#Rough Draft1

**Deanonymizing Techniques:**

**The Sniper Attack:** The Sniper Attack, an extremely low cost but highly destructive denial of service attack against Tor that an adversary may use to anonymously disable arbitrary Tor relays. The attack utilizes valid protocol messages to boundlessly consume memory by exploiting Tor’s end-to-end reliable data transport. The attack enables the deanonymization of hidden services through selective denial of service by forcing them to choose guard nodes in control of the adversary.

**Website Fingerprinting:** This attack demonstrates that a *local passive* adversary observing the (SSH, IPsec, or Tor) encrypted traffic is able, under certain conditions, to identify the website being visited by the user. The attacker tries to emulate the network conditions of the monitored clients by deploying his own client who visits websites that he is interested in classifying through the live network. During this process, the attacker collects the network traces of the clients. Then, he trains a supervised classifier with many identifying features of a network traffic of a website, such as the sequences of packets, size of the packets, and inter-packet timings. Using the model built from the samples, the attacker then attempts to classify the network traces of users on the live network.

**Torben:** A novel deanonymization attack against Tor. The attack is based on an unfortunate interplay of technologies: (a) web pages can be easily manipulated to load content from untrusted origins and (b) despite encryption, low latency anonymization networks cannot effectively hide the size of request-response pairs. Torben operates entirely on the application layer and does not require Tor nodes or routers to be controlled by the adversary.

**Caronte:** CARONTE, a tool to automatically identify location leaks in hidden services. CARONTE implements a novel approach that does not rely on flaws on the Tor protocol and assumes an open world, i.e., it does not require a short list of candidate servers known in advance. CARONTE visits the hidden service, extracts Internet endpoints and looks up unique strings from the hidden service’s content, and examines the hidden service’s certificate chain to extract candidate Internet endpoints where the hidden service could be hosted. Then, it validates those candidates by connecting to them.

**Deanonymizing Techniques (for Investigations):**

**Techniques Based on Traffic Analysis:** Deanonymization techniques that leverage traffic analysis usually rely on the ability to observe nodes participating in the anonymity network and record traffic features on their incoming and outgoing links, including, for example, the volume and timing of network packets.

An example of such an approach is the **Packet-Counting attack**, which requires a very low degree of precision.

More invasive approaches consist of injecting a traffic perturbation pattern on one end of a connection, such as an HTTP connection to a hidden server under investigation, with unique characteristics, such as, for example, by applying a “square wave” pattern to the output transfer rate of an HTTP request.

**Future Development** - Among other variants of traffic analysis techniques that are being researched, a method that relies on the ability to fingerprint both the presence of nodes and hidden service availability over time is being developed and will be presented by Simioni et al. Such an approach does not require the deployment of expensive high-resolution traffic monitors and demonstrates how it is possible to extract simple time-based correlations that enable the deanonymization of a hidden service.

**Exploitation of Implementation Vulnerabilities:** Exploiting the vulnerabilities discovered in an anonymity network protocol or application layer implementation has been proven to be an effective approach for discovering the IP addresses of users or servers connected to anonymity networks along with information on their online activity.

**The “relay early” traffic confirmation attack**, a vulnerability discovered in the Tor protocol that allowed a Tor relay to forge one of the Tor protocol headers at one end of a circuit. By leveraging this header information as a signal for tagging Tor circuits, security researchers were able to deanonymize several users of the Tor network.

An implementation vulnerability was discovered by Exodus Intelligence, and it affected the I2P network. The security firm discovered several XSS vulnerabilities in the I2P router configuration web interface, and the exploitation of these weaknesses allowed the firm to abuse the I2P plugin framework to reveal the IP address of its user.

**Exploitation of Bad Operational Security Practices:** (Case Study)

1 -Ross Ulbricht, the creator of Silk Road, the most popular marketplace that leveraged anonymity networks to enable traffic of illegal goods and services,6 was identified because of bad operational security practices. Ulbricht started the first known posts about Silk Road using his personal email addresses and aliases, which were, in turn, traceable to his real identity.

2 - A case of bad operational security led to the takedown of another popular marketplace, AlphaBay. It has been detailed how, during investigations, authorities found an email address in the protocol headers of emails sent to users of AlphaBay who had forgotten their passwords. They were able to eventually trace that email address to the individual who allegedly administered the marketplace.

**Securing TOR against Deanonymization exploits:**

A diagram of a computer process

Description automatically generated

**Selfrando:** an enhanced and practical load-time randomization technique for the Tor Browser that defends against exploits, such as the one FBI allegedly used against Tor users.

**-Practical Randomization Framework**

**-Increased Entropy and Leakage Resilience**

**-Hardening the Tor Browser**