

# What Future for Anonymity Research?

(Anonymity: what is it good for?)

George Danezis

Computer Security Group  
University of Cambridge Computer Laboratory

# Outline

- Brief introduction to the state of the art constructions for anonymous communications.
- Some notes on latest theory and attacks.
  - Future (We could have stopped here!)
- Requirements engineering
  - How is anonymity used (function it fulfills).
  - New requirements or new primitives?
- A comment on the order.

# Theory

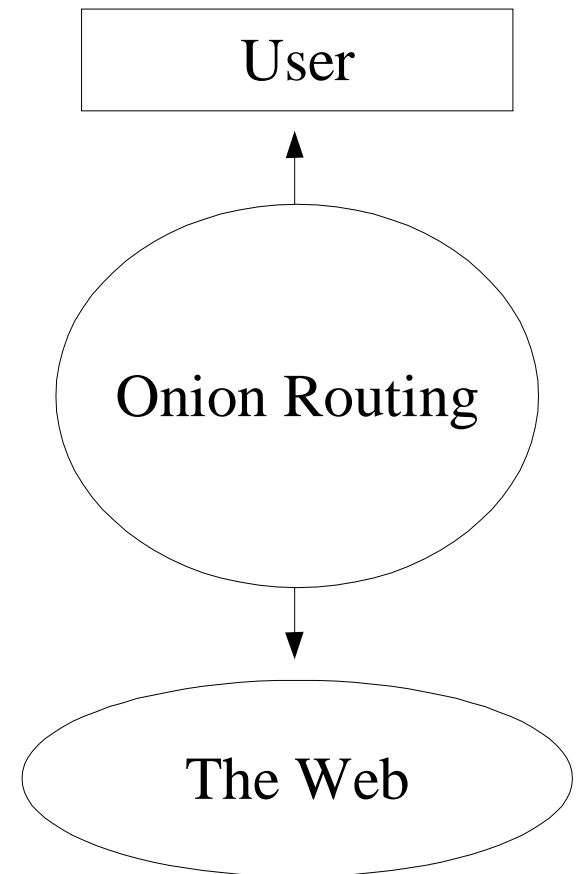
- Measures of anonymity:
  - Degrees of anonymity
  - Anonymity sets
  - Information theoretic definitions
    - “The amount of missing information to uniquely identify an actor”*
- Understanding Batching strategies
- Understanding network topologies
- New attacks

# Practice: Mix Systems

- Chaum 1981: Proposes the concept of mix nodes, networks, cascades, replies, receipts...
- Anonymise email (**Low volumes, High Latency**)
- Designed: Babel
- Deployed: Type I remailers, , Mixmaster ('90)
- *Type III “Mixminion” Remailer* ('00)
  - Anonymous forward messages and replies.
  - Resistant to traffic analysis, passive and active attacks.

# Practice: Onion Routing

- ISDN mixes (telephony)
- Anonymise bidirectional Streams/Web traffic using anonymous circuits.  
**(High volumes, Low Latency)**
- Onion routing: Cover traffic, exit policies, ...
- Peer to Peer:
  - All nodes are mixes
  - Tarzan, Morph Mix



# The bad news: Attacks

- Same route, high volumes, low latency = Attacks
- Very vulnerable to traffic analysis:
  - Intersection attacks (Pfitzmann, Berthold),  
(Statistical) disclosure attacks (Kesdogan, Danezis)
  - Packet counting attacks (Serjantov, Raymond)
  - Pattern detection attacks (Danezis)
  - Adaptive traffic modulation (Dai, Kuhn)
- Do we still believe we can do Anonymous Web browsing? Are we stuck?

# Back to Basics: Why Anonymity

- Primitives out of context are difficult to implement (e.g. asymmetric encryption).
- Need to think about the **contexts** in which a **security policy** would require properties that can be fulfilled by anonymity primitives.
- Threat models: how does anonymity breaks in the Real World.
- Come back with new sets of requirements, that we might have a chance to fulfill.

# e-Elections

- Anonymity used for privacy. (What does that mean anyway?)
- Sought property:
  - Freedom from coercion or fear of reprisal.
  - Inability to sell vote!
- *Receipt freeness*
- Not considered a requirement even in “secure” mix based systems. (Embarrassing)

# Censorship Resistance

- Anonymous publication and reading (Why?)
- Cannot coerce holders of documents to delete, cannot persecute writers or readers.
- Tensions between efficiency and hiding (impossibility?)
- But original objective more fundamental: “*survivability and accessibility of published content*”
- Would wider distribution rather than hiding be more effective? Is anonymity impeding this?
- Example: Church of Scientology cases.

# Web browsing (revisited)

- Model that uses an “anonymous channel” is vulnerable.
- But other models are available to perform the required functionality: “*allow readers to access a set of documents without any third party being able to link them.*”
- One could see the problem holistically (move away from the anonymous channel paradigm)
- Contrast the Onion routing approach with Freenet, Gnutella.

# Real World Attacks

- Java Anon Proxy: Court compels logging, police raids to seize logs.
- No traffic analysis
- RIP legislation & Co can require
  - the recording of traffic data
  - decryption of intercepted data
  - disclosure of secret keys
- Very different model from Global Passive Adversary.

# The Future?

- Think of anonymity as part of a system & integrate it within the security policy.
- Unobservability might be more promising for web browsing, and wider distribution for censorship resistance. (Accepting loses?)
- Receipt freeness *and* plausible deniability *has to be a core requirement, not just for elections but also to protect against adversaries with compulsion powers.*
- Is this the dual property of revocable anonymity?