

**Session  
OV120**

# ***Security Guidelines for New and Existing OpenVMS Applications***

**Robert Gezelter Software Consultant  
35 – 20 167th Street, Suite 215  
Flushing, New York 11358 – 1731  
United States of America  
  
+1 718 463 1079  
gezelter@rlgsc.com**

***Tuesday, November 9, 1999  
10:00 am – 11:20 am  
Room 3***

***Fall 1999 US DECUS Symposium  
San Diego Convention Center  
San Diego, California***

Security Guidelines for New and Existing OpenVMS Applications

Slide 1

© 1992, 1996, 1999, Robert Gezelter, All Rights Reserved

**Robert Gezelter**

+1 718 463 1079

Software Consultant 35 – 20 167th Street, Suite 215, Flushing, New York 11358 – 1731 USA

## *What makes a secure OpenVMS Application?*

***OpenVMS itself is rated C2.  
Running a C2-rated operating  
system is not sufficient.  
Applications must be designed  
to not compromise the  
integrity and containment  
of the C2-criteria.***

Security Guidelines for New and Existing OpenVMS Applications

Slide 2

© 1992, 1996, 1999, Robert Gezelter, All Rights Reserved

**Robert Gezelter**  
Software Consultant

## *Security Critical Areas*

- Access Control***
- Privileges***
- Contamination***
- Re-invention***

Security Guidelines for New and Existing OpenVMS Applications

Slide 3

© 1992, 1996, 1999, Robert Gezelter, All Rights Reserved

**Robert Gezelter**  
Software Consultant

## **NOTES**

## *Access Control*

### ***Three sample areas:***

- ***Password Management***
- ***DECnet TASK Object***
- ***File Protection and Applications***

Security Guidelines for New and Existing OpenVMS Applications

Slide 4

© 1992, 1996, 1999, Robert Gezelter, All Rights Reserved

**Robert Gezelter**  
Software Consultant

## *Password Management*

- ***Change Frequency – Too Often is not good***
- ***Pronounceability – Important***
- ***Machine Generated – Good, if pronounceable***

Security Guidelines for New and Existing OpenVMS Applications

Slide 5

© 1992, 1996, 1999, Robert Gezelter, All Rights Reserved

**Robert Gezelter**  
Software Consultant

## **NOTES**

## *DECnet TASK Object*

- *facility used for worm attacks*
- *worm attacks have used GUEST and default accts*
- *No alternative if network applications are to be developed (alternatives require  $\geq$  SYSPRV)*
- *safe if used properly*
  - *NO DEFAULT ACCOUNTS*
  - *NO GUEST ACCOUNT*
  - */NONETWORK qualifier*
  - *NONETMBX qualifier*

Security Guidelines for New and Existing OpenVMS Applications

Slide 6

© 1992, 1996, 1999, Robert Gezelter, All Rights Reserved

Robert Gezelter  
Software Consultant

## *File Protection and Applications*

- *Access Control Lists and Identifiers*
  - *Do NOT grant access to individuals*
  - *Files may be accessed by identified classes of users*
  - *Individual accounts are given access to classes of data*
  - *Procedures at access removal/de-briefing*

Security Guidelines for New and Existing OpenVMS Applications

Slide 7

© 1992, 1996, 1999, Robert Gezelter, All Rights Reserved

Robert Gezelter  
Software Consultant

## NOTES

## *File Protection and Applications (cont'd)*

- ***Do NOT block attempts beyond authorization – let the OpenVMS Security Alarms be triggered***
- ***Break single files into multiple files to permit different security levels***

Security Guidelines for New and Existing OpenVMS Applications

Slide 8

© 1992, 1996, 1999, Robert Gezelter, All Rights Reserved

**Robert Gezelter**  
Software Consultant

## *Privileges*

***In a word: DON'T***

***Permissible: TMPMBX***

***Possible: NETMBX***

***Never: Any Devour Class  
NO SYSPRV, CMKRNL, etc.***

Security Guidelines for New and Existing OpenVMS Applications

Slide 9

© 1992, 1996, 1999, Robert Gezelter, All Rights Reserved

**Robert Gezelter**  
Software Consultant

## **NOTES**

## *Contamination*

***Single Thread Application:  
Generally safe and within  
the OpenVMS security model.***

***Multi-threaded Applications:  
Integrity and security  
outside of the OpenVMS model;  
You are on your own!***

***Suggestion:  
Use Shareable Libraries to get  
the memory advantages of  
common executables without  
the Contamination hazard.  
(See session AD021).***

Security Guidelines for New and Existing OpenVMS Applications

Slide 10

© 1992, 1996, 1999, Robert Gezelter, All Rights Reserved

Robert Gezelter  
Software Consultant

## *Re-Invention*

***When you re-write something, it  
a reliable bet that you will  
forget about some seemingly  
small feature. Unfortunately,  
system security depends upon  
the interaction of many small,  
seemingly baroque details.***

Security Guidelines for New and Existing OpenVMS Applications

Slide 11

© 1992, 1996, 1999, Robert Gezelter, All Rights Reserved

Robert Gezelter  
Software Consultant

## NOTES

## *Re-Invention (cont'd)*

### ***Example:***

***If you need a LOGIN authentication mechanism, use LOGINOUT and AUTHORIZE in concert with SYSUAF to validate and login your users. Attempting to replicate the functionality is more likely to lead to a breach***

***If you require some capability not in standard LOGINOUT, consider using the exit or use or use a image executed during SYLOGIN.COM.***

Security Guidelines for New and Existing OpenVMS Applications

Slide 12

© 1992, 1996, 1999, Robert Gezelter, All Rights Reserved

Robert Gezelter  
Software Consultant

## *Summary:*

***It is possible to build extremely robust and secure applications under OpenVMS; provided that you do not compromise the integrity of the system; instead using OpenVMS and its underlying capabilities to leverage your own efforts.***

Security Guidelines for New and Existing OpenVMS Applications

Slide 13

© 1992, 1996, 1999, Robert Gezelter, All Rights Reserved

Robert Gezelter  
Software Consultant

## NOTES

# Questions?

**Robert Gezelter Software Consultant**  
**35 – 20 167th Street, Suite 215**  
**Flushing, New York 11358 – 1731**  
**United States of America**

**+1 718 463 1079**  
**[gezelter@rlgsc.com](mailto:gezelter@rlgsc.com)**

Security Guidelines for New and Existing OpenVMS Applications

Slide 14

© 1992, 1996, 1999, Robert Gezelter, All Rights Reserved

**Robert Gezelter**

Software Consultant 35 – 20 167th Street, Suite 215, Flushing, New York 11358 – 1731 USA

+1 718 463 1079

## NOTES