The Rupture API: Productizing TLS attacks

Aggelos Kiayias
Eva Sarafianou
Dionysis Zindros

Real World Crypto 2017
Attack Anatomy
- Attacker guesses part of secret
- Uses it in reflection
- Compressed/encrypted response is shorter if right!
Adaptively choosing reflections strings can lead to **full recovery**.

But there are challenges:
1. Noise
2. Antagonistic compression methods (Huffman coding)
3. Unrelated static content on page matching candidates
Our Contributions

- **Usable** open-source tool
- Demonstrate attack is **easy** and **practical** via web UI
- Reusable **RESTful API**
Demo
Network Overview

Completed

Running & Paused

Not started
Network Overview

Completed

Running & Paused

Not started

Scan for victims

Add custom victim
Network Overview

Completed

Running & Paused

Not started

Scanning...

Add custom victim
Network Overview

Completed

Running & Paused

Not started

Not started
192.168.1.1

Not started
192.168.1.2

Not started
192.168.1.3

Not started
192.168.1.4
Choose Target: ruptureit
IP: 192.168.1.5

Attack
Choose Target: Demo
IP: 192.168.1.5
Attack
Network Overview

Completed

Running & Paused

running
192.168.15
Demo

0:0:2
more details

Not started
Ruptureit

Scan for victims
Add custom victim
Choose Target: ruptureit

IP: 192.168.1.2

Attack
Create Target

Name: Demo
Endpoint url: https://ruptureit.com/test2.php?r
Known prefix: biben
Secret length: 8
Secret Alphabet: abcdefghijklmnopqrstuvwxyz
Alignment Alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ
Record cardinality: 1
Method: Serial

Submit
Demo

192.168.1.5

Decrypted secret: biben

<table>
<thead>
<tr>
<th>Round</th>
<th>Batch</th>
<th>Alignment Alphabet</th>
<th>Possible Knownprefix</th>
<th>Confidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>NQIPLUJDCKBMYEAHSTZGOFWVRX</td>
<td>bibend</td>
<td>0.546875</td>
</tr>
</tbody>
</table>
Demo

192.168.1.5

Decrypted secret: biben

<table>
<thead>
<tr>
<th>Round</th>
<th>Batch</th>
<th>Alignment Alphabet</th>
<th>Possible Knownprefix</th>
<th>Confidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>NQIPLUJDCKBMYEAHTSZGOFWVRX</td>
<td>bibend</td>
<td>0.546875</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>TIROYSXHEKJMBADGLZPWUVCNQ</td>
<td>bibend</td>
<td>0.5</td>
</tr>
</tbody>
</table>
### Demo

**192.168.1.5**

Decrypted secret: biben

<table>
<thead>
<tr>
<th>Round</th>
<th>Batch</th>
<th>Alignment Alphabet</th>
<th>Possible Knownprefix</th>
<th>Confidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>NQIPLUJDCKBMYEAHTSZGOFWVRX</td>
<td>bibend</td>
<td>0.546875</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>TIROYSXHEKJMBADGLZPWUVFCNQ</td>
<td>bibend</td>
<td>0.5</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>QBCRAVFWMHYZTGOLKDJISUPXE</td>
<td>bibend</td>
<td>0.578125</td>
</tr>
</tbody>
</table>
https://github.com/dionyziz/rupture

https://ruptureit.com/
Thank you! Questions?
https://github.com/dionyziz/rupture

http://www.kiayias.com
E5F2 7045 437B 168B 39AD 1BFA C876 8019 6DBB 04E0

https://esarafianou.github.io
2FA9 7528 9554 F1EB F5F8 675B E371 5849 8CD0 92EE

https://dionyziz.com
45DC 00AE FDDF 5D5C B988 EC86 2DA4 50F3 AFB0 46C7