(TS//SI//REL) VPN SigDev Basics

S31244 - OTTERCREEK
Overall Classification:

TOP SECRET/COMINT/REL TO USA, FVEY
(U) What is a VPN?

- (U) A Virtual Private Network or VPN is a computer network that uses encryption to securely connect remote users/networks over an otherwise insecure network, usually the public internet.

- (U) Common Types:
  - PPTP, IPSec, SSL

- (U) Public Key Encryption
  - Diffie-Hellman, RSA
(U) PPTP

- (U) Microsoft Point-to-Point Tunneling Protocol
- (U) Control Channel
  - TCP port 1723
- (U) Data Channel
  - GRE-Next Protocol 47
- (U) RFC 2637, RFC 3078
(U) IPSec

- (U) Authentication
  - Pre-shared key (PSK) or Public key certificates
- (U) ISAKMP/IKE packets are used for key exchange and to establish the secure connection
  - UDP port 500, 4500; TCP port 500
- (U) ESP packets contain the encrypted data
  - IP Next Protocol 50; UDP port 500
- (U) RFC2402, RFC2406, RFC2409, RFC4306, RFC2408
(U) IPSec in a nutshell
(U) SSL/TLS

· (U) Secure Sockets Layer/Transport Layer Security
· (U) WARNING! e-commerce = tons of uninteresting SSL traffic
· (U) Common ports: TCP ports 443, 995
· (U) RFC2246, RFC4346, RFC5246
(U) SSL in a nutshell

(U) SSL Exchange
1. Client connects to server
2. Server sends cert to client
3. Client validates cert
4. Key exchange
5. Pass encrypted material
(TS//SI//REL) Who works VPNs?

- (TS//SI//REL) VPN Working Group (go vpn)
  - S2, SSG, CES (OTTERCREEK, NSP, S31322, S3117, S3112), TAO, etc.
- (TS//SI//REL) Alias: [REDACTED]
  (Board alias: [REDACTED])
- (TS//SI//REL) Meets every other Thursday at 1300
(TS//SI/REL) Who works VPNs?

Know your target
- S2
- NAC
- OTTERCREEK

Find Target VPNs

Gain Access
- S2 (if tasking needed)
- S3112
- TAO
- OTTERCREEK

Decrypt
- S3117 + S3142
- OTTERCREEK
- NSP
- S313

Determine Intel Value

Check and Report
- S2
(TS//SI//REL) So you think your target is using a VPN...
(TS//SI//REL) SigDev Tools

<table>
<thead>
<tr>
<th>(TS//REL) VPN Specific</th>
<th>(TS//REL) Also useful</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BLEAKINQUIRY</strong></td>
<td><strong>MARINA</strong></td>
</tr>
<tr>
<td><strong>DISCOROUTE</strong></td>
<td><strong>MASTERSHAKE</strong></td>
</tr>
<tr>
<td><strong>TOYGRIPPE</strong></td>
<td><strong>NKB</strong></td>
</tr>
<tr>
<td></td>
<td><strong>PINWALE</strong></td>
</tr>
<tr>
<td></td>
<td><strong>RENOIR</strong></td>
</tr>
<tr>
<td></td>
<td><strong>TREASUREMAP</strong></td>
</tr>
<tr>
<td></td>
<td><strong>TUNINGFORK</strong></td>
</tr>
<tr>
<td></td>
<td><strong>XKEYSCORE</strong></td>
</tr>
</tbody>
</table>
(TS//SI//REL) TOYGRIPPE

- (TS//SI//REL) Database of VPN metadata
  - IPSec, PPTP, ViPNet
**TYG Tips:**

- Populate “Display Fields”
- For both directions between 2 Ips, use **AND**
- For either direction connecting to a single IP, put IP in both “Source” and “Destination” boxes, and use **OR**
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>Authority</th>
<th>Status</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011-04-02</td>
<td>09:13</td>
<td></td>
<td>DE</td>
<td>pre-shared key</td>
</tr>
<tr>
<td>2011-04-02</td>
<td>10:18</td>
<td></td>
<td>DE</td>
<td>pre-shared key</td>
</tr>
<tr>
<td>2011-04-02</td>
<td>11:31</td>
<td></td>
<td>DE</td>
<td>pre-shared key</td>
</tr>
<tr>
<td>2011-04-02</td>
<td>12:22</td>
<td></td>
<td>DE</td>
<td>pre-shared key</td>
</tr>
<tr>
<td>2011-04-02</td>
<td>13:00</td>
<td></td>
<td>DE</td>
<td>pre-shared key</td>
</tr>
<tr>
<td>2011-04-02</td>
<td>17:37</td>
<td></td>
<td>DE</td>
<td>pre-shared key</td>
</tr>
<tr>
<td>2011-04-02</td>
<td>17:51</td>
<td></td>
<td>DE</td>
<td>pre-shared key</td>
</tr>
<tr>
<td>2011-04-01</td>
<td>00:22</td>
<td></td>
<td>DE</td>
<td>pre-shared key</td>
</tr>
<tr>
<td>2011-04-01</td>
<td>05:40</td>
<td></td>
<td>DE</td>
<td>pre-shared key</td>
</tr>
<tr>
<td>2011-04-01</td>
<td>07:56</td>
<td></td>
<td>DE</td>
<td>pre-shared key</td>
</tr>
<tr>
<td>2011-04-01</td>
<td>08:20</td>
<td></td>
<td>DE</td>
<td>pre-shared key</td>
</tr>
<tr>
<td>2011-04-01</td>
<td>09:22</td>
<td></td>
<td>DE</td>
<td>pre-shared key</td>
</tr>
<tr>
<td>2011-04-01</td>
<td>10:16</td>
<td></td>
<td>DE</td>
<td>pre-shared key</td>
</tr>
<tr>
<td>2011-04-01</td>
<td>11:50</td>
<td></td>
<td>DE</td>
<td>pre-shared key</td>
</tr>
<tr>
<td>2011-04-01</td>
<td>12:34</td>
<td></td>
<td>DE</td>
<td>pre-shared key</td>
</tr>
<tr>
<td>2011-04-01</td>
<td>13:23</td>
<td></td>
<td>DE</td>
<td>pre-shared key</td>
</tr>
<tr>
<td>2011-04-01</td>
<td>13:32</td>
<td></td>
<td>DE</td>
<td>pre-shared key</td>
</tr>
<tr>
<td>2011-04-01</td>
<td>13:45</td>
<td></td>
<td>DE</td>
<td>pre-shared key</td>
</tr>
<tr>
<td>2011-04-01</td>
<td>15:52</td>
<td></td>
<td>DE</td>
<td>pre-shared key</td>
</tr>
<tr>
<td>2011-04-01</td>
<td>15:07</td>
<td></td>
<td>DE</td>
<td>pre-shared key</td>
</tr>
<tr>
<td>2011-04-01</td>
<td>16:10</td>
<td></td>
<td>DE</td>
<td>pre-shared key</td>
</tr>
<tr>
<td>2011-04-01</td>
<td>17:48</td>
<td></td>
<td>DE</td>
<td>pre-shared key</td>
</tr>
<tr>
<td>2011-04-01</td>
<td>19:35</td>
<td></td>
<td>DE</td>
<td>pre-shared key</td>
</tr>
<tr>
<td>2011-04-01</td>
<td>00:01</td>
<td></td>
<td>IR</td>
<td>pre-shared key</td>
</tr>
<tr>
<td>2011-04-01</td>
<td>00:41</td>
<td></td>
<td>IR</td>
<td>pre-shared key</td>
</tr>
<tr>
<td>2011-04-01</td>
<td>01:50</td>
<td></td>
<td>IR</td>
<td>pre-shared key</td>
</tr>
<tr>
<td>2011-04-01</td>
<td>01:45</td>
<td></td>
<td>IR</td>
<td>pre-shared key</td>
</tr>
</tbody>
</table>

(U) Export results to excel or text doc for easier sorting.
(TS//SI//REL) XKEYSCORE

(TS//REL) Fingerprints
- IPSec
  - vpn/esp
  - vpn/isakmp
- PPTP
  - vpn/pptp*
- SSL
  - network_encyption/ssl

(TS//REL) Search Forms
- Start with FULL DNI
  - vpn/*
  - network_encyption/*
- IPSec
  - IKE Parser
- SSL
  - SSL Parser
For initial searches, you may want to leave this blank to see all of the different kinds of traffic are found on the IP pair.
(TS//SI//REL) PINWALE

- (TS//SI//REL) Both VPN traffic and Sys Admins passing information about VPN setup

- (TS//SI//REL) IP addresses and port numbers (ex. AP 00500) ***Document Zone = C2C

(TS//SI//REL) DISCOROUTE

- (TS//SI//REL) Router configuration data
  - From passive and active collection
  - Key terms to search for within configs:
    - ‘crypto map’, ‘isakmp’, ‘ipsec’, ‘pre-shared-key’
<table>
<thead>
<tr>
<th>Name</th>
<th>Model</th>
<th>DCX</th>
<th>Vendor</th>
<th>Sigal</th>
<th>Case</th>
<th>Manual</th>
<th>KIS Image</th>
<th>Source IP</th>
<th>S Country S City</th>
<th>Session</th>
<th>Quiet</th>
<th>SPort</th>
<th>DPoort</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>FW_MX</td>
<td>200901.17</td>
<td>200902.17</td>
<td>Huawei</td>
<td>USL-1011</td>
<td>MROAQ</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FW_SMK</td>
<td>200904.12</td>
<td>200904.12</td>
<td>Huawei</td>
<td>USL-1011</td>
<td>MROAQ</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>FW_SMK</td>
<td>200904.13</td>
<td>200904.13</td>
<td>Huawei</td>
<td>USL-1011</td>
<td>MROAQ</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AS-VPN</td>
<td>200901.10</td>
<td>200901.10</td>
<td>Huawei</td>
<td>USL-750</td>
<td>SCZVDR-00003</td>
<td>952</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AS-VPN</td>
<td>200902.15</td>
<td>200902.15</td>
<td>Huawei</td>
<td>USL-750</td>
<td>SCZVDR-00003</td>
<td>2823</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AS-VPN</td>
<td>200902.17</td>
<td>200902.17</td>
<td>Huawei</td>
<td>USL-750</td>
<td>SCZVDR-00003</td>
<td>1077</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AS-VPN</td>
<td>200905.01</td>
<td>200905.01</td>
<td>Huawei</td>
<td>USL-750</td>
<td>SCZVDR-00003</td>
<td>1387</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>AS-VPN</td>
<td>200906.01</td>
<td>200906.01</td>
<td>Huawei</td>
<td>USL-750</td>
<td>SCZVDR-00003</td>
<td>1387</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Password cipher 10, [114, 114, 102, 102]!
Service-type help terminal
level 3, 1...

The peer peer_id
exchange-mode aggressive
pre-shared key KeyTubes AS
id type name
remote address
not traversal
peer multi-subnet 1, v...
(U) Others

- (TS//REL) NKB
- (TS//REL) TUNINGFORK
- (TS//REL) TREASUREMAP
- (TS//REL) RENOIR
- (TS//REL) MASTERSHAKE
- (TS//REL) ROADBED
- (TS//REL) BLEAKINQUIRY
(TS//SI//REL) Basic VPN rules of thumb

- Check TOYGRIPPE and XKS
  - Look for paired traffic
- For IPSec, check sys admin chatter for PSK (DISCOROUTE; PINWALE; MARINA)
- Share your data with OTTERCREEK for vulnerability assessment (XKEYSCORE or DROPBOX)
- Submit tasking

- Look in DISCOROUTE
- Query Sys Admins in PINWALE and MARINA
- Check your targets TAO projects

EITHER WAY, JOIN THE VPN WORKING GROUP FOR ALL OF YOUR VPN SIGDEV NEEDS
(U//FOUO) Useful Links

- (TS//SI//REL) VPN Working Group (go vpn)
- (TS//SI//REL) OTTERCREEK (go VPN XFT)
  - VPNXFT DROPBOX
- (TS//SI//REL) Network Security Products (go NSP)
(U) Questions?

OTTERCREEK