TOP SECRET STRAP1 COMINT
The maximum classification allowed on GCWiki is **TOP SECRET STRAP1 COMINT**. Click to report inappropriate content.

TOR deanonymisation research (MIP)

From GCWiki
Jump to: navigation, search

OPC-MCR Mathematical Information Processing Research Task:
TOR deanonymisation

Customer: ICTR-NE
Status: in pullthrough (started December 2010)

MCR lead: [redacted]
Team: [redacted]
(ICTR-NE)

Can we denonymise TOR? In other words, if given some traffic from a TOR exit node, can we find the IP address of the user associated with that traffic?

Mathematical Information Processing Research

- Home
- Tasks:
  - active
  - all
  - in pullthrough, suspended, completed
- Papers
- Staff
- Monthly notes:
  - Current (open access)
  - Pre-July 2011: web RSS
  - Notes (pre-2010 limited access)
- Our processing user: brule
- Seminars
- Software

v · d · e

[edit] Research

A circuit tracing attack was first considered. However ICTR-NE signatures run by TDSD showed that our coverage of TOR is too low to have a reasonable chance of doing such an attack; on JTRIG paths we only saw 2 out of 8294 potential inter-TOR-node links.

Instead we are now considering an entry-exit correlation attack. Data collected from ICTR-NE/JTRIG infrastructure showed that some timing structure is preserved between entry and exit node.

The successful outcome of this entry-exit correlation attack is documented in OPC-M/TECH.B/61. An R package implementing the attack is available: src, doc.

The work was presented at SANAR11. The slides are here.

We plan to prototype the technique in the REMATION II workshop. The introductory slides are here.

Go Search

TOP SECRET STRAP1 COMINT
The maximum classification allowed on GCWiki is **TOP SECRET STRAP1 COMINT**. Click to report inappropriate content.