++

Hacking HyperCard Stax FAQ

By mephistopheles ... satan@cafemagnolia.com

The few days it took to write this fiel had been some time after using
hypercard so the scripting might be a little rough.

++

Hacking HyperCard is really rather simple if you have a high command of the HyperTalk language. The truth is, _any_ stack written in HyperCard 2.3.5 or earlier can be hacked. I am writing this text for HC novices because the HyperCard Gurus out there could do all this blindfolded and with their hands tied behind their backs.

The Tools you will need:
HyperCard 2.2 or later (is there? whatever happened to HC3?)
ResEdit or other resource editor

Why hack HyperCard Stacks?
Maybe there is some code or graphix you want to 'borrow' or maybe you just
want to be able to modify it enough to call it your own. Or you just do it
for the kick of it.

What are the basic HC Hacking techniques?
Well, usually the first thing you need to do is get the scripts of stack X (your target)

a sample script that you would put in a button in another stack would be:

```
on mouseUp
        lock errormessages
        lock screen
        push card
        go cd 1 of stack X
        get the script of stack X
        put it into stackXscript
        pop card
        put stackXscript into cd fld "stack script"
        push card
```

```
        go cd 1 of stack X
        get the script of this card
        put it into cardXscript
        pop card
        put cardXscript into cd fld "stack script"
        unlock screen
        unlock errormessages
end mouseup
```

You get the idea. Basically, you go to the other stack, get the scripts and then put them into a field in your stack.
Then you want to look for things like this:

```
on openStack
        set userlevel to 1 --or anything less than 5
        set userlevel(1)
        set cantmodify of this stack to true
        set cantabort of this stack to true
        pass openStack
end openStack
```

Once you find where the stack is locked check if the openstack executes anything before the locking lines. such as

```
on openStack
        global lastUser
        ask "Please log in" with lastUser
        if it = "bob" then
                ask password clear "Password?" with ""
                put it into cd fld "logged in"
        end if

        set userlevel to 1 --or anything less than 5
        set cantmodify of this stack to true
        set cantabort of this stack to true
        pass openStack
end openStack
```

So, before the locking code it will bring up a dialog box that asks for a username and then, if you type "bob" it will ask for a password. Then, what ever you type in that field will be logged into a field.
What do you do to bypass security? as soon as the dialog box pops up, press command-. to stop the script and the stack is yours for the taking.

I used that technique to hack into the popular hypercard game

"Immortal Combat" Before the stack was locked it brought up a dialog that said "Did you read the read-me?" with "OK." I hid command-. and stole all of the graphics and used them to create my own IC hack: Mirror Match.

There are only 2 times stopping the script before the locking code won't work
1) When "set cantabort to true" is set very early in the script, before you have a chance to hit command-.
2) When the author of the stack uses HyperCards built in security (the "protect
stack" menu item under the File menu) is used.

Another thing you might see is something like this

```
--*/ Security /*--
  if the optionkey is down then
    ask password clear "Enter the password:" with ""
    if it is "Secretpassword" then --change for yr stack
      --enter w/o lock--
    else
      systemslock
    end if
  else if the optionkey is not down then
    systemslock
  end if
--*/ End Security /*--
```

This is a back door. It is something only the programmer (or the cracker) knows about that would easily bypass all security.

Another script that is EXTREMELY useful is the auxilary input: script.
Insert this in your Home stack script:

```
on commandKeyDown x
Ê Êif the shiftKey is down then
Ê ÊÊ Ê Êif x=u then
Ê ÊÊ Ê Ê Ê Ê ask "auxiliary input:"
Ê ÊÊ Ê Ê ÊÊÊ do it
ÊÊ ÊÊÊÊÊend if
ÊÊ Ê Êend if
Ê Êpass commandKeyDown
end commandKeyDown
on god
        set userlevel to 5
```

```
        set cantabort of this stack to false
        set cantmodify of this stack to false
        show msg
end god
```

obviously, this script brings up an ask dialog box when you type command-shift-u. ÊType what you want to execute and press OK.Some commands you would want to throw at it are:

```
set userlevel to 5 --god mode
set cantabort to false --means you can press command-. to stop scripts
set cantmodify to false --means you can modify the stack
```

or you could just type god (god script above)

The only times the auxiliary input wont work is when they have the following script in their stack:

```
on commandkeydown x
        --do nothing
        --this blocks all commandkeydown messages from reaching the home staq.
end commandkeydown
```

or if they have HC's built-in security enabled.

How do I bypass HyperCard's built-in security?

First look under the file menu. If you don't see a menu item "Protect stack" then let go, hold down the command key and look under File again. Then select "Protect Stack" and you will see one of two things.

1) an ask dialog box asking for a password
2) the protect stack dialog box. That means the staqs author was stupid enough not to set a password. Yahoo!

If you see the protect stack dialog box uncheck all of the check boxes and set the user level to Scripting. That stack is cracked!

If you are asked for a password, you may as well hit cancel unless you think you know the password.
Then, run the following script. WARNING: DONT RUN THE FOLLOWING SCRIPT ON A STACK THE IS SET TO PRIVATE ACCESS! IT COULD DAMAGE

THE STACK. But if you can get into a stack without having to type in a password, you can try it.

```
on mouseUp
  put the long name of this stack into stackname
  answer "CAUTION: This script could damage the stack.  Make sure
you have a copy." with "Cancel" or "Continue"
  if it is "Cancel" then exit mouseUp
  answer file "Select the stack to deprotect:" of type stack
  if it is empty then exit mouseUp
  put it into longStack
  set cursor to busy
  set the itemDelimiter to colon
  put last item of longStack into stackName
  set the itemDelimiter to comma
  set lockMessages to true
  deprotect longStack
  if the result is empty then
    set cursor to busy
    lock screen
    go stack stackName
    set cantModify of this stack to false
    set cantDelete of this stack to false
    set cantPeek of this stack to false
    set cantAbort of this stack to false
    get the userLevel
    set the userLevel to 5
    go to card 3 of stackname
    unlock screen
    answer "Stack now deprotected!" with "OK"
  else
    if the result is -49 then
      answer "That file is open by another application"
    else
      if the result is -44 then
        answer "The disk is locked.  Please move to a unlocked
volume and try again."
      else
        answer "Failed: unexpected file system error: " & the
result with "OK"
      end if
    end if
  end if
  set lockMessages to false
end mouseUp
```

notice it calls an xternal command called deprotect. That XCMD is in this text file. So open up this file with ResEdit, copy the XCMD resource and paste it into your home stack. This script I...uh....borrowed from a stack called 'deprotect stack' that you should be able to find in the INFO-MAC archive.

There is also another XCMD&XFCN bundle in the fiel called "unprotect" and "filename." which you should use on a stack that does have "Private Access" enabled. To use unprotect, copy the unprotect XCMD and filename XFCN and paste them into your home stack. Then run the following script:

```
on mouseUp
  put filename("STAK") into fname
  if fname is empty then exit mouseUp
  unprotect fname
  if the result is empty
  then answer "Deprotect Successful" with "OK"
  else if the result is -49
  then answer "Sorry, that file is busy."
  else if the result is -44
  then answer "Sorry, the disk is locked."
  else answer "Failed: unexpected file system error: " & the
result with "OK"
end mouseUp
```

Are there any other Stack hacking techniques?

The one other method only works if there is an xcmd or xfcn in the stack. (Note: this may not work due to scripting anomalities and/or different versions of hc)

1. Delete the XCMD or XFCN rsrc
2. Open the stack and fiddle around with it. *Sometimes* you will get an error about that XCMD or XFCN and the stack will pop open by itself.

I only read about this in comp.sys.mac.hypercard a while back and have never tried it.

++
Have fun...
Some of these external rsrcs and scripts are from Flux's Devils Workshop (which is a great hc hacking stack) and Deprotect.
Sorry if i offended anyone butÉ uhÉ thats life.