SIPSA - one step closer to real anonymity on the Internet

Source IP spoofing for anonymization over UDP

Kiriis Solovjovs, BalCCon2k16
Who is this guy?

- IT security expert; researcher at 1st Ltd, Latvia
- Skills: network flow analysis, reverse engineering, social engineering, penetration testing, security incident investigation, and the legal dimension of cyber security and cyber defence
- The responsible disclosure guy
- Still an inventor at heart
What is this talk? Why does it exist?

- To introduce SIPSA to the world,
- thus encouraging discussion
  - on real-life applications of the technology
  - and improvements to it,
- and hopefully getting merge/pull requests.
Intro crash-course: networking
Application Layer
- Message format, Human-Machine Interfaces

Presentation Layer
- Coding into 1s and 0s; encryption, compression

Session Layer
- Authentication, permissions, session restoration

Transport Layer
- End-to-end error control

Network Layer
- Network addressing; routing or switching

Data Link Layer
- Error detection, flow control on physical link

Physical Layer
- Bit stream: physical medium, method of representing bits
TCP vs UDP
TCP features

- Stateful, connection-oriented
- "Reliable" transport
- Notable features include:
  - 3-way handshake
  - Error detection
  - Ordered transfer
  - Flow control
UDP features

- Stateless, transaction-oriented
- "Best effort" transport
- Notable features include:
  - Minimalist design
  - No control
  - No retransmissions
Anonymity on the Internet... ?
Problem?

- IPs on Layer 3 needed for routing
- Cannot remove or encrypt them
- Yes, problem!
A statistical solution!

- Global bandwidth is increasing by an order of magnitude every 5 years!
- We need MORE DATAGRAMS
- Yes, a statistical solution!
No, it does not come with a logo. It's not a vulnerability, ffs.

SIPSA
A dream come true?
SIPSA overview

- Protocol goes on top of Layer 4, but below Layer 3 [!] 
- Instead of sending a single UDP datagram, many are sent
  - Different pairs of (randomised) source and destination IPs
- Protocol allows for the expansion / version support
- Current version (04) chooses IPs in pairs within a class C network
- Metadata currently includes (encrypted) real IPs and a list of the fakes
- Payload is not encrypted
Thus SIPSA should provide anonymity and deniability
SIPSA datagram format

<table>
<thead>
<tr>
<th>Header 5B</th>
<th>Reserved 1B</th>
<th>Proto ver 1B</th>
<th>Metalen 1B</th>
<th>IV 16B</th>
<th>Real src IP 4B</th>
<th>Real dst IP 4B</th>
<th>Src IP list 4B x n</th>
<th>End marker 1B</th>
<th>Dstd IP list 4B x n</th>
<th>End marker 1B</th>
<th>Padding 0B - 15B</th>
<th>Payload 0B +</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;SIPSA&quot;</td>
<td>&quot;00&quot;</td>
<td>&quot;04&quot;</td>
<td></td>
<td></td>
<td>4B may be zeros</td>
<td>4B may be zeros</td>
<td>n≥0</td>
<td>&quot;xFF&quot;</td>
<td>n≥0</td>
<td>&quot;xFF&quot;</td>
<td>0B – 15B</td>
<td>0B +</td>
</tr>
</tbody>
</table>

ENCRYPTED with AES256, CBC mode, 16B block, iv=IV, total size = (Metalen-1)*16B

*** Layer 2 Layer 2 Layer 2 Layer 2 Layer 2 ***

Layer 3 Layer 3 Layer 3 Layer 3 Layer 3 Layer 3 Layer 3

Layer 4 Layer 4 Layer 4 Layer 4 Layer 4 Layer 4 Layer 4

0x00 0x0a 0x0b 0x0c...

SIPSA
BCP38

- Network Ingress Filtering
- Drops packets having unknown source prefix
- Supposed to solve DoS
- Worked well, but did not solve DoS in the long term (today)
The good

- BCP38 has been sparsely implemented
- SIPSA may provide an additional layer of anonymity as part of a larger suite
- SIPSA provides deniability by virtue of UDP (and having fixed port numbering)
“No, your honour. My devices neither requested nor acknowledged receipt of the communication in question.”

--You, on SIPSA
The bad

- BCP38 is not going away; it's being slowly deployed on additional networks
- SIPSA gives only statistical improvement not 100% anonymity, so statistical attacks are likely possible
- Success largely depends on the ISPs involved
- Network load increase
  - 3x3 addresses 8x
  - 2x5 addresses 9x
  - 6x6 addresses 35x
And the demo
Future testing and research

- Anonymity
- General security
- Other ideas
Anonymity

- Consider not including real source IP in the metadata
  - Even the server has no way of knowing or logging client IPs
- Consider not sending packet from the real source at all
  - It's of course impossible to do both
General security

- Check validity of the crypto
- Key management
- Try attacking to find weak spots
- Obfuscate the protocol
Other ideas

- IPv6 support
- Include the random seed instead of the IP map in the metadata
- Stateful SIPSA
  - = a bit less bandwidth usage
- NAT? :( 
1. All feedback is welcome

2. Please fork and send merge/pull requests!

3. https://GitHub.com/0ki/SIPSA

4. I am @KirilsSolovjovs

5. Thank you for joining me and have a great con!