

Mix Behaviour Under Multiple Independent Attacks

J David Smith

Problem

- Alice & Bob attempting to communicate anonymously over a mix network.
- Gary attempting to determine with whom Alice is communicating.
- Hannah attempting to determine with whom Bob is communicating.
- Gary and Hannah are oblivious to each other's existence (and so they cannot communicate).
- How does the *strength* of the attacks change? How does the *cost* of the attack change?



What is Strength? What is Cost?

- Depends on attack.
- Example: Blending Attack
 - Strength: inversely proportional to size of final anonymity set (or entropy of final anonymity set). High final set size weak attack.
 - Cost: Number of messages \mathcal{A} has to delay or insert. Amount of time required to execute attack.
- These definitions may not apply to other attacks.

Approach

- Look at attacks that are well-understood with respect to a single attacker.
- Answer: what happens when 2 attackers? n attackers?
- Specifically: various blending attacks on mixes, beginning with simple threshold mix. (eg *From a Trickle to a Flood* [1])
- Hopefully: extend to other attacks on related tech (such as flow marking on Tor [2])
- Note: this only applies to active attackers, multiple passive adversaries will not interfere with each other

- Related works...
 - still trying to find works dealing with multiple independent attackers
 - Presently have found none, but found some dealing with collaborating attackers
 - Developing idea of how to work this problem from these previous works.

-  Andrei Serjantov, Roger Dingledine, and Paul Syverson. “From a trickle to a flood: Active attacks on several mix types”. In: *Information Hiding*. Springer, 2003, pp. 36–52. (Visited on 10/21/2015).
-  Wei Yu et al. “DSSS-Based Flow Marking Technique for Invisible Traceback”. In: *IEEE Symposium on Security and Privacy, 2007. SP '07*. IEEE Symposium on Security and Privacy, 2007. SP '07. May 2007, pp. 18–32.