Secure software development in the Russian IT Security Certification Scheme

Alexander Barabanov, Alexey Markov, Valentin Tsirlov
Agenda

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

- **1995**: Establishment of Russian IT Security Certification Scheme
- **1997**: Mandatory requirements for firewall and access control systems
- **1999**: Mandatory requirements for source code analysis
- **2003**: Guidance based on CC v.2.1
- **2012**: Mandatory requirements for antiviruses (based on CC)
- **2013**: Mandatory requirements for IPS/IDS (based on CC)
- **2014**: Mandatory requirements for trusted boot loader (based on CC)
Brief overview: who takes part in the certification process?
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
- **Obtaining a certificate from FSTEC of Russia**: Normally 1 month
Brief overview:
Accredited Evaluation Laboratories
Brief overview:
Accredited Certification Bodies

![Graph showing the number of accredited certification bodies from 2003 to 2014. The graph indicates a steady increase in the number of bodies over the years.]
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 Evaluations

![Bar chart showing the number of product evaluations from 2003 to 2014. The number of evaluations varies significantly, peaking in 2011.](chart.png)
Current status of the Russian Scheme: Certified Products by Types

2011-2014 Evaluation Timeline

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

Echelon information security
Current status of the Russian Scheme: Russian vs. Non-Russian Developers

- 2014
- 2013
- 2012
- 2011

Echelon Information Security
Current status of the Russian Scheme: Non-Russian Developers (2)

- Cisco: 58%
- Microsoft: 7%
- Juniper: 6%
- Oracle: 5%
- Symantec: 3%
- IBM: 3%
- Check Point: 2%
- McAfee: 1%
- Siemens: 1%
- Other: 14%

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

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

2011-2014 Evaluation Timeline
Steps Toward Common Criteria Approach:
Step #1 (1)
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)

The Legal Act

Approved Protection Profile

Target of Evaluation

IT Security Environment

Security Target

Evidences
Steps Toward Common Criteria Approach: Step #2 (2)
Steps Toward Common Criteria Approach: Step #2 (3)

FSTEC of Russia Approved Protection Profiles

- PP for IPS/IDS
- PP for Antiviruses
- PP for Trusted Boot Loaders
- PP for Removable Storage Protection

Protection Profiles in Development

- PP for Firewalls
- PP for Operating System
- PP for DBMS
Steps Toward Common Criteria Approach: Step #2 (4)

http://fstec.ru
Certifications against new FSTEC of Russia requirements: projects summary

Summary:
- **TOE Types**: IDS/IPS, Antivirus, Trusted boot loader
- **Vendors**: HP, McAfee, ESET, Trend Micro, PineApp, Kaspersky Lab, Cisco, Echelon, Altx-Soft, Secure Code
- **Number of active labs**: 4
Certifications against new FSTEC of Russia requirements: Russian vs. non-Russian TOE
Steps Toward Secure Software Development

Russian standard
«Information protection. Secure Software Development. General requirements» (draft)

Proposed Secure Software Development Controls:

- information security threats modeling
- source code static/dynamic analysis
- source code review
- penetration testing
- ...

Echelon
information security
1. First certifications according to the new requirements were provided for non-Russian products.
2. More and more leading non-Russian developers provide the Russian Evaluations Laboratories with access to their source code, and this tendency shall be observed in the future.
3. Efficiency in detection of vulnerabilities in software submitted for certification will advance.
4. Russian developers will pay more for certification.
5. The number of actively working Evaluations Laboratories will degrade.
Contact Information

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

- Alexey Markov, Dr.Sc., CISSP, Member of IEEE
  NPO Echelon
  am@cnpo.ru

- Valentin Tsirlov, Ph.D., CISSP, CISM
  NPO Echelon
  z@cnpo.ru
Thank you for your attention!