Attacks on Anonymity Systems:
The Practice

Roger Dingledine

http://freehaven.net

Len Sassaman

http://anonymizer.com

Attack Methodology

- What attacks really exist?
- When building anonymity systems:
  - Designers anticipate possible attacks, and try to protect against them
  - Many of these attacks may not be feasible
  - Some may not be preventable
- Implementers must focus first on thwarting attacks that are most likely to be used

Threat models

- In order to evaluate an anonymity system, one must know the threats it addresses
- What are the attacker(s) capabilities?
- What kind of damage is acceptable?
- What are the reasonable performance, reliability, and price trade-offs?

Types of Adversaries

- Global Observer
  - Has omniscient network view (and can process data effectively!)
- External Attacker
  - No special advantages
  - Can send messages into system, observe output
- Rogue Operator
  - Owns a node and knows the business

Attack Goals

- Break anonymity
  - Compromise selective users
  - Compromise all users
  - Conditional anonymity
- Break utility
  - Prevent anonymity service from being reliable
  - Redirect potential users to less secure services
  - *Breaking utility leads to breaking anonymity*
  - Deny service entirely

Anonymity Breaking Attacks

- Replay Attacks
- Blending Attacks
- Attacks on multiple messages / large files
- Pseudospoofing
- Tagging attacks
- Partitioning attacks (passive and active)
- Intersection attacks
- Timing and packet counting attacks

Replay Attacks

- *"Déjà vu"*
- A captured message will follow the same path when resent
- Traceable by a Global Observer
- Provides clues to Rogue Operators, and possibly to External Observers
  - Posts to Usenet, etc.

Blending Attacks

- *"an unfriendly crowd"*
- Trickle, flood, *n* -1
- Intended to defeat a mix
- Requires observation capabilities
- Requires traffic flow manipulation

Attacks on Multiple Messages

- *"We're not like everyone else"*
- Large files become multiple messages
- Traffic analysis is easier
- Input and exit correlation
- Mix network can be a black box

Pseudospoofing

- *"tentacles and sock-puppets"*
- An attacker running many nodes increases the chance of chains consisting of entirely his nodes
- Users don't know operators are all one entity acting as multiple personas

Tagging attacks

- *"shuffling a marked deck"*
- Bit flipping
- Tracking identifying markings
- Allows blind-spots in observable network

Partitioning attacks

- *"divide and conquer"*
- Key rotation
- Node list discrepancies
- Capability changes
- Uniquely identifiable clients
  - (compatibility isn't the issue -- anonymity system components must operate *identically*)

Intersection attacks

- *"it's only a matter of time"*
- Usage pattern data over time

Timing and Packet Counting Attacks

- Statistical analysis of network traffic
- Low-latency systems at great risk

Utility Breaking Attacks

- Economic/incentives attacks
- Reputation attacks
- Flooding attacks

Economic/Incentives Attacks

- Drive users to less secure systems
- Increase cost of more secure systems
- Discourage committed operators
- Less users mean less security

Reputation Attacks

- *"a good old smear campaign"*
- Cast doubts on security of strong systems
- Spread FUD to less informed users
- Discourage development of software and operation of services by targeting principal contributors
- Cause confusion

Flooding Attacks

- Exhaust node resources
- Harm node reliability
- Create abuse complaints
- Can be economic or reputation attacks
- Often exacerbated by protocol mistakes
  - Ex.: Cypherpunk Remailers

Capabilities of Attackers

- Three types of attackers
  - Global Observer
  - External Attacker
  - Rogue Operator
- Three sets of goals
  - Compromise of Anonymity
  - Denial of Service
  - Degradation of Utility

Determining Threat Model

- Attackers will pick the type of attack which most easily achieves their goals
- Anonymity systems should identify the user's needs as well as his potential adversaries

Building the Perfect Anonymity System

- Systems which sacrifice usability and reliability in order to protect against attacks that are not able or likely to be used are flawed
- Systems should strive for the strongest threat model possible within the existing constraints
  - "zero-cost improvements"
- Remember: More users means more anonymity