Large Scale Simulation of Tor: Stream Correlation Attacks

Gavin O' Gorman

Dublin City University

December 8, 2007

Large Scale Simulation of Tor: Stream Correlation Attacks

Gavin O' Gorman

Anonymous Networks Mix Networks Low latency Networks

Network Simulation

Results

Anonymous networks



Large Scale Simulation of Tor: Stream Correlation Attacks

Gavin O' Gorman

Anonymous Networks Mix Networks Low latency Networks

Network Simulation

Results Attacks

Proxy

Large Scale Simulation of Tor: Stream Correlation Attacks

Gavin O' Gorman

Anonymous Networks

Mix Networks Low latency Networks

Network Simulation

Results

Conclusior



◆□▶□★@▶|★ 国▶|★ 国▶| - 国|-

Simple Mix

Large Scale Simulation of Tor: Stream Correlation Attacks

Gavin O' Gorman

Anonymous Networks

Mix Networks Low latency Networks

Network Simulation

Results



Cascade Mix

Large Scale Simulation of Tor: Stream Correlation Attacks

Gavin O' Gorman

Anonymous Networks

Mix Networks Low latency Networks

Network Simulation

Results

~ · ·



Free Cascade Mix



Large Scale Simulation of Tor: Stream Correlation Attacks

Gavin O' Gorman

Anonymous Networks

Mix Networks Low latency Networks

Network Simulation

Results

.....

Low latency network



Large Scale Simulation of Tor: Stream Correlation Attacks

Gavin O' Gorman

Anonymous Networks Mix Networks Low latency Networks

Network Simulation

Results

Attacks

Traffic Analysis



Large Scale Simulation of Tor: Stream Correlation Attacks

Gavin O' Gorman

Anonymous Networks Mix Networks Low latency Networks

Network Simulation

Results

Attacks

Currently deployed anonymous networks

- Over 1500 nodes
- Over 100 countries
- Hundreds of thousands on connections through the network

イロト 不得 トイヨト イヨト 三日

Theorized traffic analysis attacks

Large Scale Simulation of Tor: Stream Correlation Attacks

Gavin O' Gorman

Anonymous Networks Mix Networks Low latency Networks

Network Simulation

Results

Currently deployed anonymous networks

- Over 1500 nodes
- Over 100 countries
- Hundreds of thousands on connections through the network

イロト イポト イヨト イヨト 三日

- Theorized traffic analysis attacks
- How anonymous is a user ?

Large Scale Simulation of Tor: Stream Correlation Attacks

Gavin O' Gorman

Anonymous Networks Mix Networks Low latency Networks

Network Simulation

Results

SSFNet

- Scalable Simulation Framework Network (SSFNet)
- Simulate TCP/IP, Ethernet, Socket interfaces
- ► Has HTTP/TCP generators.
- TCPDump compatible output
- Simulated Tor circuits, routing, traffic fragmentation
- US ISP Topology
- 6,000 nodes
- Run the simulation for 1060 seconds to settle and then 60 for data

Large Scale Simulation of Tor: Stream Correlation Attacks

Gavin O' Gorman

Anonymous Networks Mix Networks Low latency Networks

Network Simulation

Results

Tor Simulation Process



Large Scale Simulation of Tor: Stream Correlation Attacks

Gavin O' Gorman

Anonymous Networks Mix Networks Low latency Networks

Network Simulation

Results

ALLACKS

Results

- Probability of correctly identifying streams entering the network with streams exiting the network
- Several attacks used
 - Start and End timing
 - Packet counting
 - Cross-Correlation Pearson Function
- Run the attacks with increasing numbers of streams

Don't know the transit time, so have to test

Large Scale Simulation of Tor: Stream Correlation Attacks

Gavin O' Gorman

Anonymous Networks Mix Networks Low latency Networks

Network Simulation

Results

Start & End stream timing

Compare the start and end times of streams 98% to 94% of streams filtered

ヘロン ヘロン ヘロン ヘロン

э

Large Scale Simulation of Tor: Stream Correlation Attacks

Gavin O' Gorman

Anonymous Networks Mix Networks Low latency Networks

Network Simulation

Results

Attacks

Packet counting

Count the number of cells in a stream 5% to 15% of streams are removed.

Large Scale Simulation of Tor: Stream Correlation Attacks

Gavin O' Gorman

Anonymous Networks Mix Networks Low latency Networks

Network Simulation

Results

Attacks

(日)((四))(日)(日)(日)(日)

Cross-Correlation

$$r(d) = \frac{\sum_{i}((x_{i} - \mu)(x'_{i+d} - \mu'))}{\sqrt{\sum_{i}(x_{i} - \mu)^{2}}\sqrt{\sum_{i}(x'_{i+d} - \mu')^{2}}}$$

Set a windows size W and count the number of packets received

- x_i is the *i*th packet count of stream x
- x'_i is the *i*th packet count of stream x'
- μ is the average of packet counts in stream x
- d is the variable delay value

Large Scale Simulation of Tor: Stream Correlation Attacks

Gavin O' Gorman

Anonymous Networks Mix Networks Low latency Networks

Network Simulation

Results

Attacks

Cross-Correlation



ヘロト ヘロト ヘヨト ヘヨト

Large Scale Simulation of Tor: Stream Correlation Attacks

Gavin O' Gorman

三 のへで

Conclusion

- Initial results show promise
- Future work the simulation will allow us to:
 - Introduce delay and measure QoS & Anonymity
 - Test active attacks
 - Modify Tor protocol to account for specific attacks scenarios

Large Scale Simulation of Tor: Stream Correlation Attacks

Gavin O' Gorman

Anonymous Networks Mix Networks Low latency Networks

Network Simulation

Results

Thank you!

 Thanks for listening and thanks to Science Foundation Ireland

science foundation ireland

ヘロト ヘロト ヘヨト ヘヨト

э

Large Scale Simulation of Tor: Stream Correlation Attacks

Gavin O' Gorman

Anonymous Networks Mix Networks Low latency Networks

Network Simulation

Results

Attacks

Any questions ?

Large Scale Simulation of Tor: Stream Correlation Attacks

Gavin O' Gorman

Conclusion ヘロト ヘヨト ヘヨト ヘヨト ъ