Analysis of the X Protocol for Security Concerns

David P. Wiggins, X Consortium

Analysis of the X Protocol for Security Concerns

! " ##$
% & ' © ##$ % (

Abstract

)' & & (& & & ('
* + ' ' , (' ('
+' ' (' & & (
' (' ' -

(' ' & & ' +
(. ' /0 + /1 ' 0 + + ' + ' (' '
& ((& ' 2 & ' 0 + & (&
+' (' 0 + ' 3 ' + 4

)' & ' ' & (' & & '
0 +

)56 078) 9 6 *0 7 * 6 :90 *0; *)57<) 9 9=)> 78 9=> ?*= 6 600 7 *! @*6 *=%@< *=A
B<) =7) @*!*)6)7)56 9 9=)*60 78 !6 %59=)9B*@*)> 8*)=600 87 9 9)*%<@9 < 706 9=
=7=*=8 *=A6!6=) *= =7 6 6=) 059@@)56 %7=07)*<! B6 @*9B@6 87 9=> %@9*! 9!9A60 7
7)56 @*9B*@*)> 56)56 *= 9= 9%)*7= 78 %7=) 9%))7) 7 7)56 *06 9 *0*=A 8 7! 7<) 78
7 *= %7==6%)*7= *)5)56 078) 9 6 7)56 <06 7 7)56 69@*=A0 *=)56 078) 9 6

6C & ' ' (' % (' ' +
& (' ' ' 0 + + ' & + ' , (' % (

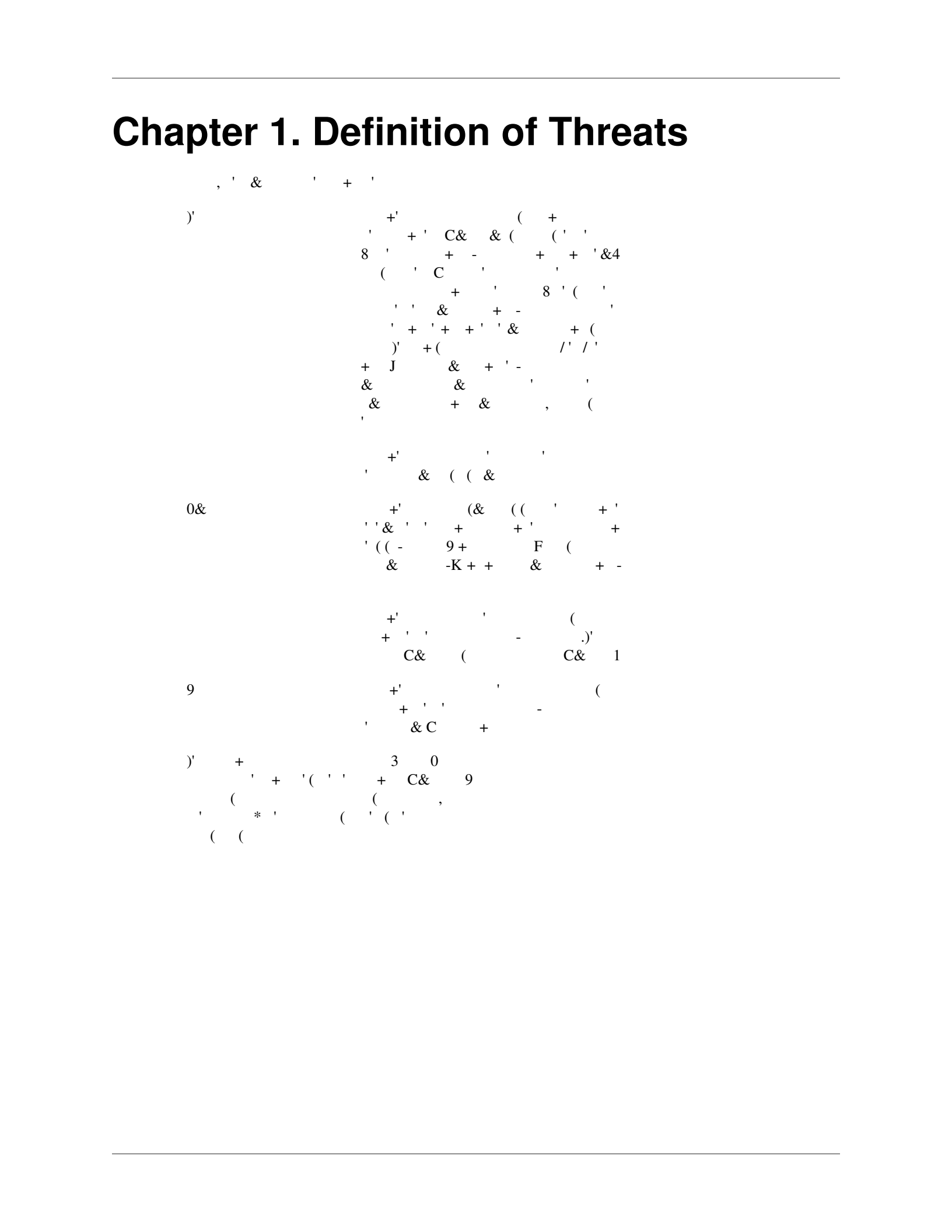
+ 0 ((-)' 7& A &

Table of Contents

)'
A (
9 0
0 D
! (6C' D
% < ! & , E
D 0 + ' & + + H
B - & C(& H
% & 8 (H
7 $
E 0 + ' & F
% +
%' +9
A +9 I
+ 0 + + I
%' 0 0 I
! & + #
+ 7& #
A A ("
G) "
* 9 ("
A 9 (= (
%' &
&
A &
&
@ &
0 0 7+
A 0 7+
% 0 D
0 6 D
? A D
%' 9 A E
A 0 E
G E
A ! 6 E
) % E
& H
0 * & 8 H
A * & 8 H
G ? (& H
8 F H
% 8 $
0 8 ' $
A 8 ' $
% C(&
8 C(&
% A%
% & A%
%' A% 0 ' 0 % &
8 A%

+ F I
A *(I
% % (& I
8 % (& I
% & % (&9 8 #
* % (& < % (& #
@ * % (& #
% 9 F #
8 % "
0 % 0 = (% "
G % @ - &% "
% % % A &'% "
8 % "
% "
G B 0 ,
@ 6C G 6C
? F
? F F
%' % 0 ! &&
A % A ! &&
0 0 0
A 0 0
8 0 0
%' 5
@ 5
0 9 %
0 % + ! D
? % D
% F D
H 6 E
? (&= E
6C& E
A &' 6C& E
= E
& = E
% = H
% F H
0 % H
0 F H
! && = H
$ 6 $
8 -
I I

Chapter 1. Definition of Threats



Chapter 2. General security concerns and remedies

)' + & (' 9
('& (+ & (9 ++ '
 & (+ ' & (' & +

* (& ' & ' (- ' +
 ' 4

 6C ' F ( )' ' ' ' +' + '
 & ' ' +

 6C ' F (((
 (' F ' &

D 9 - ' +' (' ' ' '
)' (& ' & ((&

E) ' F & * ' + & (
 - ' ' + ' '

H 0 & ' * ' + ' '
 ' & ' + & ' (+ (
 - ' ' + (' '

 ? ')' (' ' ' ' ' '
 '

* (+ & ' & ' ((&& &
' ' - ' ' ' ' (& (
 ' (& && 7 '
 + ' ' (& ' 9 + (&
 & && ' ' + + ' +
&& + '

* (+ + 9 +' ' &
 C& +)' + 9 +' &
 (. (& 1 ' &)' +
& 9)' + +

Access to Server Resources

)' & + (& . 3 1 '
 ' 9 F ' & *
 (' ' 0 ' F & +
 * ' 9 (- &
 * ' F - + ' (
* ' / * / ' +

7 - ' & (' ' && &
& ' C & ' J

' 9 ' & & &
' ' J ' ' &)' B + & 3
+ (' ' + &
) ' ')' +
& (+ + < +
& (' ')' ' ' + ' +
(- ' + ' & ' (& .(' + 1 &

! ' (&& ' J ' +
' (& + ' ' (( )' +
C & (+' ' + ' &
F)' 4 *%%%! ! &
- ' + + (& 9 ' (3 C &
' + + (+' ' (& + + ' &&
)' + + (+ ' (&&

)' (& (('
9 + + L C2
M4 LookupIDByType LookupIDByClass 9 + ' - '
& ' + (' ' ')' (& (
' +' ' ' - & '
' & (.& + &
(& 1 ' F %

*00<64 + + + ' '
+ ' - ! & C& '(N .6
' + ' & '
+ ' (1 * ' (' ' *%%%! ' -
' N

Denial of Service

Memory Exhaustion

9 F ' ' (.& ((1
- 9 ' F &
' ((' ' '&& ' + ' '
9)' (
F % C(& & F
(((& & ' (& (
8 ' ' F 3 ' (+
(&

) ' (' & F
(((& ' ' (& ' 9
)' && (& ((' && + '
F)' (& ('

% & (4 (& ' + ' (((
. 1 & & ' J '
' ( )' & ((' + J ' 4 '

J +' ' ' < -
- & (& + '
& ' ' F % & (

)' & (&)' ' ' '
(=<@@ < '
(& ' ' + ' '&& ! '
& /& / ' ! O' O((
) ' ' & ' & (- && ' (
' - ! O' O(( ))' + & '
' ' & B + 9 '
' ' ' - (' (& (
(& ' F

9 ' & (' ' & + (' , ' -
((3 & ' ' - ' J '
Xrealloc Xfree)' (& ' ,
(+' ' + + ((' ((& (
(- , 7 & ' ' -- &
+ ' & (7 ((' ' '
&& ' (' & B +

% ' + ' - ' ((C'
& (? & ' (+' F (
' +

CPU Monopolization

9 ' + ' '
+ ' F)' + & & ('
F & ' ' & (6
F + + '
F 9 ' - ' + ' + (&

) ' ' '
'(' ' ' (& , ' (&
9&& & &
' '(+ ' ' ' ( )' 0
' , C & + & (& &
' C ' && ' ' (&

Chapter 3. Security concerns with specific window attributes

Background-pixmap

```
%          +   + + ' '   -     & C( &           =   .'
    /  -        +   + /1         (        '  +   +   9   -
       +   +     &       +   -       +'    ' &&
  '     +'  ' +   ++  ( &&          ( '   -
+   + + ' A  *(    )'  (  +            (  '  +   +   )'  %
     +   %'      +9       F          '   -     & C( &
          =      (   +   + &               (  '  +
 +            -       +   +                                ReparentWindow MapWin-
dow MapSubwindows ConfigureWindow     CirculateWindow

B  -       +   +                 &&          9
       +   + + '  -          +     )'   +   +   &&
  '          ' +   +    + '   -       +   +

)   (    '   &    (   '                +         -
+'        &      =    *     '          -     +     -
     '   (  ' +   +  '  '    +   J         9      &
 (  &&  &              (   ( '                 '   '
    +  &&       '              -         (         '
'    +          '                '            *(&  (
     '          &    (   '   @  -    ' +   +   -
       '  ' '   &        + + J '     (



    *00<64  0 (        '    C              F     ' +   +   -
           +          (     ' N



    *00<64     '          &     &&         -  N %     '
      (        &      + ' ' +         -     +'  ' +   +
                    (       +   + N
```

ParentRelative and CopyFromParent

```
0     +   +           -    &         '       '(
.         1     &  .% & 8  (     1  '   (          ( ' +   +J
&      )'                  '     )'  +   +                  -
    & C( &       & C( &        ( &  9      '          + '                                  Cre-
ateWindowK                 + '              ChangeWindowAttributes

)'     (     '      J  &                          J    (
 &&  &      0                          (      '
```

& ' - <
& (+ + ' '
. % + +1 ((' ' (
' '

Override-redirect

+ + ' ') '
+ +(9 (& + + ' (
' ' && + J

) & ' ' & (' & .
1 ' (+ +

7 + + (- (& - '
(' & ' + + (('
& + ! & +

Chapter 4. Security concerns with specific requests

) ' & " F (' +
, (9 ' + (& ( )'
(& 3 ' 3
8 + ' ' (+ '/ 4/ ((
(' & ' . 1

+ ' ' ' + + ' (&
+

CreateWindow

9 4 + + ' ' J + +
'

4 + 0& ' + + ' & + '
+ ' '

)' 4 * & 7 + + + + + ' - &
' J + + - 2(& ' + +
' &)' & 0 6 & ' C
' ' & && ' ' ' + J + -
+ ' ' - ' + + &&

4 & * & 7 + + . &
' 1 % (- 0 6
+'

*00<64)' ! & & (& ' + +
. "" "" , "C "1 / ' F + +& &
& F / & 4 +
' + + +' ' + F ' -
! & + % + & +

)' 4 * .& - & C(& & C(& (&
1

4 + C(& % (& %

4 + + ' ((

4 F

9

ChangeWindowAttributes

9 4 ' ' ' J + +

)' 4 ' J + +

' ' 4 +

*00<64)' ! & & ' /' '
= ' + + ' ' + &
' /)' + & (' +
+ ' % ' & ' & + ' ' ' &
' (, ' & & + '
= ' (N

*00<64)' ! & & & F '
6 2@ = & + + 0 (& (
' &

)' 4 * . - & C(& & C(& (&
1

4 C(& % (& %

9

GetWindowAttributes

)' 4 ' ' J + +

)' 4 * .+ +1

' ' 4 +

DestroyWindow, DestroySubwindows

4 ' J + +

)' 4 * .+ +1

' ' 4 +

ChangeSaveSet

9 4 ' J + + & ' +' '
. ' ' J + + + + ' J
+ + 1

4 & ' F ( )' + (
& + + + +

)' 4 * .+ +1

4 +

MapWindow

0& 4 (& + + ' (+ + '
9 F + & (& '

4

& '
+ ' ' & + +)' & ' (
' - + +' - (C &
) (& ' ' ' + & + ' ' (
C &)' + & ' + '
(4

9 + + + ' + + '
* ' & &

*00<64 + - (N 0' ' + +
+ + C (& N

*00<64 (' ' ' ' +
& ' - N

9 + (+ + *

)' (+ ' C 8 * 8 7
6 = @ = 8 * 8 7 + +
- +' + +. 1 ' J & < '
& ' 2
&

*00<64 (' - ' ('
+ +N + & + '
P ' P ' +' ' N

= ' ' ' && (&

)' + + (- (& ( )' ((
' ' (- + + ' +' '
(' & (' + + ' + ' + ' + ' +
+ +

Window Operations

0& & + ! & + ! &0 + + < (& + <
(&0 + + % + % +

9 4 (& ' J + +

)' 4 * .+ + 1

' ' 4 + + +
+' ' + ' 9

GetGeometry

)' 4 ' (' J +

)' 4 * . + 1

' ' 4 + 5 + + + +
+

QueryTree

)' 4 * .+ +1

4 +

)' 4 + + * ' '

4 8 ' ' + + ' & (+ + * '
9 + ' + + 8 ' & + +
' + + '
' + + C ' + +
' & + +

*00<64 + (&& + ' + + (
(+ +. 1 ' + + + ' F + +
' + +N

*00<64 ' ! & . ' & (1
' & + + & & 0 9
0

InternAtom

)' 4 ((')'
(& (' +' '('

4)' ((' B - + + ' (&
((& & ' ' '

4 (' ((

4 F

GetAtomName

)' 4 (((')'
(& (' +' '('

4)' ((' & & ' ' '

ChangeProperty

9 4 ' & & ' J + + ' +
'

)' 4 * .+ +1

' ' 4 +

*00<64 0 F ' + ' & &
' F J + + ' (' N
' ' & & (+ + & % 0
(& + ' + + & & + N

*00<64 ' + + & & + N

4 & & ' ((

4 F

DeleteProperty

4 & & '

)' 4 * .+ +1

' ' 4 +

GetProperty

)' 4 & & '

)' 4 * .+ +1

' ' 4 +

*00<64 ' + + & & N &
+ 4 (' & & &
N

*00<64 ! & ' + & &
4 !O0)9)6 & + + O!7)*8O 9AO *= 7
' + + O!7)*8O 9AO)9 A6)0 ' + + '
O!7)*8O 9AO *= 7 & & O!7)*8O 9AO 6%6* 6 O*=87
+ + + ' & 9 (& & '
' C (

RotateProperties

9 4 & & '

)' 4 * .+ +1

' ' 4 +

ListProperties

)' 4 & & '

)' 4 * .+ +1

' ' 4 +

*00<64 ' + + & & N

SetSelectionOwner

)' 4 0 + '&

4 ' & ' ' + '

' ' 4 ' '
+ 8 ' ' F &

*00<64 ' + ' (' N * ' '
' ' ' N

)' 4 * .+ +1

4 +

GetSelectionOwner

)' 4 ' * ' J + + ' + ' &

4 ' ' ('
+ + * =

*00<64 ' + ' (' N

ConvertSelection

)' 4 ' . ' *%%%!1 +' ' '
(' + +' ' (' ' F

4 (% 0 &
& ' + '
)' ' ' (' '

)' 4 * . F 1

4 +

SendEvent

9 0 6 & + +
' 0 (0 6 + + + + + '
& &) ' & & & + +
+ % 0 6 +
(' ' +

4 ' F ' % !
+' ' (' ! &
& (' ' ' + -

*00<64 + % ! & & ' N

)' 4 * .+ +1

4 +

Keyboard and Pointer Grabs

0& A ? A A ? A B

2)' 4 - ' - &)' +
& ' (- (
& + ' ' & ('
'

4 & + - (- - ('
' ' + +' ' & .0 ! & + 1

)' 4 * . + + 1

4 + %

ChangeActivePointerGrab

)' 4 * . 1

4 %

GrabServer

4 ' - '

4 & + - (- - (

QueryPointer

)' 4 9 & (& & (-
& + + ' + ' ' F

4 ' F J ' ' & ' &
+ + ' (,

)' 4 * .+ +1

4 +

GetMotionEvents

)' 4 & (& ' + '

4 ' + & & ' +
)' (& (' & + ' '
(* + + + (& (

)' 4 * .+ +1

4 +

TranslateCoordinates

)' 4 (' J + + 4 & &
' * ' + +

4 + + + + ' F

)' 4 * . + + + +1

4 +

WarpPointer

9 & (' J + +

4 & & + & & ' (' (
(

' ' 4 ' F J ' ' &
' & + + ' F &

)' 4 * . + + + +1

4 +

SetInputFocus

)' 4 ' F (- + + + ' ' &
.- 1)' (+ ' - - +
+ +

4 & & & (' -

' ' 4 + 0 * & 8 &
' '

*00<64 ' + - ' A 9 * & (
E ' *%%%!

)' 4 * . 1

4 +

GetInputFocus

)' 4 ' & (' * ' J + +

4 + + = ' ' &

QueryKeymap

)' 4 & ' - + ' ' +' ' - &

4, ' ' ' &

Font Requests

0& 7& 8 G 8 @ 8 @ 8 '* G) C 6C

)' 4 (&' ((' + &
' . ' & '1 ' ' '
((' J & ' & +' '
' ' C ' & '

4

! + & & '
)' ' , ' & ' 0 F
' ' ' 0 +
& ' (' +
& ' & ' (

)' 4 * . 1 .G 8 G) C 6C 1

4 8

4 & ' ((.7& 8 1

4 F

CloseFont

4 ' J

4 8

SetFontPath

4 ' ' & ' ' ' '

9 4 ' ' & ' ' ' ' '
C&

' ' 4 & & '
' 8 F

*00<64 ' & & 3 & & '
' + ' - ' & ' &
+ ' ('('
+' + ' K J (' '
'

GetFontPath

)' 4 & ' (' + '

< - + (& ' ((' - -
' & '

' ' 4 & & '
' 8 F

CreatePixmap

)' 4 * . + 1

4 +

4 & C(& ' ((

4 F

FreePixmap

4 ' J & C(&

4 C(&

CreateGC

)' 4 * . + && & (-1

4 + C(& 8

4 A% ' ((

4 F

CopyGC

)' 4 & A% ' J A%

9 4 & A% ' J A%

' ' 4 A%

ChangeGC, SetDashes, SetClipRectangles

9 4 ' ' J A%

)' 4 * . && & (-1 .
%' A% 1

' ' 4 A%

FreeGC

4 ' J A%

4 A%

Drawing Requests

0& % 9 % & 9 % & @ 0 (
9 8 8 8 9 *(
)C I)C $ *( )C I *( )C $

9 4 + ' J +

)' 4 * 4 % 9 + +K % & 9 % & +
+ K ' +

' ' 4 && &

*00<64)' ! & & F +
+ + ' 2

0& 4 + + + (- (+ + '

4 ! & +

GetImage

)' 4 ' (' J +

)' 4 * . + 1

4 +

)' 4 ' (+ + + +' ' (& '
&& + +

4 (' (
+ +

CreateColormap

)' 4 * .+ +1

4 % (&

4 (& + ' ' F '
((

4 F

FreeColormap

4 ' J (&

4 % (&

CopyColormapAndFree

)' 4 * . (&1

4 % (& 5+ (& + +

*00<64 (&& + (&N
.0 (@ * % (& % 9 F 8 %
0 % 0 =(% G % @ -&% 1

4 (& + ' ' F '
((

4F

InstallColormap, UninstallColormap

)' 4 *

4 % (&

4 . 1 (& & & + + (
&

4 ' F & 0 E I ' *%%%! '
. 1 (& ' & ' + +(

*00<64 ' *%%%! + (& ' '
' & + + ' N

ListInstalledColormaps

)' 4 * .+ +1

4 % (&

)' 4 ' * ' J (& (' &

4 (' (&* K ' ' (&
(&

Color Allocation Requests

0& 9 % 9 =(% 9 % % 9 %

9 2 4 ' J (&*
' + J '
7' + 3

)' 4 * . (&1

' ' 4 % (& 5 + (&
+ +

FreeColors

)' 4 * . (&1

4 % (& 5 + (& + +

StoreColors, StoreNamedColor

9 4 ' ' ' J (&

)' 4 * . (&1

' ' 4 % (& 5 + (&
+ +

QueryColors, LookupColor

)' 4 (' ' J (&

)' 4 * . (&1

' ' 4 % (& 5 + (&
+ +

CreateCursor, CreateGlyphCursor

)' 4 * . (- (- 1

4 C(& 8 5 + ' + +

4 ' ((

4 F

FreeCursor

4 ' J

4 %

RecolorCursor

9 4 ' J

)' 4 * . 1

' ' 4 %

QueryBestSize

)' 4 * . + 1

4 +

ListExtensions, QueryExtension

(' C && ' ' ' C
& - (&

4 C + ' + ' +' '
' ( )' F + (C
' (

Keyboard configuration requests

0& %' ? % %' ? ! && 0 !
! &&

9 4 ' ' - & (' + ' '

4 + ' %' ? % & - -
' ' %' ? ! && 0 ! ! && ' ' -
(&& ' ' - (&

' ' 4 ' F &

Keyboard query requests

0& A ? % A ? ! && A ! ! &&

)' 4 - (' + ' '

4)' ((' & & ' ' '

ChangePointerControl, SetPointerMapping

9 4 ' ' & & (' + ' '

4 ' & & (' ' & (
&

' ' 4 ' F &

GetPointerControl, GetPointerMapping

)' 4 & & (' + ' '

4)' ((' & & ' ' '

SetScreenSaver

9 4 ' ' & (' + ' '

4 ' & (' ' +
+

' ' 4 ' F &

GetScreenSaver

)' 4 & (' + ' '

4)' ((' & & ' ' '

ForceScreenSaver

4 & ' ' '
' + - +' '

4 & ' & (

' ' 4 ' F &

ChangeHost

! ' (+' ' ' F
+' ' ' + && (& (&

4 (' (' & (
(' '

9 ' ' % (' ' (' ' ' -
&

' ' 4 9

ListHosts

)' 4 ' & ' +

@ ' - & ' ' 2

' ' 4 '

SetAccessControl

! ' (+' ' ' F
+' ' ' + && (& (&

9 4 ' ' ' ('

+ +' + (
)' (' ' ' - &

' ' 4 9

SetCloseDownMode

4 ' + (( )(&
')' ' '
' ((' '
&& & ? % ' ( )' ' ((
+' ' C' + & +

4 ' F &

KillClient

2 4 - '

4 - ' ' (+ ' + ( )(
& (

4 & 9)(& '
' ' (+ ' + ( )(&

' 4

Clean Requests

7 ' ' ' F ' - +
49 +6 < < B < ? <
? < 0 = 7& B

Chapter 5. Events

)' ' & ' 0 ' J
+ ' ' (' '
+ ' - +' ' ' &
('

KeymapNotify

)' 4 ' ' - +' ' ' '
&)' & ? (&= + +
6 = ' + + ' &

4 , ' ' ' &

Expose

)' 4 +' ' J + + & + 8 (&
+ + + ')' C& +'
' + +

4 ' ' ' -
+ + ' + & (' ((
& & ' ' '

GraphicsExposure

)' 4 +' ' J + + & + 8
% & 9 & ' + +J C &)'
A &' 6C& +' ' + + +

4 6C& & & ' ' '

VisibilityNotify

)' 4 ' & & (' ' '
' +' ' '

4)' (' + & & '
' '

ReparentNotify

)' 4 ' & + + ((' .& ' + +
(1

4 * ' & + + '
+ + ' ' + + C
' + + ' & + +

*00<64 +' ' && (& N

ConfigureNotify

)' 4 ' + +(('

4 = ' + +

*00<64 +' ' && (& N

ConfigureRequest

)' 4 ' + +(('

4 = ' + +

*00<64 +' ' && (& N

SelectionClear

)' 4 ' + + +(('

4 = ' + + +

SelectionRequest

)' 4 ' F + +(('

4B - ' ' + ++ &
((+ - & & '
' ' ')' ((' C&
+ +* (' +

MappingNotify

)' 4 - & ((&& ('

49 (& + ' ' + '
+ ' - & +' ' - '
& & ' ' '

Chapter 6. Errors

)' && ' &

Chapter 7. Future Work

)' C & ' ((- *00<6 '
& & ' QC (& &
2 ' (& (' ' & + ' F

Chapter 8. References

B /8 (+ - A F (+ 0 (0 /) '
9 89 0)0 "" D E * 9 ##

/! 9 & / & '

? ' B @ /0 < *= 7 0>0)6! & 9 8 + /
& ')' !*) 6 % & ##H

' 0 5 /@*= @ *= / 0 ! (# '
9& #I#

' ! - 0 /* % % ((%
! " / &422 & C 2& 2 $ 2C 2 2' & 2*%%%!2 (0 R

0 ' / + 0 (/ &422 & C 2& 2 $ 2C 2 2
' & 2 2& 0 R

) A (9 /)' ' ' 8 + 7 ' 9&&
/ 6F &(% & % (' @) '
& 0 % @ #D2 " ! D ##D