CSE 410 Fall 2025
Privacy-Enhancing Technologies

Marina Blanton

Department of Computer Science and Engineering
University at Buffalo

Lecture 15: Attacks on TOR, Censorship

Tor Network

TOR is the largest anonymous communication network in existence

- there are thousands of distinct server nodes around the world
- there are millions of users around the world
- it carries at least terabytes of traffic every day

TOR is an open-source project used for a variety of purposes

- by military and law enforcement agencies
- by journalists and activists
- by people wanting to circumvent censorship
- to avoid surveillance and protect sensitive information

Tor Network

Despite the Tor Project's good intentions, it also developed bad reputation

- it provides a hideaway for illegal activities such as selling drugs
- this has drawn the attention of government agencies to Tor
- documents leaked by Snowden revealed that NSA monitored inexperienced users of Tor for security loopholes

Tor Network

The growing popularity of Tor has also led to an increasing number of de-anonymizing attacks

- these attacks become increasingly advanced and effective
- one example is adding compromised servers to the Tor network

These raise questions about the anonymity and security of Tor

Tor Connections

Recall the Tor protocol

- communication goes through a number of onion routers or relays
- the first one is called the entry node
- the last one is called the exit node
- a circuit commonly consists of three onion relays

All relays are listed in the directory servers

This suggests an immediate attack by a censor: block the IP addresses of all relays listed in the directory servers

- Tor bridges are used to help discover an unlisted entry node

Tor Threat Model

Most attacks on Tor focus on identifying a relationship between a client and a server that use Tor to communicate

- this process is called de-anonymization

Often an adversary is assumed to be passive

- it is able to observe a part of the Tor network
- it can operate its own onion routers
- an attacker observes patterns and correlates inputs and outputs, i.e., performs
- traffic analysis is also used to de-anonymize users running hidden services

Tor Threat Model

An adversary can also be active

- it guesses communicating points and analyzes individual links to validate the guess
- it can inject, modify, or delete traffic going through corrupt ORs

Defense mechanisms focus on detecting deviation from the prescribed behavior

Because Tor relies on volunteers running nodes, we need to assume some nodes are controlled by an adversary

Types of Attacks

Categories of attacks on Tor

- correlations attacks
- congestion attacks
- timing attacks
- fingerprinting attacks
- denial of service attacks
- other (supportive) attacks

Correlation Attacks

Correlation attack is a de-anonymization attack

- the attacker controls both the entry node and the exit node of a circuit between a client and a server
- it is looking for a correlation in traffic between the entry node and the exit node

One example is a relay early traffic confirmation attack

- it attempts to identify clients using a hidden service
- a correlation attack is executed to confirm the relationship between a client and a hidden service
- the attack has been carried out on the real Tor network

Correlation Attacks

Relay early traffic confirmation attack

- a malicious onion router becomes a hidden service directory and an entry node
  - this is accomplished by means of a Sybil attack
- it needs to control the entry node and the hidden service directory a client will use
- a client requests introductory points from the hidden service directory
- the directory server encodes the hidden service in a pattern of relay and relay-early cells
  - relay-early cells are used to prevent building long circuits (which are used in congestion attacks)
- the entry node decodes it from the pattern when a client initiates a connection

Congestion Attacks

In a congestion attack, an attacker tries to determine the onion routers in a circuit of a target client

- the adversary congests onion routers one by one
- it looks for latency differences in the traffic flow of the target
- e.g., a client is downloading a large file from a website controlled by the adversary
- it measures latency differences by detecting a slowing down in the download

Congestion Attacks

A practical congestion attack can be mounted as follows

- an adversary controls an exit node
- it wants to confirm that a target client uses a specific entry node
- the exit node injects some JavaScript code into an HTML response being delivered to the target
- the JavaScript code causes the target's browser to send HTTP requests at short regular intervals
- the HTTP requests contain the time the request was sent
- this allows the attacker to measure arrival time without congestion

Congestion Attacks

Congestion attack continued

- the attacker creates congestion by creating a circuit from a client it controls
- it is a long circuit of length m that repeatedly includes the entry node being tested
- a relay cannot extend a circuit to the previous relay
- thus two high bandwidth relays are used to create a larger loop
- $m = 24$ was determined to be effective
- Tor consequently limited the length of circuits to 8
- the adversary now needs multiple circuits to congest the node being tested

Timing Attacks

Timing attacks are also de-anonymization attacks

- during a timing attack, the adversary manipulates the entry and exit nodes of the target user
- the adversary correlates patterns in traffic flow from the entry node to traffic flow to the exit node
- this allows the attacker to determine the server the client is communicating with

Timing Attacks

One attack uses congestion control behavior of TCP

- it is possible to signal congestion to TCP
- it will scale down the congestion window making transmission slower
- a significant slowdown of the tested server is detectable by the adversary

Another attack uses autonomous systems (AS) to uncover a target

- this attacks uses network maps of ingress and egress routers of ASes
- bandwidth is varied resulting in predictable patters

Denial of Service Attacks

Denial of service attacks flood the network resource of a user

- the goal may not be to de-anonymize a user
- it might be to make a victim's connection very slow or unavailable
- it can also be used to force honest users to use malicious relays

Denial of Service Attacks

An example of this type is the Sniper attack

- it can be used to anonymously disable arbitrary Tor relays
- it exploits Tor's congestion and flow control mechanisms
- the target node is used as the entry node
- the attacker starts two very large downloads over the circuit
- the attacker sends messages to the exit node to maintain the dataflow
- it, however, does not read the arriving data from the entry node
- the Tor process becomes killed on the entry node by the OS

Fingerprinting Attacks

In a fingerprinting attack, an adversary relies on the fact that traffic often has distinct characteristics

- this can be used to identify which webpage a client is requesting
- or to gain knowledge about the path traffic traverses in the network
- or to determine if a client is connecting to a hidden service

Fingerprinting Attacks

One example is website fingerprinting

- the attack assumes access to the entry node of a victim and otherwise requires little resources
- a typical webpage consists of many different files
- each file is typically downloaded through a separate TCP connection
- the number and size of the files can form a unique fingerprint
- the attacker records the size of each file the victim receives
- it compares the collected data

Fingerprinting Attacks

Fortunately, Tor design makes this attack difficult to carry

- Tor employs fixed sized data cells (512 bytes)
- this makes it difficult for an attacker to determine the precise file size
- Tor combines all TCP streams into a single connection
- this make it difficult for an attacker to distinguish different files
- the second characteristic is most effective in deterring this attack

Sybil Attacks

Sybil attack is a supplemental attack that makes other attacks easier

- in 2010, the number of active relays suddenly increased
- someone set up several hundred Tor relays on PlanetLab machines
- the danger is with an attacker having a disproportionally large influence on the network
- this has direct impact on anonymity of users

Summary

A large number of attacks on Tor have been developed over the years

Mitigations are added as attacks get discovered

Perfect protection is not achievable