Stopping Silent Sneaks: Defending against Malicious Mixes through Topological Engineering

Xinshu Ma [1] Florentin Rochet [2] Tariq Elahi [1]

[1]University of Edinburgh [2]University of Namur

Problem

Trustworthy Mixnet Construction from Untrusted Resources

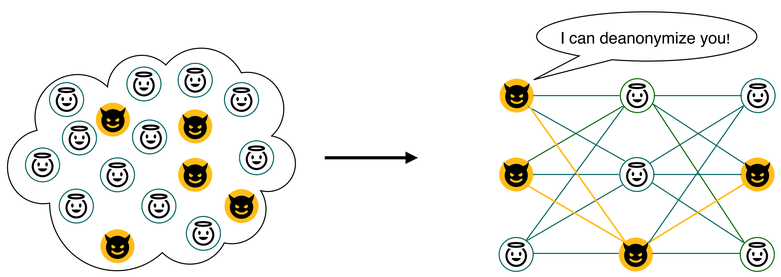
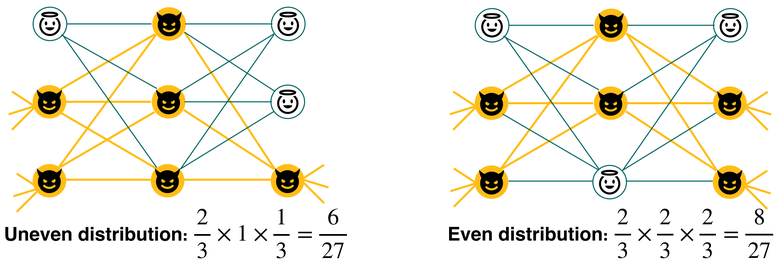


Figure 1. **Anytrust assumption** might break in the real world: users suffer from **end-to-end compromise** and **client enumeration** by passive adversary.



Uneven distribution: $\frac{2}{3} \times 1 \times \frac{1}{3} = \frac{6}{27}$

Even distribution: $\frac{2}{3} \times \frac{2}{3} \times \frac{2}{3} = \frac{8}{27}$

Figure 2. Adversary **maximizes** the compromised rate by achieving even distribution.

Mixnet construction model:

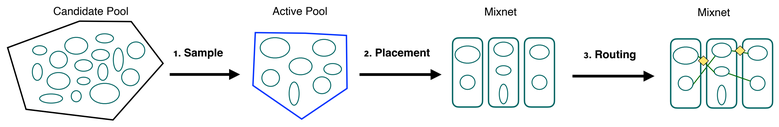


Figure 3. 3-stage process: periodically reconstruction; only use a subset of nodes.

Example of Adversary's Manipulation

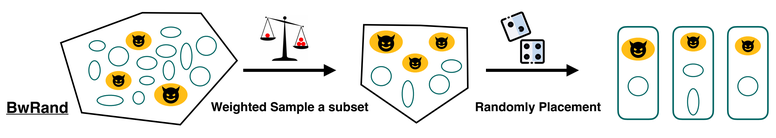


Figure 4. Adversary can compromise more than 10% of total traffic with $\alpha = 0.2$ resources by manipulating mixes' bandwidth.

Design

Challenges

1. An adversary's manipulation is hard to detect.
2. An adversary can perform client enumeration at a low cost.
3. Tolerating nodes churn.
4. Performance bottleneck comes from the layer with lowest capacity.

Our Approach

1. Contradictory requirements creates challenges for even distribution.
2. Guard layer mitigates the risk of client enumeration.
3. Stability tracking and network maintenance design.
4. Bin-packing placement to reach even layer capacity.

Bow-Tie: High-level Overview

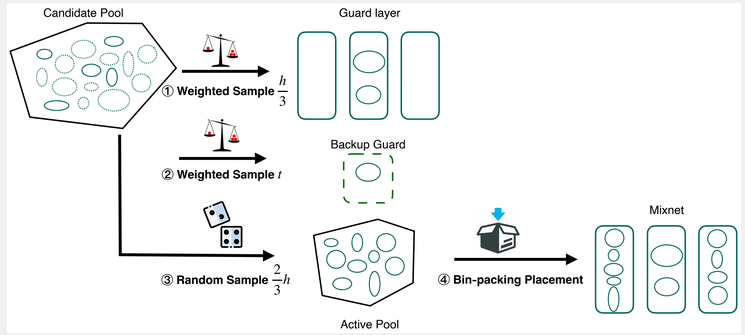


Figure 5. Mixnet Initialization

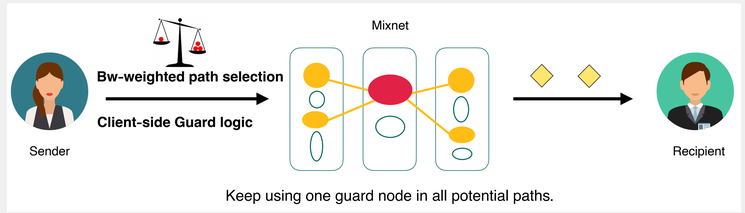


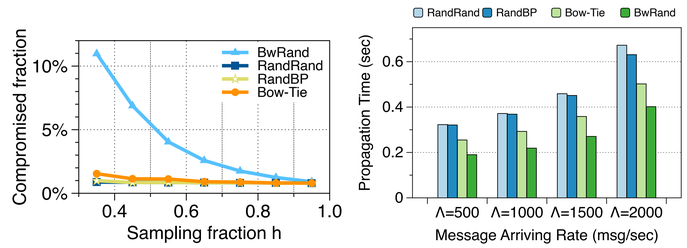
Figure 6. Mixnet Routing

Takeaways

- Design: A constrained guard layer that is populated with stable and high performant relays creates a challenge for the adversary.
- Results: Bow-Tie finds a good balance between security and performance.

Analysis

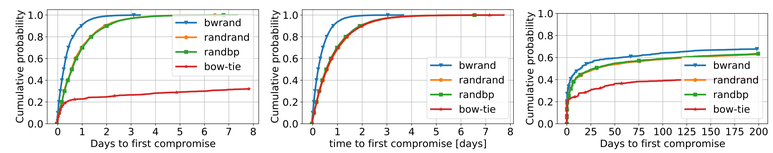
A Balance between Security and Performance



(a) End-to-end compromise rate (b) Average queuing delay

Figure 7. Adversary controls $\alpha = 0.2$ of the total bandwidth. h denotes the active pool size at the sampling step.

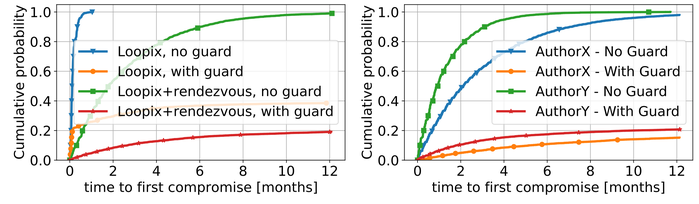
Necessity of Guard Design



(a) Bow-Tie vs others (b) Turn of guard logic (c) Turn on guard logic

Figure 8. The combination of guard layer and client-side guard logic reduces clients' exposure more effectively than they each could do.

Influence of Protocol Design and User Behaviour



(a) Influence of protocol design (b) Influence of individual behaviours

Figure 9. (a) Bow-Tie's effect is compatible to mixnet protocol designs. (b) Users can figure out how long they could safely use the network based on their behaviours.

Contact

x.ma@ed.ac.uk
frochet@ed.ac.uk
t.elahi@ed.ac.uk

THE UNIVERSITY of EDINBURGH

UNIVERSITÉ DE NAMUR

REPHRAIN Protecting citizens online