Data Seepage

Robert Graham – Founder & CEO
David Maynor – Founder & CTO
What is Data Seepage?

• Don’t Confuse it with Data Leakage.

• Data Leakage is when information you care about is accidentally revealed.
  – This can be due to programming errors, improper handling of sensitive information, or malicious internal threats.
What is Data Seepage?

• What is Data Seepage then?
  – Information that is broadcast or available via simple inquiry or spoofing that may not by itself seem critical but become more important as pieces of a larger puzzle.
What is Data Seepage?

- Think about what your laptop does when it starts up.
  - Programs set to autostart
  - Looking for certain resources like intranet homepage and shared drives
  - Email clients
  - Instant messaging clients
The military is well aware of this.

A military intelligence term meaning “essential elements of friendly information”

- Key questions likely to be asked by adversary officials and intelligence systems about specific friendly intentions, capabilities, and activities, so they can obtain answers critical to their operational effectiveness.

- http://usmilitary.about.com/od/glossarytermse/g/eefi.htm
Him: When can I see you again?
Her: How about next week? My boss, the director of the NSA has a trip he is going on he can’t even tell me about. It makes me so mad, how am I suppose to help coordinate things if I don’t even know where he is going. He did ask me to buy a lot of suntan lotion though…
Him: Excuse me, I have to make a phone call.....to my sister...about...trees.
Her: Ok hurry back, I am going to order another drink.
Him: The director of the NSA is going somewhere that requires a lot of suntan lotion.

Terrorist: We have gotten word that a major US Intelligence officer will be visiting Baghdad soon. Director of NSA == US Intelligence officer, therefore I deduce that the Director of the NSA will be visiting Iraq next week.

Him: Why did you say “equal equal” out loud? lol

Terrorist: It makes me seem creepier.
EEFI doesn’t apply to you?

- Think of things the movements of your CEO, sales staff, or even engineers can tell a diligent observer about your business.
  - Repeated trips to a competitors headquarters?
  - Sales guys cancelling dates near end of month or end of quarter.
  - Engineers cars in parking lots as a ship date comes and goes.
Him: When can I see you again?
Her: How about next week? My boss, the CEO, is out all next week on some sort of secret trip. It's his third time going to Redmond this month and he hasn't even brought me a present, but I have to be on call at all hours to coordinate a conference call with all the C level execs.
Him: Excuse me, I have to make a phone call.....to my brother...about...a playdate for our dogs...
Her: That's so sweet, Hurry back, I am ordering more drinks.
Him: Hey, something's up with XYZsoft.

Stock Broker: My friend on a project at Microsoft just got reassigned to a different project. He said the would solve the problem a different way. Microsoft must be buying XYZsoft.

Him: Has anyone told you that for a stock broker you sure look like a terrorist?

Stock Broker: I use to be, taking advantage of your capitalist systems pays better though.

Him: I am strangely comfortable with that.
More EEFI examples

• The Pentagon ordering a lot of delivery food.
• Warehouses of business shipping items like crazy as end of quarter approaches.
• A small company placing an order for 50 new workstations or placing an order to for more VoIP quality circuits to locations they don’t have offices.
Data Seepage…

- So how does this apply to computers?
- You laptop, PDA, even mobile phone will give up information that may not seem important but combined with other info can paint a picture for malicious intruders.
Data seeps via the network…

• Wifi packets
• DHCP Broadcast
• NetBIOS/SMB Broadcast
• DNS/Bonjour Requests
• Probe Requests
  – [http://www.theta44.org/software/karma.READ ME](http://www.theta44.org/software/karma.READ ME)
  – When a wifi enabled laptop starts up it will look for a list of “known networks” or networks it has connected to before.
  – This list can be used to determine where the laptop has been used.
• You can offer up an address and pretend to be whatever server you are looking for.
• Look at the Karma project.
  – Respond to WiFi “probe”
  – Respond with DHCP address
  – Respond to ARPs
  – Respond to NetBIOS queries
  – Respond to SMB/DCE-RPC connections
  – Respond to DNS queries
  – Respond to SMTP connections
NetBIOS/SMB Broadcast

- WKSSVC announcements
- AD activity
- Attempting to connect to shared drives
- Printers
DNS Requests

• Almost all internet activity requires a DNS lookup
  – Connecting to intranet sites
  – Connecting to mail servers
  – Almost any other application starting up
    • IM apps
    • VoIP apps
    • Games (yes even poker games)
Other Protocols

- Bonjour
  - Very chatty about who you are
- Skype
  - It always finds a way
- Security tools
  - They are always update hungry
- OS
  - They love the updates as well
- AIM will update you to all you buddies status.
  - This tells an eavesdropper who is on your buddy list.
What does all this mean?

• Lets look at the information that can be gathered:
  
  A machine with the Mac Address of 00-18-f3-57-24BD belongs to John Smith.
  This laptop has connected to wifi access point at Hartsfield airport, Heathrow, SeaTac, and various T-Mobile spots, and ABCsoft and XYZsoft.
  John has the AIM name “PrschDude9” and has XYZsoft1 on his buddy list.
  He uses a popclient to check his personal email and his passwd is porsche911turbo.
  John works for ABCsoft because his browsers attempts to go to internal.abcsoft.com when it first starts up.
  It also attempts to connect to \internal.abcsoft.com\sales and \internal.abcsoft.com\public on start up.
  He has a myspace account where he had pics of the last company party.
Applying information

• So what can you determine about this if you know ABCsoft and XYZsoft are bitter rivals?
  – **Sounds like a merger or buyout.**
• Since you know Johns pop password you can try it against ABCsoft’s webmail client, he might use the same password.
• Social Engineering – “Hey wasn’t that a horrible shirt John was wearing at the last company party…run this program to update your accounting software.”
• You know portions of the internal layout of the ABCsoft intranet.
  – **Make trojans and client side exploits more efficient because you have a target to attack.**
THEORY-CRAFT
Process of collecting seaped information

- **Identity**
  - Tell me everything knowable about the subject

- **Opportunity**
  - What can I do with the subject

- **Baconizing**
  - Create a graph of who contacts whom
    - Which servers they connect to
    - Who they have in their buddy lists
    - Who they send e-mail to
WEBSITES
PACKETS
<table>
<thead>
<tr>
<th>Offset</th>
<th>Value</th>
<th>Description</th>
<th>AES Key</th>
<th>EEA Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000</td>
<td>08 01 2c 00 00 15 c7 a4 d5 30 00 17 f2 41 31 6d</td>
<td>data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0010</td>
<td>01 00 5e 00 00 fb e0 06 aa aa 03 00 00 00 08 00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0020</td>
<td>45 18 01 dc 36 19 00 00 ff 11 99 01 45 5e c4 84</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0030</td>
<td>e0 00 00 fb 14 e9 14 e9 01 c8 05 08 00 00 84 00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0040</td>
<td>00 00 00 09 00 00 00 00 00 2d 44 61 76 69 64 20 4d</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0050</td>
<td>61 79 6e 6f 72 e2 80 99 73 20 43 6f 6d 70 75 74</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0060</td>
<td>65 72 20 5b 30 30 3a 31 36 3a 63 62 3a 64 32 3a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0070</td>
<td>30 37 3a 61 61 5d oc 5f 77 6f 72 6b 73 74 61 74</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0080</td>
<td>69 6f 6e 04 5f 74 63 70 05 6c 6f 63 61 6c 00 00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0090</td>
<td>21 80 01 00 00 00 00 00 00 00 00 00 00 00 00 00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00a0</td>
<td>64 61 76 69 64 2d 6d 61 79 6e 6f 72 73 2d 63 6f</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00b0</td>
<td>6d 70 75 74 65 65 72 2d 33 c0 4c c0 c0 0c 10 80 01</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00c0</td>
<td>00 00 11 94 00 01 00 09 5f 73 65 72 76 69 63 65</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00d0</td>
<td>73 07 5f 64 6e 73 2d 73 64 04 5f 75 64 70 c0 4c</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00e0</td>
<td>00 0c 00 01 00 00 11 94 00 02 c0 0c c0 0c 0c 0c 80 01</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>00f0</td>
<td>00 01 00 00 11 94 00 02 c0 0c c0 0c 0c 0c 80 01</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0100</td>
<td>00 00 00 07 80 00 10 fe 80 00 00 00 00 00 00 02 17</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0110</td>
<td>f2 ff fe 41 31 6d 01 44 01 36 01 31 01 33 01 31</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0120</td>
<td>01 34 01 45 01 46 01 46 01 46 01 32 01 30 01 30</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0130</td>
<td>01 31 01 32 30 30 30 30 30 30 30 30 30 30 30 30</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0140</td>
<td>01 30 01 30 30 30 30 30 30 30 30 30 30 30 30 30</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0150</td>
<td>01 30 01 30 30 30 30 30 30 30 30 30 30 30 30 30</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0160</td>
<td>00 0c 80 01 00 00 00 00 00 00 00 00 00 00 00 00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0170</td>
<td>80 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0180</td>
<td>31 2c 31 44 4d 61 63 20 4f 53 20 58 20 31 30 2e</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0190</td>
<td>34 2e 38 20 28 38 4c 32 31 32 37 29 2c 20 6d 44</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01a0</td>
<td>4e 53 52 65 73 70 67 69 63 70 30 30 30 30 30 30</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01b0</td>
<td>32 20 28 41 25 75 67 20 32 35 20 32 30 30 36 30</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01c0</td>
<td>34 3a 35 30 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a 3a</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01d0</td>
<td>00 78 00 04 45 5e c4 84 03 31 33 32 03 31 39 36</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01e0</td>
<td>02 39 34 02 36 39 07 69 6e 2d 61 64 64 72 c1 1e</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>01f0</td>
<td>00 0c 80 01 00 00 00 00 78 00 02 c0 63</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transaction ID:</td>
<td>0x0000</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Questions:</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Answer RRs:</td>
<td>9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Authority RRs:</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Additional RRs:</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Frame 65 (508 bytes on wire, 508 bytes captured)**
- **IEEE 802.11**
- **Logical-Link Control**
- **Internet Protocol, Src: 69.94.196.132 (69.94.196.132), Dst: 224.0.0.251 (224.0.0.251)**
- **User Datagram Protocol, Src Port: 5353 (5353), Dst Port: 5353 (5353)**
- **Domain Name System (response)**
  - Flags: 0x8400 (Standard query response, No error)
  - Questions: 0
  - Answer RRs: 9
  - Authority RRs: 0
  - Additional RRs: 0

  - **Answers**
    - David Maynor\342\200\231s Computer [00:16:cb:d2:07:aa]._workstation._tcp.local: type SRV, class FLUSH, pr
    - David Maynor\342\200\231s Computer [00:16:cb:d2:07:aa]._workstation._tcp.local: type TXT, class FLUSH
    - _services._dns-sd._udp.local: type PTR, class IN, _workstation._tcp.local
    - _workstation._tcp.local: type PTR, class IN, David Maynor\342\200\231s Computer [00:16:cb:d2:07:aa]._work
    - david-maynors-computer-3.local: type AAAA, class FLUSH, addr fe80::217:f2ff:fe41:316d
    - D.6.1.3.1.4.E.F.F.F.2.F.7.1.2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.E.F.1p6.arpa: type PTR, class FLUSH, david-ma
    - david-maynors-computer-3.local: type HINFO, class FLUSH, CPU MacBook1,1, OS Mac OS 10.4.8 (8L2127), mDNS
    - david-maynors-computer-3.local: type A, class FLUSH, addr 69.94.196.132
    - 132.196.94.69.in-addr.arpa: type PTR, class FLUSH, david-maynors-computer-3.local
Frame 125 (776 bytes on wire, 776 bytes captured)
Ethernet II, Src: Dell_6b:1b:cb (00:13:72:6b:1b:cb), Dst: JetwayIn_77:1b:8a (00:30:18:77:1b:8a)
Internet Protocol, Src: 192.168.2.30 (192.168.2.30), Dst: 216.73.86.52 (216.73.86.52)
Transmission Control Protocol, Src Port: 4046 (4046), Dst Port: http (80), Seq: 1, Ack: 1, Len: 722

Hypertext Transfer Protocol
GET /adi/N2992.Yahoo__/B2112371.8;dcadv=1281487;sz=728x90;dcdept=rcl;click=http://us.ard.yahoo.com/SIG
Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/x-font
Referer: http://my.yahoo.com/
Accept-Language: en-ca\r\nUA-CPU: x86\r\nAccept-Encoding: gzip, deflate\r\nUser-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; .NET CLR 1.1.4322; .NET CLR 2.0.50727)
Host: ad.doubleclick.net\r\nConnection: Keep-Alive\r\nCookie: id=800000a9c7b526e\r\n\r\n
DEMOS
FERRET – Data seapage monitor

• Like password sniffer, but sniffs more than just passwords
• Like intrusion-detection, but sniffs legitimate operations rather than intrusions
• Protocols: DHCP, SNMP, DNS, HTTP, AIM, MSN-MSGR, Yahoo IM, …
• Ferret Viewer: allows you to browse the data easier
Example: Bonjour

- Lists services on a machine
- Tells you which ones you can attack
Example: iTunes server

- iTunes uses Bonjour to advertise it’s existence
- This tells you that you can connect to that iTunes server and download all the music with no password
Example: CUPS

- Tells you about printers available
- Tells you about drivers that may have bugs
  - Printer driver bugs are common, which is why Microsoft moved them to user-mode drivers
- Tells you about vulnerable printers
- Maps out the network
Example: ID

- Tells you about the system, pulling interesting identification info from various protocols.
Example: ID (more)
Example: ID (more)
Example: MSN-MSGR

- Builds ‘friends’ list
- Grabs user of machine
Example: WiFi probes

- A list of every place the person has been
Example: e-mail
• Finding the 6-degrees of Kevin Bacon
- Current build of the software
How to protect?

• Personal firewalls?
  – Don’t allow any traffic unless you are on a trusted network.
  – Users will just blindly click through them.

• Corporate Policies…
  – Do these ever really work?

• The best solution for this is to be aware of the danger.
  – Everyone really doesn’t need to work from a coffee shop.