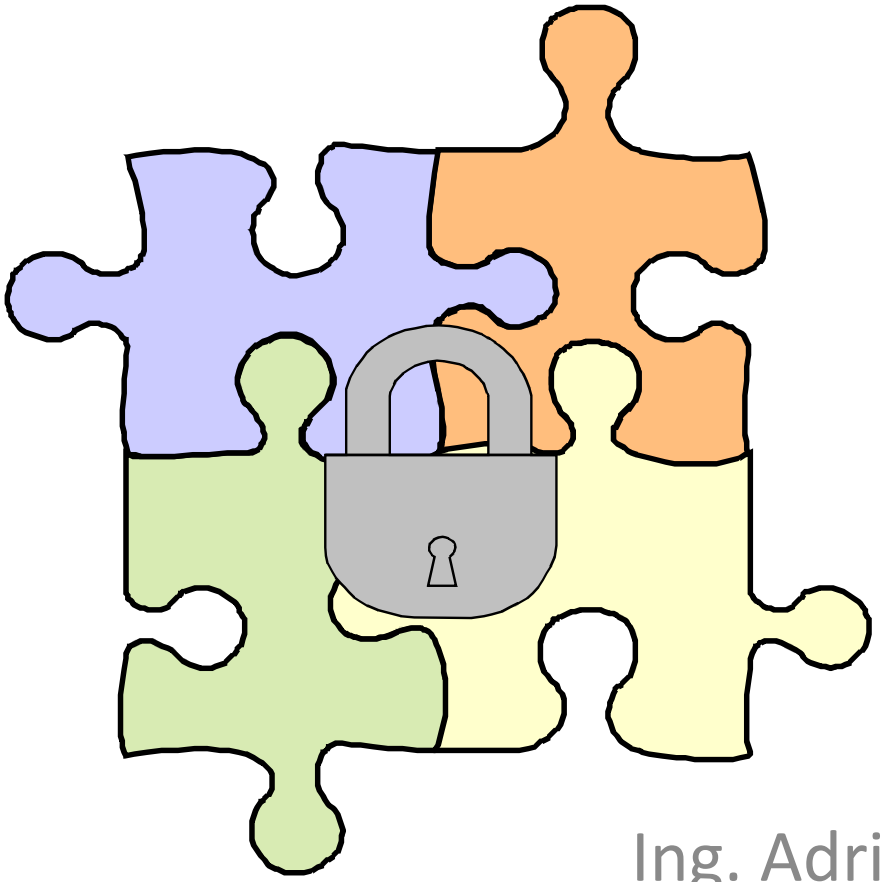
Multi-Level Security (MLS)



Ing. Adrian Demeter

Technical Director

GC System a.s.

The MLS History

60‘ – 70‘ Introduction of MLS

1974 Bell-LaPadula Model

Secure Computer System: Unified Exposition and Multics Interpretation

(approved1976)

1983 US DoD Standard DoD 5200.28-STD:

DoD Trusted Computer System Evaluation Criteria (TCSEC)

(Orange Book – 2nd edition in 1985)

A1, B2, B1, C2, ...

88-90 IBM MVS, RACF, JES2, JES3, TSO, VTAM, DFP, PSF meet B1

1990 Common Criteria (CC) introduced (Canada, Europe)

EAL7, ..., EAL5, EAL4+, EAL4, EAL3+, EAL3, ...

1999 CC approved as ISO 15408

2000 Evaluated Products List

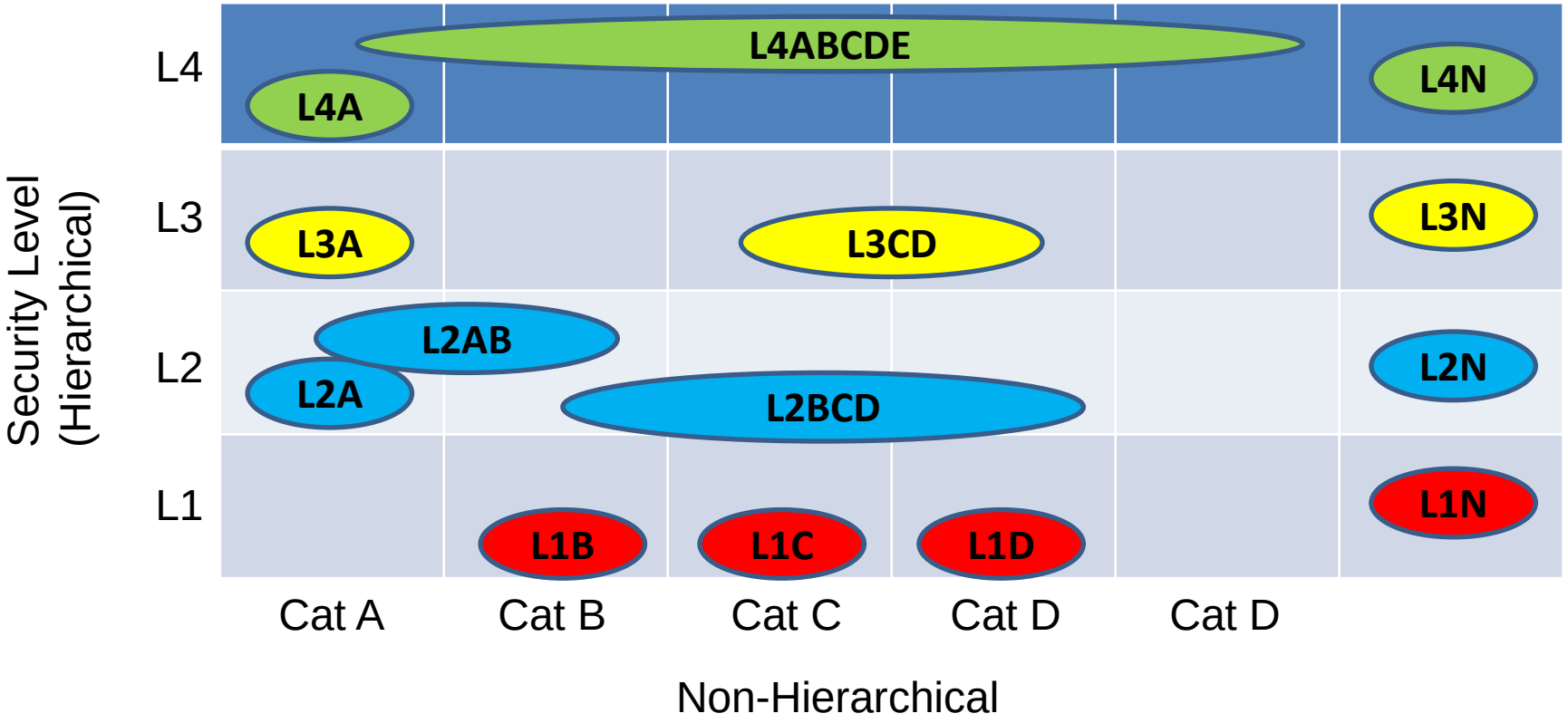
2003-2004 Linux: Fedora, RHEL, SLES

MLS Characteristics

- ✓ Access Control to resources
- ✓ Object Reuse
- ✓ Accountability
- ✓ Labeling hardcopy with security information
- ✓ Name hiding function
- ✓ Write-down
- ✓ Performance

SECLABEL

GC System a.s.



User

SECLABEL: L3CD

→ Cat C

→ Cat D

MLS Granularity

- HW level
- Partitioning & Virtualization
- Operating System
- File (filesystem) level
- Database object level (object, raw, ...)
- Application level
- Presentation level

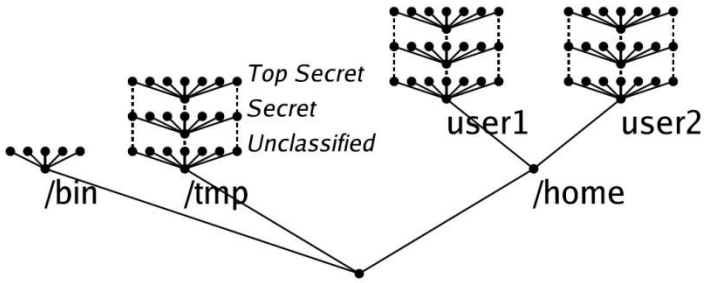
MLS Considerations

- ✓ Security labels
- ✓ Mandatory Access Control (MAC)
- ✓ Discretionary Access Control (DAC)
- ✓ Security labels for data transferred to Tape or Disk
- ✓ Printing security information on hardcopy output
- ✓ Changing a SECLABEL
- ✓ Associating SECLABELs with remote users and restricting „su“
- ✓ SECLABELs for files and directories
- ✓ SECLABEL processing for inter-process communications

  (IPC, signals, ptrace, sockets, FIFO, ...)
- ✓ System-specific labels – e.g. Clustering (SYSPLEX), shared filesystems
- ✓ Encryption and key management
- ✓ etc.

MLS in UNIX World

- ✓ EAL4+
- ✓ Controlled Access Protection Profile (CAPP)
- ✓ Labeled Security Protection profile (LSPP)
- ✓ Role-Based Access Control Protection Profile (RBACPP)
- ✓ Multi-Level Operating Systems Protection Profile (MLOSPP)
- ✓ Polyinstantiated directories



- ✓ IPSec, SSH/Shell login, multi-level cron, labeled print

Examples

IBM: System Z, z/OS, zFS, JES2/JES3, PSF, RACF, zSecure, DB2, zVM, ...

IBM: POWER Systems, AIX with TCB+Enhanced security enabled, PowerVM

Linux: SELinux

RedHat: RedHat Enterprise Trusted Linux

Oracle: Trusted Solaris

Other: Switches, Printers, Message handling, Web Portal, Data Diodes, firewalls

References

Securing DB2 and Implementing MLS on z/OS, SG24-6480-01, 2007
Security on the IBM Mainframe, SG24-7803-00, 2010
http://www.redbooks.ibm.com/

Planning for Multilevel Security and the Common Criteria, GA22-7509-07, 2008
http://publib.boulder.ibm.com/infocenter/zos/v1r10/index.jsp?topic=/com.ibm.zos.r10.e0ze100/e0z2e14003.htm

Secure Computer System: Unified Exposition and Multics Interpretation,1976
http://csrc.nist.gov/publications/history/bell76.pdf

Department of Defense Standard, (Orange Book, TCSEC)
Department of Defense Trusted Computer System Evaluation Criteria
http://csrc.nist.gov/publications/history/dod85.pdf

The Path to Multi-Level Security in Red Hat Enterprise Linux
http://www.redhat.com/f/pdf/sec/path_to_mlsec.pdf

Extending Linux for Multi-Level Security
http://publib.boulder.ibm.com/infocenter/lnxinfo/v3r0m0/topic/liaav/SELinux/lspp-rbac.pdf

Thank you

Ing. Adrian Demeter
demeter@gcsystem.cz

GC System a.s.

Na Strži 3/342
Praha 4
140 00

T: 225987987

Špitálka 41
Brno – město
602 00

T: 543537111

Výstavní 1928/9
Ostrava
702 00

T: 599505120

info@gcsystem.cz

www.gcsystem.cz