X Access Control Extension Specification

Eamon F. Walsh

X Version 11, Release 7.7

!

" # $

%

"&' ()"*+,' - ,(.-/'/ 0+ - 1 *-"&(2" *+,,+3"4 () +34
5-3/ '6 ,' (, -7 8-'/ -3982/-3: ;2" 3(" 8-7-'"/ "("&'
*+,,+3"-' () 7',9&+3"+;-8-"4)-"3')(, + +,"-928+, 2,
(' +3/ 3(3-3),-3:'7'3'% -3 3('.'3" &+88 "&' +2"&(, (,
9(4,-:&" &(8/', ;' 8-+;8')(, +34 98+-7 /+7+:' (, ("&
', 8-+;-8-"4 *&'"&', -3 +3 +9"-(3 () 9(3",+9" "(," (, ("&
',*- ' +,- -3:),(7 (2" () (, -3 9(33'9"-(3 *-"& "&' ()"
+,' (, "&' 2 ' (, ("&', /'+8-3: -3 "&' ()"+,'%

2009

Revision History		
Revision 1.0	19 Oct 2006 Initial Version	efw
Revision 2.0	10 Mar 2008 Version 2.0	efw
Revision 2.1	19 Jun 2009 Version 2.1 (XI2)	efw
Revision 2.2	29 Jun 2009 Version 2.2 (Property post-data hook)	efw

Abstract

" 6 + 9 '$ 6+9' <
6 $ < % " 6+9' #
$ # < % "
8 $ 7 8 7 8 $ 5 %

6+9' # =%> ? '92,-"4 $ #
% - <
'92,-"4 < %
6+9' # @%> <
% 9 # $ $
, 9 %)
%

" 6+9' # @%> #
/-6 (#
< 6+9' % - $
6+9' %
6+9' %

Table of Contents

- %%% K
A %%% K
%%% K
* < %%%L
. @%> 9 %%% L
) * < %%% M
2 %%% N
%%% N
2 & < %%% N
%%% @=
, A %%% @=
'# %%% @=
' %%% @=

Introduction

Prerequisites

" $
6% - 9 % -
< 6
6 # %

Purpose

6+9' < 6 #
< $ % " #
$ /-6 (6 # % "
# $ # <
6 # # 6 # #
%

) $ 6%(6 # C
< # -/ % " <
-/ # $
< %) $
$ C
< ifdefC % & # $
if
% + $
< # <
$ < < %)
$ $
$ %

" 6 + 9 '$ <
6+9' #
% ($?
< < % * < #
< % " < #
<
% 6+9' <
< % 6+9'
; +
A %

" <
# # #
% "
< < # < #
% (# <
%

Prior Work

Security Extension

6+9' '92,-"4 $ % " $
#
? < % 2
< 3
<
% # $
$ # %

Solaris Trusted Extensions

" '$ 6 $ 6
% 6+9' < #
< 6 % - 6 '92,-"4
$ # < 6+9' < %

Linux Security Modules

6+9' 8 $ 7 #
< < 8 $ < %

Version 2.0 Changes

Different Return-Value Semantics

" # %)
$ #)
% - # @%> # < %
6
%" BadAccess
BadAlloc BadMatch
< 0 1 %

DevPrivates Mechanism

" # # 6 # #
$ %" # #
# % #
# # $
% 9 < #
? %)
< # #
C %

New Access Modes

- # # D
! % - # @%> #
6 % "
D <
< %

Polyinstantiation

6+9' %
0 + 1 0 + 1
<
<
< % "
%

Removed Hooks

" < < # # %
" # < % "
< # # <
0 # + 1 % " $
< # # '92,-"4 $ #
A %

New Hooks

3 # < # # #
% 9 # <
$ KillClient #
$ %
# < #
# A % + < %

Changes to Existing Hooks

E " <
% "
*
DixCreateAccess%

E " # < , A #
%

E " < 3 #

% " $ #
0 1 % 3
%

E " $ < %

Future Work

Security Hooks

- < # 6+9'
% < % 7 < <
6 # % '$ <
$ % 9
6+9' # $
%

- 6+9' <
$ $ A $
A # % "
<
6+9' < % " # # <
%

Core X Server

" $ 6% $ % 7
#
% " :86 $ <
%

" # C # # <
6+9' % - $
$
# # # #
% " # #
$
< # %

Usage

Storing Security State

" $
$ % 6+9'
# %

(# $ % "
< # ?
% (6
#
< %

+ $ C
# % " # devPrivates
# /-6 %
# # %) # #
6 # %

Using Hooks

Overview

6+9' $ % -
Xext/xacestr.h 6+9' <
% (Xext/xace.h #
%

6+9' < 6 # < % 4
$ C < !

```
void MyCallback(CallbackListPtr *pcbl, pointer userdata,
pointer calldata);
```

* < *pcbl* < % " 6 < # 6+9' < % , $ <% *userdata* XaceRegisterCallback F $ <% *calldata* # 6+9' <% " < % 4 $ %

" < # < XaceRegisterCallback!

```
Bool XaceRegisterCallback(int hook, CallbackProcPtr call-
back, pointer userdata);
```

* *hook* 6+9' < *callback* < *userdata* < # % " Q= 06+9' < %1 6+9' < % XaceRegisterCallback $? F '92,-"4 $ % " # TRUE FALSE %

" < XaceDeleteCallback!

```
Bool XaceDeleteCallback(int hook, CallbackProcPtr callback,
pointer userdata);
```

XaceRegisterCallback% " # TRUE FALSE %

Hooks

" 6+9' < " Q= 06+9' < %1 % + 0 & < 1 < < 6+9' 6 # %

6 6

	!	"
XACE_CORE_DISPATCH	6 9 / ,	09 / 1
XACE_EXT_DISPATCH	6 '$ + ,	0'$ / 1
XACE_RESOURCE_ACCESS	6 , + ,	0, + 1
XACE_DEVICE_ACCESS	6 /# + ,	0/# + 1
XACE_PROPERTY_ACCESS	6 + ,	0 + 1
XACE_SEND_ACCESS	6 + ,	0 + 1

	!	"
XACE_RECEIVE_ACCESS	6 , #+ ,	0, # + 1
XACE_CLIENT_ACCESS	6 9 + ,	09 + 1
XACE_EXT_ACCESS	6 '$+ ,	0'$ + 1
XACE_SERVER_ACCESS	6 # + ,	0 # + 1
XACE_SELECTION_ACCESS	6 + ,	0 + 1
XACE_SCREEN_ACCESS	6 + ,	0 + 1
XACE_SCREENSAVER_ACCESS	6 + ,	0 # + 1
XACE_AUTH_AVAIL	6 + +# ,	0+ ? +# & <1
XACE_KEY_AVAIL	6 5 +# ,	05 +# & <1
XACE_AUDIT_BEGIN	6 + ,	0+ & <1
XACE_AUDIT_END	6 + ,	0+ & <1

- # Xext/xacestr.h #
%

Core Dispatch

" < $ $ A
% " <
6 9 / , % " *client* 9
status %

" *client* < A % 3
A # *requestBuffer*
% " REQUEST include/dix.h #
%

" *status* ? 6 % - #
A
%

Extension Dispatch

" < $ $ $
A % " <
6 '$+ , % " *client* 9
ext '$ ' G *access_mode* 7 < *status*
%

" *client* < A % 3
A # *requestBuffer*
% " REQUEST include/dix.h #
%

" *ext* $ % " A
$ %

" *access_mode* DixUseAccess < $ %

" *status* ? 6 % - #
A
%

Resource Access

" < $ < % " <
6 , + , % "
client 9 *id* 6-/ *rtype*
,' "4 ' *res* *ptype* ,' "4 ' *parent*
access_mode 7 < *status* %

" *client* < %
3 serverClient # < %

" *id* -/ < %

" *rtype* < %

" *res* ! < %

" *ptype* ,"D3(3' %

" *parent* 3288 % "
! " A
access_mode DixCreateAccess
A % " QB 0,
< %1 % "
%

" *access_mode* % " #
include/dixaccess.h% "
% " " Q@ 0,
< %1 % 3 DixCreateAccess
!
% " # $?
# # % -

-/%

" *status* ? 6 % - #
< #
%

6# 6''

$ %	$	& ! '
DixReadAccess	" %	: - : 9 - 9 H 9
DixWriteAccess	" %	- , ") 9 + 9 , 9
DixDestroyAccess	" # %	9) / *) $) 9 ,)
DixCreateAccess	" %	9 * 9 $ 9 :9 9 9
DixGetAttrAccess	" C A %	: * + : : H) 9 :9 H ; ?
DixSetAttrAccess	" C %	* + 9 :9 9 , 6) $ 9 3
DixListPropAccess	2 %	8
DixGetPropAccess	+ %	: ,
DixSetPropAccess	+ %	9 , /
DixListAccess	9 %	H " 7 2
DixAddAccess	+ %	9 * , * + 9 , 9 , + :
DixRemoveAccess	+ # %	/ * , *) 9 ,) :
DixHideAccess	(# %	2 * 6) $ & 9

$ %	$	& ! '
DixShowAccess	(%	7 * 6) $ 9
DixBlendAccess	/ $ %	; < 3 9 , * 9 ,
DixGrabAccess	(# %	9 * 9 * +
DixInstallAccess	9 %	- 9
DixUninstallAccess	9 %	2 9
DixSendAccess	+ # %	'#
DixReceiveAccess	+ # < %	9 * + 6 '$ '#
DixUseAccess	" %	9 *) : ; 9 :9
DixManageAccess	* %	9 * 9 # , *

6(6" !)

" !	* " !	+
RT_WINDOW	RT_WINDOW	9 % " 3288 %
RT_PIXMAP	RT_WINDOW	9(7 (-"' $! $ %
RenderPictureType	RC_DRAWABLE	" , %

Device Access

" < $ # %"
< 6 /# + , %"
client 9 *dev* /# -
access_mode 7 < *status* %

" *client* # < %
3 serverClient%

" *dev* # %

" *access_mode* % " #
%

" *status* ? 6 % - #
# #
%

6, 6- .

$ %	$	& ! '
DixGetAttrAccess	+ # A %	: 5 7 6 : 5 9 6< : / # -
DixReadAccess	" # %	H H 5 6< :
DixWriteAccess	" # %	* 6") < - 6 '$ '#
DixSetAttrAccess	# %	6< 9)
DixManageAccess	: # %	9 5 7 6 9 / # 9 6< 9
DixUseAccess	" # %	6 (/ # 6< '#
DixGrabAccess	" # %	: : ; : 5
DixFreezeAccess	" # ? %	: 5 :
DixForceAccess	" # # %	: : ;
DixGetFocusAccess	" # # %	: -) 6 : / #)
DixSetFocusAccess	" # %	-) 6 / #)
DixBellAccess	" # %	; 6 / # ;
DixCreateAccess	" # %	6-9 / # & 6-+ 7
DixDestroyAccess	" # # %	6-9 / # & 6-, # 7
DixAddAccess	+ # # # %	6-9 / # & 6-9 +
DixRemoveAccess	+ # # # %	6-9 / # & 6-9 +

$ %	$	& ! '
DixListPropAccess	# %	8 /# 6-8
DixGetPropAccess	+ # %	: /# 6-:
DixSetPropAccess	+ # %	/# 6-

Property Access

" < $
% " <
6 + , %" client
9 *pWin* * *ppProp* G
access_mode 7 < *status* %

" *client* % 3
serverClient # < %

" *pWin* %

" *ppProp* ,
%" $ # F %
- $

" *access_mode* %" #
%

" *status* ? 6 % - #
A
% & # BadMatch F %

6/ 6* !

$ %	$	& ! '
DixCreateAccess	" DixWriteAccess %	9
DixWriteAccess	" # %	9 ,
DixBlendAccess	" %	9
DixReadAccess	" %	:
DixDestroyAccess	" %	/

$ %	$	& ! '
DixGetAttrAccess	'$ %	8
DixPostAccess	DixWriteAc- cess %	9

3 6+9' . @%> < %
" $ #
$ % "
$ <
!

E * DixCreateAccess $
% -
ppProp %

E * < *ppProp*
< # % " $
<
, *next*
%

E + < *status* Bad-
Match /-6 $ % "

< %

3 6+9' . @%@ < $ #
% (
< % " # # %
" # DixPostAccess DixWriteAccess
ppProp % *status*
Success #
%

3 DixCreateAccess *pp-*
Prop % & $ #
< DixPostAccess DixCreateAccess
DixWriteAccess% - $
DixPostAccess %

Send Access

" < $ # # 6
% " <
6 + , % " *client* 9 *dev*
/# - *pWin* * *events*
count *status* %

" *client* SendEvent A
% " 3288 *dev*
%

" *dev* # # #
% " 3288 *client* %

" *pWin* %

" *events* # %

" *count* # *events* %

" *status* ? 6 % - #
% %

0

" < # # # %

Receive Access

" < $ # # 6 #
% " <
6 , #+ , % " *client*
9 *pWin* * *events* # *count*
status %

" *client* # # %

" *pWin* # %

" *events* # %

" *count* # *events* %

" *status* ? 6 % - #
%

0

" < # # # %

Client Access

" < $ #
% " < A Kill-
Client% " < 6 9 +
, % " *client* 9 *target*
9 *access_mode* 7 < *status* %

" *client* < A %

" *target* %

" *access_mode* % " #
%

" *status* ? 6 % - #
A #
%

61 6

$ %	$	& ! '
DixGetAttrAccess	+ A %	:
DixSetAttrAccess	+ %	
DixManageAccess	" C # %	9 / 7
DixDestroyAccess	" < %	5 9

Extension Access

" < $ # A # #
$ # % " # $
# % " < 6 '$ + , %
" *client* 9 *ext* '$
' G *access_mode* 7 < *status* %

" *client* < A
QueryExtension ListExtensions%

" *ext* $ % " A
$ %

" *access_mode* DixGetAttrAccess < $ %

" *status* ? 6 % - #
$ QueryExtensions
ListExtensions %

0

- < $ <
< # <
$ %

Server Access

" < $ # A 6
% " < 6 # +
, *client* 9 *access_mode*
7 < *status* %

" *client* < A %

" *access_mode* % " #
%

" *status* ? 6 % - #
A #
%

62 6' .

$ %	$	& ! '
DixGetAttrAccess	+ # A %	:)
DixSetAttrAccess	+ # %	)
DixManageAccess	# %	9 + 9 8 &
DixGrabAccess	+ # %	: #
DixReadAccess	" # C %	, 6'.-' $
DixDebugAccess	# %	6" $ 6< /)

Selection Access

" < $
% " <
6 + , % " *client*
9 *ppSel* GG *access_mode* 7 <
status %

" *client* % 3
serverClient # < %

" *ppSel*
% " $ # F
% - $
, G %

" *access_mode* % " #
%

" *status* ? 6 % - #
A
% & # BadMatch F %

63 6'

$ %	$	& ! '
DixCreateAccess	" DixSe- tAttrAccess %	(
DixSetAttrAccess	" %	(
DixGetAttrAccess	" A %	: (

$ %	$	& ! '
DixReadAccess	+ # A %	9 #

" < % "
$ # $
% "
$ < !

E * DixSetAttrAccess
$ <
% - *ppSel* %

E * < *ppProp*
< # % " $
<
next %

E + < *status* BadMatch /-6 $ % "

< %

Screen Access

" < $ # A
" < 6 +
, % " *client* 9 *screen*
access_mode 7 < *status* %

" *client* < A %

" *screen* %

" *access_mode* % " #
%

" *status* ? 6 % - #
A
%

64 6'

$ %	$	& ! '
DixGetAttrAccess	+ A %	8 - 9 H ; ?
DixSetAttrAccess	+ %	- 9
DixHideAccess	" %	6) $ & 9
DixShowAccess	" %	6) $ 9

Screen Saver Access

" < $ # A
% " < 6
+ , %" *client* 9 *screen*
access_mode 7 < *status*
%

" *client* < A %

" *screen* %

" *access_mode* %" #
%

" *status* ? 6 % - #
A
%

6 5 6' .

$ %	$	& ! '
DixGetAttrAccess	+ # A %	: # # H -
DixSetAttrAccess	+ # %	# # -
DixHideAccess	" # #	) # / 7'
DixShowAccess	" # # %	) # / 7/

Authorization Availability Hook

" < $ $?
%"
? % " <
6 + +# , %" *client*
9 *authId* 6-/%

" *client* %

" *authId* -/ C ? %

" < # %

+

" <
% 5 $
ClientStateCallback < < %

" < + :,(2 '$ % - <
ClientStateAuthenticat-
ed%

Keypress Availability Hook

" < $ $ <
% " # < % "
< 6 5 +# , % "
event $'# *keybd* /# -
count %

" *event* < # KeyPress KeyRelease%

" *keybd* # # %

" *count* # =>>IJ
%

" < # %

Auditing Hooks

" < # % " <
A <
09 / 1 % " <
A % " <
6 5 +# , % " *client*
9 *requestResult* %

" *client* < A %

" *requestResult* A Success
% 3 <%

" < # # %

Protocol

Requests

6+9' 6 %

Events

6+9' 6 %

Errors

6+9' 6 %