

TOP SECRET STRAP1

Tor: Overview of Existing Techniques (15 minutes)

ICTR-NE







Previous Work/Current Techniques

NETWORK EXPLOITATION

ICTR-related techniques

- . Identification of events by content
- . Tor node dictionary generation available from web site
- HOMING TROLL Bridge discovery prototype that feeds dictionary
- Statistical deanonymisation research (MCR)
- NEWTONS CRADLE (JTRIG)
- . TRIBAL CARNEM (with CT)
- . EPIC FAIL (CT)
- Bulk traffic logging
- QUICK ANT Low latency deanonymisation. Prototype under evaluation.
- Introducing timing patterns report available
- Hidden service investigation report available
- Shaping research some initial experiments.
- Some extraction of hidden service domain names from passive events.
- Tor implementation analysis (contract task)

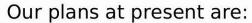
Also some work (through contract) on Freenet.





ICTR-NE Goals for 2012/13





- Tor deanonymisation collaboration with MCR and JTRIG
- Tor shaping with JTRIG
- Contract: next stage of Tor Implementation Analysis
- ICTR-CISA: record hidden service hostnames (*.onion) in NATURAL SELECTION.

... so REMATION II fits in well.

Any questions?





Reference: Ideas (2011)



- Maintain knowledge of Tor network Pullthrough from NE?
- Log Tor events into HAKIM for target discovery TR-FSP
- Build tool to implement low latency attack? ICTR
- Collecting traffic at exit nodes to feed passive SIGINT JTRIG
- Testing of MCR passive deanonymisation technique. MCR/JTRIG/ICTR
- Active injection and detection of timing patterns (probably following test of MCR technique) ICTR/JTRIG/MCR
- Herding of targets through our exit nodes (THEMP) ICTR/JTRIG
- Bulk logging of hidden service onion addresses (possibly only those hosting web sites) experiment carried out by ICTR
- Characterisation of hidden web servers by passive analysis ICTR?
- Characterisation of hidden web servers by web crawling ICTR?
- Identification of IP addresses hosting hidden services ICTR?
- Ongoing use/maintenance of TRIBAL CARNEM CT
- Find TDIs that appear on Tor and non-tor IP addresses (EPIC FAIL) CT
- Understanding Tor circuit creation and destruction ICTR contract
- Understanding future developments in Tor ICTR contract?
- Spotting private Tor networks ICTR?
- TorChat investigation? ICTR?





Reference: Data Sources



- Tor node consensus (obtained by Tor client) UNCLASSIFIED
- Information on Tor Bridges CONFIDENTIAL
- Collection from exit nodes SECRET
- Passive intercept (SECRET/TOP SECRET)
 - SSL events in cloud(s)
 - Tor packet logging (ICTR system)
 - Content exiting Tor network



