

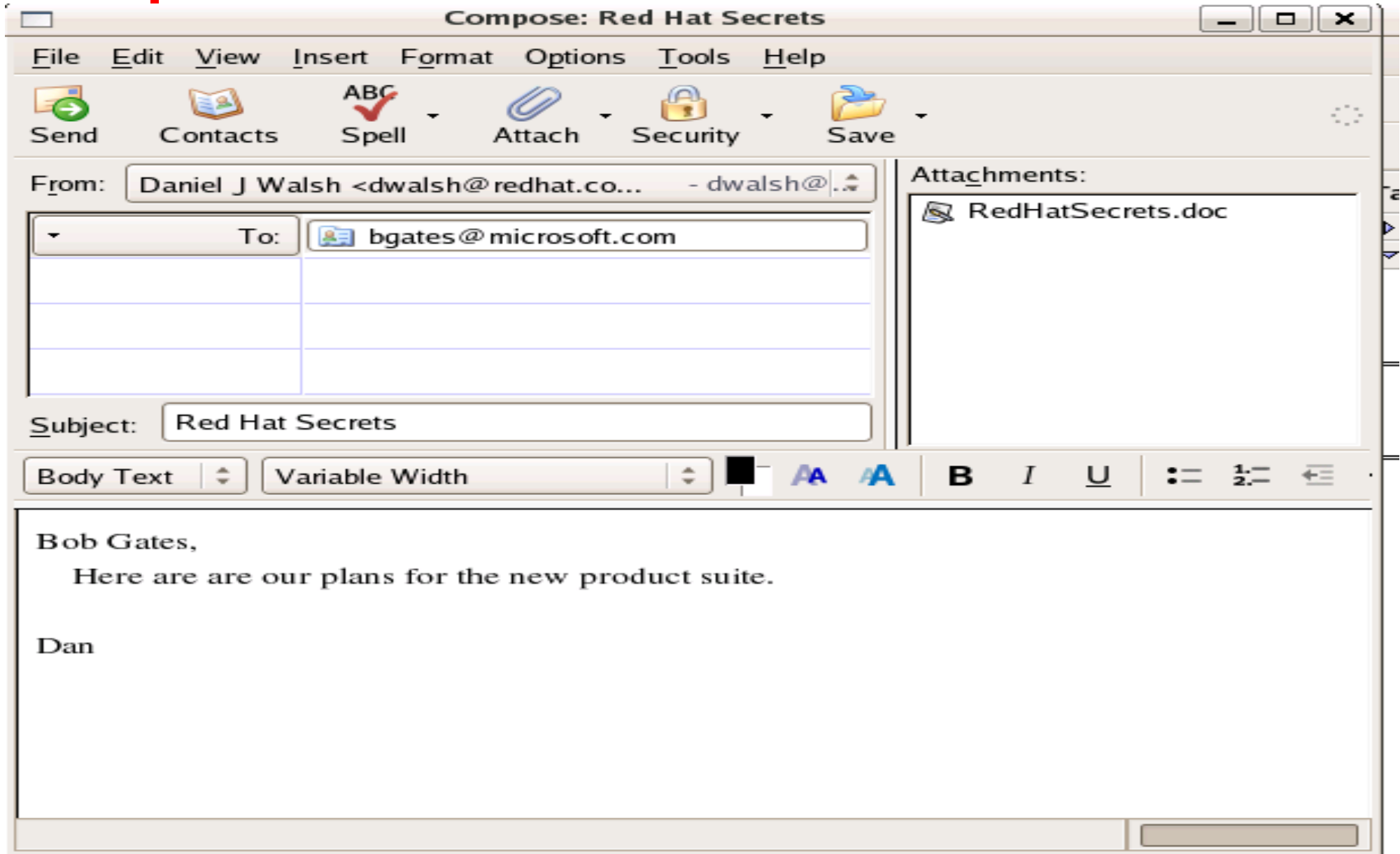


Multi- Category Security (MCS)

Daniel J Walsh
SELinux Lead Engineer
dwalsh@redhat.com



Oops!!!!



The screenshot shows a "Compose: Red Hat Secrets" window. The "From" field is "Daniel J Walsh <dwalsh@redhat.co... - dwalsh@...>". The "To" field is "bgates@microsoft.com". The "Subject" is "Red Hat Secrets". An attachment named "RedHatSecrets.doc" is listed. The email body contains the text: "Bob Gates, Here are are our plans for the new product suite. Dan". The window has a menu bar (File, Edit, View, Insert, Format, Options, Tools, Help) and a toolbar with icons for Send, Contacts, Spell, Attach, Security, and Save. The text area has a rich text editor toolbar with options for Body Text, Variable Width, bold, italic, underline, bulleted list, numbered list, and indent.

Compose: Red Hat Secrets

File Edit View Insert Format Options Tools Help

Send Contacts Spell Attach Security Save

From: Daniel J Walsh <dwalsh@redhat.co... - dwalsh@...>

To: bgates@microsoft.com

Subject: Red Hat Secrets

Attachments: RedHatSecrets.doc

Body Text Variable Width **B** *I* U : = 1: = ←

Bob Gates,
Here are are our plans for the new product suite.
Dan



Setting the record straight

- Example Policy - > Reference Policy
 - Base policies package used by distributions to build shipping policy
 - targeted, strict, MLS
- MCS Is not a new policy package
- MCS is a optional way to build targeted or strict
- Fedora/ Red Hat will ship in FC5/ RHEL5:
 - selinux-policy-targeted == targeted-mcs
 - selinux-policy-strict == strict-mcs
 - selinux-policy-mls == strict-mls



What is MCS?

- MCS Is MLS with a single Sensitivity
- MLS/ MCS flag is the fourth field of the SELinux context
 - system_u:object_r:user_home_t:s0:c1
 - MLS runs with up to 16 sensitivities, s0- s15
 - MCS runs with single sensitivity, s0
 - MLS/ MCS support 256 category combinations, c0- c255
- Prevent Stupid Mistakes versus Malicious Users
 - Discretionary/ advisory scheme
 - User- oriented
 - Prevent Accidental Leakage
- Targeted domains will be prevented by TE by default



Benefits of MLS for a Mainstream OS

- Can MCS do for MLS what targeted policy did for SELinux?
 - Potentially useful to more people
 - Mainstream use of technology
 - Higher overall quality
- User- innovation
- Currently in Rawhide
 - MCS labeling for files
 - MLS kernel flag enabled by default



MCS/MLS Infrastructure

- Needed a way to make categories human readable
 - libsetrans
 - optional library used by libselinux to translate MLS Level of security context into Human readable context



/ etc/ selinux/ POLICYTYPE/ setrans.conf

```
# Multi- Category Security translation table for SELinux
# Uncomment the following to disable translation library
# disable= 1
# Objects can be categorized with 0- 256 categories defined by the admin.
# Objects can be in more than one category at a time.
# Categories are stored in the system as c0- c255. Users can use this
# table to translate the categories into a more meaningful output.
# Examples:
s0=
s0:c0= CompanyConfidential
s0:c1= PatientRecord
s0:c2= Unclassified
s0:c3= TopSecret
s0:c1 ,c3= CompanyConfidentialRedHat
s0- s0:c0.c255= SystemLow- SystemHigh
s0:c0.c255= SystemHigh
```



Translation

- system_u:object_r:user_home_t:s0:c1
 - system_u:object_r:user_home_t:PatientRecord
- system_u:object_r:user_home_t:s0
 - system_u:object_r:user_home_t



Setting MLS/ MCS Flag

- chcon
 - chcon -l PatientRecord / opt/ patients/ dwalsh
- chcat
 - wrapper around chcon
 - chcat + PatientRecord / opt/ patients/ dwalsh
 - chcat + CompanyConfidential / opt/ patients/ dwalsh
 - user_r:object_r:type_t:PatientRecord,CompanyConfidential
- Nautilus, Mailers, OpenOffice, Web Browsers

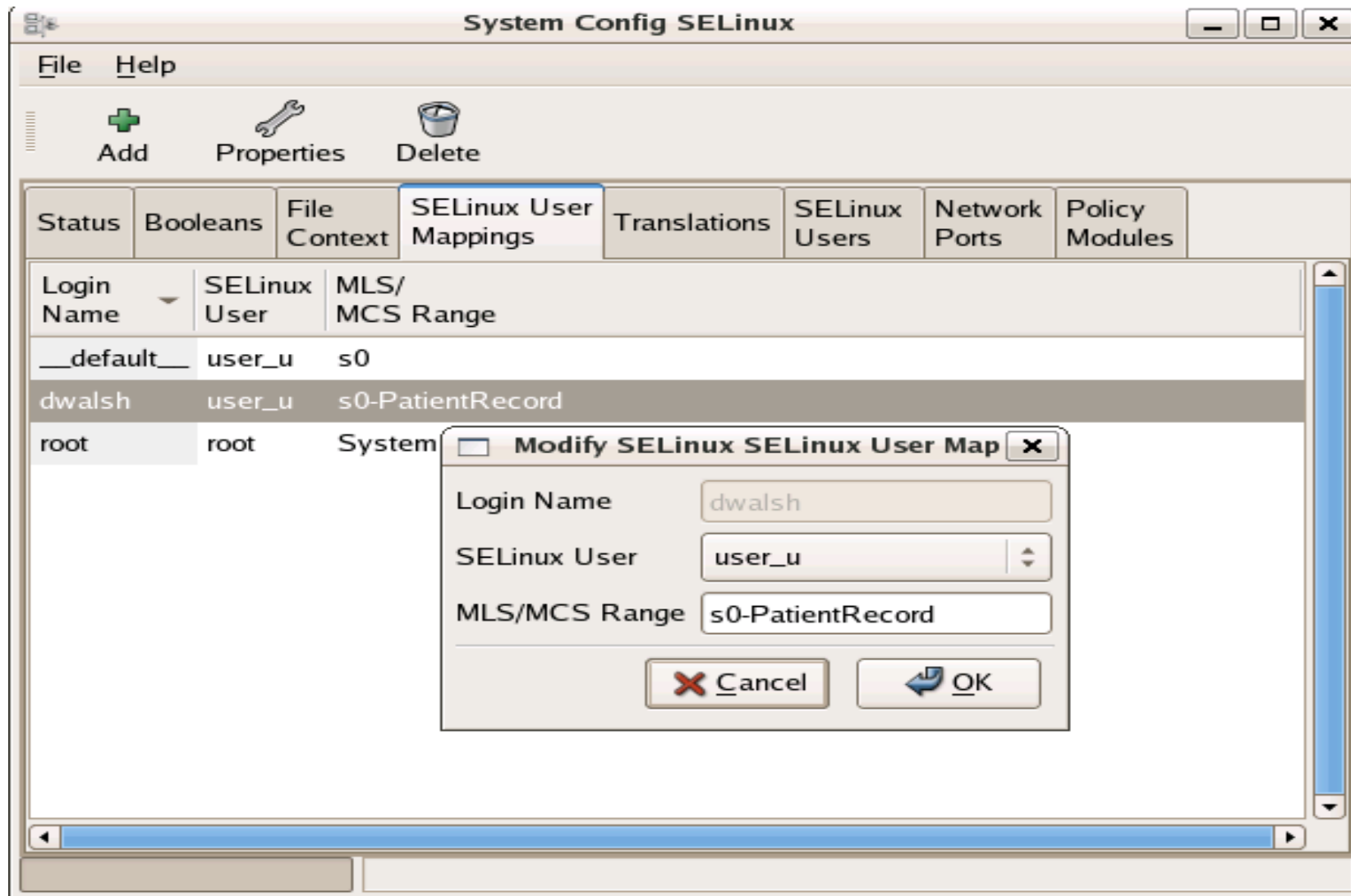


Setting Users MLS/ MCS Range

- / etc/ selinux/ POLICYTYPE/ seuser
 - semanage login - m - r s0- PatientRecord,CompanyConfidential dwalsh
 - chcat -l + PatientRecord dwalsh
- chcat -L -l dwalsh
 - dwalsh: PatientRecord
- id -Z
 - user_u:system_r:unconfined_t:s0- PatientRecord



Graphical Tools





What Next?

- Labeled Printing
 - lpr - P ReceptionistPrinter / opt/ patients/ dwalsh.pdf
 - Error: You are not allowed to print this doc on ReceptionistPrinter
 - lpr - P LabTech / opt/ patients/ dwalsh.pdf
 - Header and footer will identify document as a “PatientRecord”
- Labeled Mail
 - Mail List associated with MCS Framework
 - Mail domain (redhat.com) associated with MCS Framework.
- Auditing?
- How do I run multiple Apache servers to display different categories?
 - MLS Challenge as well