the cost and effectiveness of blending attacks against mixes

Meng Tang

10/2015

- mixes can be vulnerable to blending attacks
  - threshold mix - flood
  - timed mix - trickle
  - threshold pool mix - flood (uncertain)

  ...

  bad implementation of mixes can greatly reduce anonymity

- problem:
  - how well will blending attacks perform against different mixes?
  - how much anonymity can mixes provide with blending attacks present?
  - are there other attacking schemes that may put mix network at risk?

objective

- explore existing blending attacks against mixes and evaluate their performance
- measure different mixes' resistance to blending attacks
- try to reveal more weakness of mixes / mix network, if possible

approach

- simulate the behavior of mixes and a global active attacker

- measure attacking effectiveness by cost and accuracy

- compare between different mix types and attacks

possible experiments

- what will happen if the environment is more favorable to the attacker?
  - small number of mixes
  - specific network topology
  - preknown information

  ...

- references

  - 1.Andreas Pfitzmann, Michael Waidner. Networks Without User Observability. Computers and Security, 6(2), 1987, pp.158-166.
  - 2.Brian N. Levine, Michael K. Reiter, Chenxi Wang, Matthew Wright. Timing Attacks in Low-Latency Mix Systems. Financial Cryptography, 2004, pp.251-265.
  - 3.Claudia Diaz, Andrei Serjantov. Generalising Mixes. In Privacy Enhacing Technologies, LNCS, 2003, pp.18-31.
  - 4.David Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. Communications of the ACM, 4(2), February 1981.
  - 5.David M. Goldschlag, Michael G. Reed, Paul F. Syverson. Hiding Routing Information. Proceedings of the First International Workshop on Information Hiding, 1996, pp.137-150
  - 6.George Danezis. Designing and attacking anonymous communication systems (UCAM-CL-TR-594).
  - 7.Luke O'Connor. On Blending Attacks For Mixes with Memory Extended Version. 7th International Workshop, 2005, pp.39-52.
  - 8.Parvathinathan Venkitasubramaniam, Venkat Anantharam. On the Anonymity of Chaum Mixes. Proceedings 2008 IEEE international symposium on information theory, pp.534-538.

- questions