PROFILING SSL AND ATTRIBUTING PRIVATE NETWORKS

An introduction to FLYING PIG and HUSH PUPPY

ICTR - Network Exploitation
GCHQ
Outline

- Two separate prototypes – FLYING PIG and HUSH PUPPY
- Both are cloud analytics which work on bulk unselected data
- FLYING PIG is a knowledge base for investigating TLS/SSL traffic
- HUSH PUPPY is a tool for attributing private network traffic
FLYING PIG - TLS/SSL Background

- TLS/SSL (Transport Layer Security / Secure Sockets Layer) provides encrypted communication over the internet
- Simple TLS/SSL handshake:
Motivations for FLYING PIG

- More and more services used by GCHQ targets are moving to TLS/SSL to increase user confidence, e.g. Hotmail, Yahoo, Gmail, etc.

- Terrorists and cyber criminals are common users of TLS/SSL to hide their comms (not necessarily using the big providers).

- A TLS/SSL knowledge base could provide a means to extract as much information from the unencrypted traffic as possible.
FLYING PIG implementation

- Federated QFD approach
  - Multiple separate cloud analytics, each of which produce a QFD (Query Focussed Dataset).
  - Analytics are run once a week, on approximately 20 billion events.
  - A single query in the web interface results in calls to multiple QFDs, which are returned to the user in separate panels.
  - Results in:
    (a) fast queries,
    (b) easy-to-maintain modular code, and importantly
    (c) easy to add future TLS/SSL QFDs.
Query by certificate metadata

Server certificate fields to search within:
- Subject common name
- Subject organisation name
- Issuer common name
- Issuer organisation name
- RSA modulus

**Certificate field search:** %mail.ru

### All HTTP requests matching your query

<table>
<thead>
<tr>
<th>Server IP</th>
<th>Host name</th>
<th>First seen</th>
<th>Last seen</th>
<th>Count w/o 25th Nov</th>
<th>Count all time</th>
</tr>
</thead>
<tbody>
<tr>
<td>184.105</td>
<td>swa.mail.ru</td>
<td>2011-10-13 16:05:53:00</td>
<td>2011-11-25 21:11:59:00</td>
<td>609863</td>
<td>42647034</td>
</tr>
<tr>
<td>194.194</td>
<td>swa.mail1.ru</td>
<td>2011-10-13 17:29:18:00</td>
<td>2011-11-25 21:11:59:00</td>
<td>6073183</td>
<td>36295441</td>
</tr>
<tr>
<td>134.201</td>
<td>fc.edn.dfd.bi.a1.top.mail.ru</td>
<td>2011-10-13 21:43:10:00</td>
<td>2011-11-25 21:10:49:00</td>
<td>4049743</td>
<td>19396920</td>
</tr>
<tr>
<td>135.13</td>
<td>top5.mail.ru</td>
<td>2011-10-14 20:00:00:00</td>
<td>2011-11-25 21:12:05:00</td>
<td>3008868</td>
<td>14168963</td>
</tr>
<tr>
<td>135.12</td>
<td>top3.mail.ru</td>
<td>2011-10-14 20:00:00:00</td>
<td>2011-11-25 21:10:40:00</td>
<td>2409950</td>
<td>123066955</td>
</tr>
</tbody>
</table>

### All certificates matching your query

#### Tip 1: Right click on a row to find all server IPs that serve that certificate
#### Tip 2: Click on the disk icon in the title bar to download data in CSV format
#### Tip 3: Double-click on a field to enable copy and paste
#### Tip 4: Change displayed columns (Basic is default; Advanced adds RSA Modulus and richer suite distribution columns)

<table>
<thead>
<tr>
<th>Server IP</th>
<th>Cert count w/o 25th Nov</th>
<th>Cert count all time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>177.1</td>
<td>333952</td>
<td>1052618</td>
</tr>
<tr>
<td>191.213</td>
<td>330212</td>
<td>1308617</td>
</tr>
<tr>
<td>184.16</td>
<td>308590</td>
<td>2466916</td>
</tr>
<tr>
<td>184.17</td>
<td>297292</td>
<td>2226233</td>
</tr>
<tr>
<td>184.15</td>
<td>294437</td>
<td>2305012</td>
</tr>
<tr>
<td>189.160</td>
<td>1684415</td>
<td>650307</td>
</tr>
<tr>
<td>184.74</td>
<td>112557</td>
<td>536032</td>
</tr>
<tr>
<td>184.75</td>
<td>112574</td>
<td>536031</td>
</tr>
<tr>
<td>184.76</td>
<td>110325</td>
<td>690993</td>
</tr>
<tr>
<td>135.95</td>
<td>3777</td>
<td>6023</td>
</tr>
<tr>
<td>135.56</td>
<td>3740</td>
<td>7358</td>
</tr>
<tr>
<td>134.151</td>
<td>3564</td>
<td>8408</td>
</tr>
<tr>
<td>135.121</td>
<td>2532</td>
<td>4807</td>
</tr>
<tr>
<td>136.43</td>
<td>2523</td>
<td>9256</td>
</tr>
<tr>
<td>134.98</td>
<td>2360</td>
<td>9165</td>
</tr>
<tr>
<td>179.69</td>
<td>2277</td>
<td>7620</td>
</tr>
<tr>
<td>170.00</td>
<td>2051</td>
<td>7320</td>
</tr>
<tr>
<td>136.84</td>
<td>1981</td>
<td>8442</td>
</tr>
</tbody>
</table>
Query by server IP

SSL Traffic stats:
- For week ending 2011-12-23:
  - No unique clients = 104317
  - % client-server IP with traffic seen in both directions = 11.7%.

SSL Certificates seen on this IP:
- Average pattern of life for a client (seeded around SSL events to this server):
  - Filter by min. % occurrences of event:

Tip 1: Right click on a certificate to explore it further!

Server IP-specific panels:
- SSL Server certificates seen on this IP
- SSL Pattern of life
- HTTP requests to this IP
- Top 100 SSL clients

Top 10 SSL client geos
- Overall
- Paired (approximate)

Top 10 SSL server ports
- Overall
- Paired (approximate)

Top 10 SSL case notations
- Overall
- Paired (approximate)

Top 10 SSL client geos:
- Overall
- Paired (approximate)

Top 10 SSL server ports:
- Overall
- Paired (approximate)

Top 10 SSL case notations:
- Overall
- Paired (approximate)
# Query by server IP

## General IP info
- **Top 10 SSL client geos**
- **Top 10 SSL server ports**
- **Top 10 SSL case notations**
- **SSL Traffic stats**

## Server IP-specific panels
- SSL Server certificates seen on this IP
- SSL Pattern of life
- HTTP requests to this IP
- Top 100 SSL clients

## Certificate Field search: *%mail.ru* 
<table>
<thead>
<tr>
<th>Server</th>
<th>IP Address</th>
<th>TTL</th>
<th>Days</th>
<th>Mailing Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>184.14</td>
<td>m.mail.ru</td>
<td>80</td>
<td>29.1</td>
<td></td>
</tr>
<tr>
<td>184.14</td>
<td>a.mail.ru</td>
<td>80</td>
<td>15.1</td>
<td></td>
</tr>
<tr>
<td>184.14</td>
<td>auth.mail.ru</td>
<td>80</td>
<td>12.9</td>
<td></td>
</tr>
<tr>
<td>184.14</td>
<td>tel.mail.ru</td>
<td>80</td>
<td>10.8</td>
<td></td>
</tr>
<tr>
<td>184.14</td>
<td>e.mail.</td>
<td>80</td>
<td>10.5</td>
<td></td>
</tr>
<tr>
<td>184.14</td>
<td>mail.ru</td>
<td>80</td>
<td>10.4</td>
<td></td>
</tr>
</tbody>
</table>

## Top 100 SSL clients of serve: 184.14

### Tip 1: Filter by country of client IP (e.g. enter nothing to avoid filtering or Pi,TR,IP to filter by multiple countries): GB,US,CA,NZ,AU
- Only show clients in these countries
- Remove clients in these countries
- Remove clients that also act as servers
- Number of results returned: 100

### Tip 2: Right click on a client or server IP to explore it further!

<table>
<thead>
<tr>
<th>Client ID</th>
<th>Client country (conf)</th>
<th>Client company</th>
<th>First seen</th>
<th>Last seen</th>
<th>Count w/o 25th Nov</th>
<th>Count all time</th>
<th>Pairing status w/o 25th Nov</th>
<th>Pairing status all time</th>
</tr>
</thead>
<tbody>
<tr>
<td>89</td>
<td>ES(V)</td>
<td>Telefonica_de_Espana_SA,risa-bde.net</td>
<td>2011-10-10</td>
<td>2011-11-9</td>
<td>1415</td>
<td>30130</td>
<td>Server -&gt; Client only</td>
<td>Both directions</td>
</tr>
<tr>
<td>83</td>
<td>ES(V)</td>
<td>R_Cable_s Telecomunicaciones_Galicia S.A.,mundo-r</td>
<td>2011-10-24</td>
<td>2011-11-23</td>
<td>424</td>
<td>706</td>
<td>Client -&gt; Server only</td>
<td>Both directions</td>
</tr>
<tr>
<td>11</td>
<td>DE(V)</td>
<td>Bertelsmann_TI_Gmbh,mediakey.net</td>
<td>2011-09-23</td>
<td>2011-11-26</td>
<td>240</td>
<td>484</td>
<td>Client -&gt; Server only</td>
<td>Both directions</td>
</tr>
<tr>
<td>35</td>
<td>NO(V)</td>
<td>Telenor_Nextel AS,telenor.net</td>
<td>2011-10-26</td>
<td>2011-11-24</td>
<td>330</td>
<td>330</td>
<td>Server -&gt; Client only</td>
<td>Both directions</td>
</tr>
<tr>
<td>12</td>
<td>DE(V)</td>
<td>Bertelsmann_TI_Gmbh,mediakey.net</td>
<td>2011-10-26</td>
<td>2011-11-26</td>
<td>329</td>
<td>329</td>
<td>Server -&gt; Client only</td>
<td>Both directions</td>
</tr>
<tr>
<td>172</td>
<td>KR(M)</td>
<td>Korea_Telecom</td>
<td>2011-11-08</td>
<td>2011-11-10</td>
<td>296</td>
<td>296</td>
<td>Both directions</td>
<td>Both directions</td>
</tr>
<tr>
<td>152</td>
<td>EC(V)</td>
<td>EcuadorTelecom S.A.,eucotel.net</td>
<td>2011-11-08</td>
<td>2011-11-10</td>
<td>290</td>
<td>290</td>
<td>Both directions</td>
<td>Both directions</td>
</tr>
<tr>
<td>186</td>
<td>IE(V)</td>
<td>Vodafone_IEP,UNKNOWN</td>
<td>2011-10-26</td>
<td>2011-11-09</td>
<td>196</td>
<td>196</td>
<td>Both directions</td>
<td>Both directions</td>
</tr>
<tr>
<td>5</td>
<td>M(V)</td>
<td>TIMAT,holcom.net</td>
<td>2011-09-03</td>
<td>2011-11-04</td>
<td>199</td>
<td>363</td>
<td>Both directions</td>
<td>Both directions</td>
</tr>
<tr>
<td>153</td>
<td>KR(M)</td>
<td>QREN,RENET,UNKNOWN</td>
<td>2011-10-20</td>
<td>2011-10-20</td>
<td>181</td>
<td>181</td>
<td>Both directions</td>
<td>Both directions</td>
</tr>
<tr>
<td>102</td>
<td>IE(V)</td>
<td>Statos-Pool-Taupe</td>
<td>2011-10-21</td>
<td>2011-11-27</td>
<td>177</td>
<td>177</td>
<td>Both directions</td>
<td>Both directions</td>
</tr>
<tr>
<td>41</td>
<td>IE(V)</td>
<td>UTI,PLC,unicom,net</td>
<td>2011-11-12</td>
<td>2011-11-27</td>
<td>157</td>
<td>157</td>
<td>Both directions</td>
<td>Both directions</td>
</tr>
<tr>
<td>237</td>
<td>KR(M)</td>
<td>KRNK,ktn.or.kr</td>
<td>2011-09-03</td>
<td>2011-11-25</td>
<td>150</td>
<td>1007</td>
<td>Both directions</td>
<td>Both directions</td>
</tr>
<tr>
<td>97</td>
<td>KR(M)</td>
<td>Korea_Telecom,postman.co.kr</td>
<td>2011-10-16</td>
<td>2011-11-25</td>
<td>143</td>
<td>161</td>
<td>Both directions</td>
<td>Both directions</td>
</tr>
<tr>
<td>1</td>
<td>IE(V)</td>
<td>Vodafone_IEP,UNKNOWN</td>
<td>2011-11-18</td>
<td>2011-11-18</td>
<td>137</td>
<td>158</td>
<td>Both directions</td>
<td>Both directions</td>
</tr>
</tbody>
</table>
Query by client IP

Client IP-specific panels
- General IP info
- SSL Servers visited

Run Query

Certificate field search: .\mail.ru

General IP info for client IP

Top 100 SSL servers visited by client IP

Tip 1: Filter by country of server IP (e.g., enter PK to filter by Pakistan only or PK,IN,JQ to filter by multiple countries).
Tip 2: Right click on a client or server IP to explore it further.

1 - 8 of 8 Items

Client IP | Server IP | Server country (conf) | Server company info (from GEOFUSION export) | First seen | Last seen | Count w/ e 25th Nov | Count all time | Pairing status w/ e 25th Nov | Pairing status all time
--|---|---|---|---|---|---|---|---|---
127 | 194.16 | RU(M) | Mail.Ru,mail.ru | 03-09-11 05:18:48 | 25-11-11 10:15:23 | 269 | 2240 | Both directions | Both directions
127 | 194.15 | RU(M) | Mail.Ru,mail.ru | 05-09-11 03:20:27 | 25-11-11 11:49:27 | 213 | 2354 | Both directions | Both directions
127 | 213.87 | NL(C) | Mozilla,Corporate | | | | | | |
127 | 191.213 | RU(M) | Mail.Ru,mail.ru | 24-10-11 17:53:21 | 24-10-11 17:53:21 | 1 | | Client -> Server only | |
Query by network range

### General network info for 0/24
- **IP**: 184.14
- **Client IP**: 184.14
- **Network**: 0.24

### SSL clients in network 0.24

<table>
<thead>
<tr>
<th>Client IP</th>
<th>First seen</th>
<th>Last seen</th>
<th>Total SSL traffic w/e 25Th Nov</th>
<th>Total SSL traffic all time</th>
<th>Num. unique servers contacted w/e 25Th Nov</th>
<th>Num. unique servers contacted all time</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>2011-09-04</td>
<td>2011-09-04</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>23</td>
<td>2011-10-26</td>
<td>2011-11-23</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

### All SSL servers in network 0.24

### HTTP requests to IPs in network 0.24 (top 100)

<table>
<thead>
<tr>
<th>Server IP</th>
<th>Host name requested</th>
<th>First seen</th>
<th>Last seen</th>
<th>Count last week</th>
<th>Count all time</th>
</tr>
</thead>
<tbody>
<tr>
<td>18</td>
<td>Korea_Telecom,mailplug.co.kr</td>
<td>2011-11-11</td>
<td>2011-11-11</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

---

**Tip 1**: Right click on a client IP to explore it further.

**Tip 1**: Right click on a server IP to explore it further.
Cyber applications

- Diginotar certificate authority compromise:
  - Private keys of legitimate certificate authority, Diginotar, stolen by hacker.
  - FLYING PIG was used to identify a FIS using them to launch a MITM against their own citizens.

FLYING PIG screenshot showing fake certificate:

```
<table>
<thead>
<tr>
<th>Time</th>
<th>Port</th>
<th>Source</th>
<th>Destination</th>
<th>Date</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Time</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>2011-09-16</td>
<td>80</td>
<td>google.com</td>
<td>us</td>
<td>google inc</td>
<td>2012-09-05</td>
<td>06:15:49</td>
<td>us</td>
<td>google互联网权威</td>
<td>2012-09-20</td>
</tr>
<tr>
<td>2011-09-20</td>
<td>80</td>
<td>google.com</td>
<td>us</td>
<td>google inc</td>
<td>2012-09-20</td>
<td>06:05:49</td>
<td>us</td>
<td>google互联网权威</td>
<td>2012-09-20</td>
</tr>
<tr>
<td>2011-10-20</td>
<td>80</td>
<td>google.com</td>
<td>us</td>
<td>google inc</td>
<td>2012-11-02</td>
<td>21:08:36</td>
<td>us</td>
<td>google互联网权威</td>
<td>2012-11-14</td>
</tr>
<tr>
<td>2011-11-25</td>
<td>80</td>
<td>google.com</td>
<td>us</td>
<td>google inc</td>
<td>2011-09-02</td>
<td>08:00:28</td>
<td>us</td>
<td><a href="mailto:sfi@bluecoat.sfi">sfi@bluecoat.sfi</a>@corp.com</td>
<td>N</td>
</tr>
<tr>
<td>2011-11-25</td>
<td>80</td>
<td>google.com</td>
<td>us</td>
<td>google inc</td>
<td>2012-08-12</td>
<td>03:59:02</td>
<td>us</td>
<td>google互联网权威</td>
<td>2012-09-20</td>
</tr>
<tr>
<td>2011-11-25</td>
<td>80</td>
<td>google.com</td>
<td>us</td>
<td>google inc</td>
<td>2011-09-02</td>
<td>07:56:28</td>
<td>us</td>
<td><a href="mailto:sfi@bluecoat.sfi">sfi@bluecoat.sfi</a>@corp.com</td>
<td>N</td>
</tr>
<tr>
<td>2011-11-25</td>
<td>80</td>
<td>google.com</td>
<td>us</td>
<td>google inc</td>
<td>2011-09-02</td>
<td>07:56:28</td>
<td>us</td>
<td><a href="mailto:sfi@bluecoat.sfi">sfi@bluecoat.sfi</a>@corp.com</td>
<td>N</td>
</tr>
<tr>
<td>2011-11-25</td>
<td>80</td>
<td>google.com</td>
<td>us</td>
<td>google inc</td>
<td>2011-09-02</td>
<td>07:56:28</td>
<td>us</td>
<td><a href="mailto:sfi@bluecoat.sfi">sfi@bluecoat.sfi</a>@corp.com</td>
<td>N</td>
</tr>
</tbody>
</table>
```
Cyber applications

• Other Cyber applications:
  
  – Multiple examples of FIS data exfiltration using SSL have been found using FLYING PIG.
  
  – In particular, certificates related to LEGION JADE, LEGION RUBY, and MAKERSMARK activity were found on FLYING PIG using known signatures.
  
  – These were then used to find previously unknown servers involved in exfiltration from US companies.
  
  – FLYING PIG has also been used to identify events involving a mail server used by Russian Intelligence.
Identification of malicious TLS/SSL

- Can identify malicious TLS/SSL using signatures if known
- However this approach generally does not allow discovery of new threats
- Alternative is to use “behavioural” features to automatically identify potentially malicious traffic
- Features currently being investigated include:
  - Certificates with same subject but different issuers – may be indicative of Diginotar-style attack
  - Beaconing in TLS/SSL (indicative of botnets/FIS implants)
  - Number of client cipher suites offered
  - Repeated identical random challenges
HUSH PUPPY – motivation

- Much private network traffic seen but previously discarded
- If traffic could be attributed, potential high value – close access
- HUSH PUPPY is a bulk private network identification Cloud analytic
- Basic idea is to look for the same TDI being seen coming from a private address and then from a public address within a short time
- The private traffic can then be attributed to the owner of the public address
- Works for SSE & COMSAT
HUSH PUPPY – example

Yahoo

Internet

1.2.3.4

NAT or proxy

Private network

192.168.0.2

request to Yahoo

Y cookie:
fred@yahoo.com

Y cookie:
fred@yahoo.com
Other HUSH PUPPY datasets

- HUSH PUPPY also makes use of Yahoo T-cookies to do correlations

- A T-cookie contains the IP address of the client as Yahoo sees it

- Hence a T cookie coming from a private IP can give the public IP of the NAT or proxy

- In addition, HUSH PUPPY uses the following data to help verify results
  - Kerberos & Lotus Notes: Domains, organisations, departments, countries, machine names, user names
  - HTTP: Heuristic detection of Intranet web servers
  - SSL: Issuers, subjects, countries
  - SMTP: From & to domains
Results – what do we find?

- Foreign government networks
- Airlines
- Energy companies
- Financial organisations

- In cases of good collection, 50-80% of collected private network traffic has been attributed

- Some false positives can arise if few events correlated, due to factors such as TDIs not being completely unique and public internet proxies giving misleading public IP results

- Results can frequently be verified using Kerberos etc data
Examples of operational successes

- A large private network related to the Afghan government was identified, with ~800,000 events correlated.

- Examination of the case notations suggested it belonged to the Afghan MOD
  - A Kerberos domain mod.local
  - HTTP servers *.mod.local & mail
  - SSL certificates with the subject “Ministry of Defense” and the geo “AF”

- Results confirmed by analysis of content on XKEYSCORE

- A VSAT private network belonging to a Ministry of Foreign Affairs was identified

- NOSEY PARKER events were correlated with SSE
Contacts

- FLYING PIG – [Redacted]
- HUSH PUPPY – [Redacted]