

Reliable MIX Cascade Networks via Reputation

Paul Syverson

Naval Research Laboratory

E-mail: syverson@itd.nrl.navy.mil

URL: www.syverson.org

joint work with

Roger Dingledine

Reputation Technologies, Inc.

E-mail: arma@reputation.com



Basic Goals

Build a network

- where every message has a high probability of correct delivery
- where every message has a very low probability of anonymity compromise
- without heavyweight protocols (ZK proofs, etc.)
- without special trusted parties
- with minimal assumptions about the honesty and competence of intended participants

Basic Ideas

- Arrange network into MIX cascades (fixed route paths)
- MIXes communally generate a random seed
 - Seed determines the configuration of cascades in unpredictable manner
- A cascade fails iff a member says it fails
- Failure decreases reputation of all nodes in cascade
- MIXes test and observe their own cascade determine cascade misbehavior
- No trusted witnesses needed

Background and Prior Work

- MIXes (basic anonymity building blocks)
- Flash MIXes: provide robustness by distributing MIX
 - Mixing guaranteed as long as k of n servers are OK
 - **BUT** uses heavyweight protocols
- Reputation system given previously, for free routes not cascades
 - **BUT** Cascades give better anonymity for widely distributed adversary
 - **BUT** Require global trusted witnesses
 - **BUT** Adversary can get/analyze more traffic by gaining reputation

Our Contributions

- Removes above limitations of prior work
- Our Goal: Improve Reliability not Provable Robustness
 - Focus is on detection and deterrence rather than direct prevention
- Recall strategy: If a cascade member detects misbehavior, s/he fails the cascade.
- Our reputation system
 - Facilitates giving users information about network state: allows better informed route choices
 - Behind the scene: cascade formation algorithm improves reliability

Calculating Reputations & Forming Cascades

- Reputation points/demerits for
 - Good service, consistently revealing, adequate trust

Creeping Death attack

Assuming reputation decremented if a cascade fails, bad guys can always control a single block of any reputation, including the highest. Bad guy strategy:

- If you are only bad guy in a cascade fail, else not.
- Result is a block of bad guys that creeps up the rep chart
- Adversary can have many nodes in a single reputation \Rightarrow many all bad cascades \Rightarrow anonymity compromise
- Strategy response: Build cascades from broad enough pool that it does not matter what the reputation of adversary nodes is

Calculating Reputations & Forming Cascades 2

Free lunch problems

- Too easy to get nodes into network
 - Pseudospoofing
 - Proof of work, proof of bandwidth not strong enough
- Strategy response: Use Advogato trust metrics to enter join network
 - Bounds adversary nodes in network, even in face of unbounded bandwidth and computation abilities

Calculating Reputations & Forming Cascades 3

Let

p = fraction of nodes that are bad, e.g., 20%

s = scare factor: OK odds of cascade compromise, e.g., 10^{-5}

r = range: size of pool from which cascades are chosen, ?

l = length of single cascades, e.g., 4

c = chain length: recommended number of chained cascades, e.g., 3

$$\left(\frac{p}{r} \right)^{lc} = s \quad r = \left(\frac{p}{s^{1/lc}} \right) = \left(\frac{.2}{(10^{-5})^{1/12}} \right) = 0.522$$

Speculations about Future Work

- Working proof-of-bandwidth would reduce dependence on web of trust
- Better approaches to generating origins and destinations for dummy traffic or reduction in overhead for dummies and/or delivery
- Improved cascade configuration algorithms
- More research in understanding (countering?) creeping death
- Analysis to show bounds on adversary work under various models