Covert channel vulnerabilities in anonymity systems

Steven J. Murdoch

http://www.cl.cam.ac.uk/users/sjm217/

UNIVERSITY OF CAMBRIDGE
Computer Laboratory

www.torproject.org

Security and Trust Management, 16–17 June 2008, Trondheim, Norway
It all started with an Xbox
The competition was to play Connect-4
Our programs signalled identity through the moves they made.
We wrote a paper for InfoHiding 2004
Following PET 2004, I operated a Tor node at Cambridge University.
Our attack was to trace anonymous paths through the network.
Latency measurements showed traffic load flowing through a node.
We wrote a paper for Oakland 2005

Xbox — Connect-4 — InfoHiding

Oakland

PET

Tor Traffic Analysis
Following InfoHiding 2004, I also investigated currency watermarking.
I presented my results at again 21C3, and attended a talk on Nushu.
Initial sequence numbers have complex structure

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Dest. IP</th>
<th>S. Port</th>
<th>D. Port</th>
</tr>
</thead>
</table>

Concatenate 32 random bits

R-MD4 block: 256 random bits

Take bits 32–63

c
replace top byte with rekey counter

and add 32-bit time (µs) + T
Initial sequence numbers have complex structure

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Dest. IP</th>
<th>S. Port</th>
<th>D. Port</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>R</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Concatenate 32 random bits

R-MD4 block: 256 random bits
Take bits 32–63

\[ c \]

replace top byte with rekey counter

. . .

and add 32-bit time (\( \mu s \)) + \( T \)
Initial sequence numbers have complex structure

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Dest. IP</th>
<th>S. Port</th>
<th>D. Port</th>
</tr>
</thead>
</table>

$R$  

Concatenate 32 random bits

$\text{R-MD4}$  

block: 256 random bits
Initial sequence numbers have complex structure

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Dest. IP</th>
<th>S. Port</th>
<th>D. Port</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Concatenate 32 random bits

R-MD4

block: 256 random bits

Take bits 32–63
Initial sequence numbers have complex structure

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Dest. IP</th>
<th>S. Port</th>
<th>D. Port</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>R</td>
</tr>
</tbody>
</table>

Concatenate 32 random bits

R-MD4

block: 256 random bits

Take bits 32–63

replace top byte with rekey counter...
Initial sequence numbers have complex structure

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Dest. IP</th>
<th>S. Port</th>
<th>D. Port</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

\[ R \]

- Concatenate 32 random bits

\[ \text{R-MD4} \]

- Block: 256 random bits

\[ c + T \]

- Take bits 32–63

- ...and add 32-bit time (\( \mu s \))
Even putting perfectly random ISNs will be detectable.
We wrote a paper on TCP steganography for InfoHiding 2005.
At Oakland 2005 I attended a talk on clock skew and security
Clock skew changes with temperature

Temperature (°C)

Non-linear offset

Variable skew

De-noised

Time

Fri 11:00  Fri 21:00  Sat 07:00  Sat 17:00

Non-linear offset component (ms)
We can do the same attack on Tor, measuring skew rather than latency.
The results show clear patterns
From these results, I wrote my thesis.