Timeline
Current status of the Russian Scheme:
Russian Developers

Kaspersky Lab 6%
Datatel 4%
Security Code 4%
Altex-Soft 3%
Other (approx. 100) 83%

2011-2014 Evaluation Timeline
Current status of the Russian Scheme:

Russian Developers

20

Personal Protection from Kaspersky Lab
Steps Toward Common Criteria Approach: Step #1 (1)

- CC, v. 2.1
- CC, v. 2.3
- CC, v. 3.1
- CEM, v. 3.1

ISO/IEC 15408:1999
ISO/IEC 15408:2005
ISO/IEC 18045:2008

GOST R ISO/IEC 15408-2002
GOST R ISO/IEC 15408-2008
GOST R ISO/IEC 15408-2012/2013

Publications by FSTEC of Russia
Steps Toward Common Criteria Approach: Step #1 (2)
Steps Toward Common Criteria Approach: Step #1 (3)

- EAL1: 35%
- EAL2: 30%
- EAL3: 22%
- EAL4: 13%

2004-2014 Evaluation Timeline
Steps Toward Common Criteria Approach: Step #2 (1)
Steps Toward Common Criteria Approach: Step #2 (2)
Steps Toward Common Criteria Approach: Certified Products, Russian

<table>
<thead>
<tr>
<th>TOE</th>
<th>Developer</th>
<th>Approved PP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kaspersky Endpoint Security</td>
<td>Kaspersky Lab.</td>
<td>Host IDS, Antivirus, Security Level 2</td>
</tr>
<tr>
<td>Kaspersky Antivirus for Novell NetWare</td>
<td>Kaspersky Lab.</td>
<td>Antivirus, Security Level 2</td>
</tr>
<tr>
<td>Kaspersky Security Center</td>
<td>Kaspersky Lab.</td>
<td>Antivirus, Security Level 2</td>
</tr>
<tr>
<td>Continent 3.7</td>
<td>Security Code</td>
<td>Network IDS, Security Level 3</td>
</tr>
</tbody>
</table>
## Steps Toward Common Criteria Approach: Certified Products, Non-Russian

<table>
<thead>
<tr>
<th>TOE</th>
<th>Developer</th>
<th>Approved PP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deep Security 8.0</td>
<td>Trend Micro</td>
<td>Host IDS, Antivirus, Security Level 4 (~ EAL3+)</td>
</tr>
<tr>
<td>McAfee NSP 7.1</td>
<td>McAfee</td>
<td>Network IDS, Security Level 5 (~ EAL2+)</td>
</tr>
<tr>
<td>Office Scan 10.6</td>
<td>Trend Micro</td>
<td>Host IDS, Antivirus, Security Level 4 (~ EAL3+)</td>
</tr>
<tr>
<td>McAfee Web Gateway 7.4</td>
<td>McAfee</td>
<td>Antivirus, Security Level 5 (~ EAL2+)</td>
</tr>
<tr>
<td>ESET Antivirus</td>
<td>ESET</td>
<td>Antivirus, Security Level 4 (~ EAL3+)</td>
</tr>
</tbody>
</table>
Summary

1. Successful certification against new FSTEC or Russia requirements: 6 (timeline: 2013 - 2014)
2. Certified TOE type: IDS/IPS, antivirus
3. Vendors: McAfee, Secure Code, ESET, PineApp

Questions to research

1. Russian developers are not ready to meet new assurance requirements
2. Absence of typical test methods
3. Evaluation time increasing
NPO Echelon: Evaluation Lab Experience (2)

The diagram compares the time of evaluation (in hours) for different types of evaluation using classical and new approaches. The vertical axis represents the time of evaluation, while the horizontal axis indicates the type of evaluation.

Key Points:
- EAL2/TU
- EAL3/TU+NDO4
- EAL4/TU+NDO3
- EAL5/TU+NDO2

New approach lines are shown in blue, while classical approach lines are in red.

The graph illustrates how the time of evaluation increases with more advanced types of evaluation (EAL3, EAL4, EAL5) for both approaches.
Final Remarks

1. First certifications according to the new requirements are certification of non-Russian products.
2. More and more leading non-Russian developers provide the Russian Evaluations Laboratories with an access to their source code, and this tendency shall be observed in future.
3. Efficiency in detection of vulnerabilities in software submitted for certification shall enhance.
4. The Russian developers shall pay more for certification.
5. The number of actively working Evaluations Laboratories will reduce.
Let's go!
Contact Information

- Alexander Barabanov, Ph.D., CISSP, CSSLP
  Bauman MSTU, NPO Echelon
  ab@cnpo.ru

- Alexey Markov, Dr.Sc., CISSP, Member of IEEE, ACM
  Bauman MSTU, NPO Echelon
  mail@npo-echelon.com; a.markov@bmstu.ru

DOI: 10.1145/2799979.2799980
Thank you for your attention!