Concordia University
FACULTY OF ENGINEERING AND COMPUTER SCIENCE

Project Plan for INSE-6610
Cybercrime Investigations

Project Title:

Tor/Onion Hidden Service Deanonymization Techniques - Survey

Presented to:
Dr. Ivan Pustogarov

Presented by:

Riya Vinodbhai Patel	40224858
Anita Francis Archibong	27729790
Rahul Hulli	40234542
Sanchit Smarak Behera	40230269
Jubin Nirmal	40235087
Ugochukwu Kizito Ugwu	40244315

Table of Contents

Introduction

The Dark Web remains an enigmatic and complex realm on the internet, fostering a hidden ecosystem for various activities, including cybercrime and illicit trade. To navigate this secretive landscape, individuals and organisations often rely on Onion services hosted on the Tor network, which provide anonymous access and enhanced privacy. However, this cloak of anonymity is not impervious to the scrutiny of deanonymization techniques employed by adversaries, researchers, and law enforcement agencies.

Our Cybercrime Investigation project embarks on a captivating journey to explore the complexities of the Dark Web and the vulnerabilities associated with Onion services. Through a comprehensive survey, we will investigate Tor/Onion Hidden Service Deanonymization Techniques. By analysing six distinct techniques, namely the RAPTOR Attack, Shadow Attacks, Traffic Correlation, Website Fingerprinting, Sybil Attacks, and Intersection Attacks, we seek to unravel the mechanisms that compromise the anonymity of Onion services, contributing to the enhancement of cybersecurity in the digital landscape.

Problem Statement

The Dark Web poses unique challenges for cybersecurity, as it provides anonymous access to various illicit activities. Onion services hosted on the Tor network offer a veil of anonymity, making them attractive to threat actors seeking to operate undetected. However, the effectiveness of this anonymity is constantly tested by deanonymization techniques employed by cybercriminals, researchers and law enforcement agencies.

The goal of this project is to conduct a comprehensive survey on the Tor/Onion Hidden Service Deanonymization Techniques. By analysing six distinct techniques, namely the RAPTOR ATTACK, Shadow Attacks, Traffic Correlation, Website Fingerprinting, Sybil Attacks, and Intersection Attacks, we seek to unravel the mechanisms that compromise the anonymity of Onion services.

Project Scope and Deliverables

Our Cybercrime Investigation will delve into the following aspects:

1. **Survey and Research:** Conduct an extensive survey of existing deanonymization techniques used to uncover the identity and location of Onion services. Thoroughly research academic papers, research articles, and cybersecurity publications to gather relevant data.
2. **Methodology Selection**: Identify and select a diverse set of deanonymization techniques to be analysed during the project. These techniques will form the basis for our experimentation and evaluation.

3. **Experiment Design**: Design a structured experiment to implement and test each selected deanonymization technique. Create a controlled environment to ensure accurate results and reproducibility.
4. **Data Collection and Analysis**: Implement the chosen deanonymization techniques against our own Onion service in the controlled environment. Collect data and analyse the outcomes to evaluate the effectiveness and impact of each technique.
5. **Documentation:** Thoroughly document the survey methodology, experimental setup, data collected, and analysis performed. Prepare comprehensive reports for each deanonymization technique, detailing the results and observations.
6. **Recommendations:** Based on the findings of the survey and experimentation, formulate strategic recommendations to enhance the security and anonymity of Onion services against the analysed deanonymization techniques.

Timeline and Milestone for the project

Week 1: Survey and Research

- Conduct literature review and gather relevant research on Tor/Onion Hidden Service Deanonymization Techniques.
- Identify a diverse set of deanonymization methods for further analysis.

Week 2: Experiment Design

- Design a structured experiment to implement each selected deanonymization technique.
- Set up a controlled environment for experimentation.

Weeks 3-5: Implementation and Testing

- Implement the chosen deanonymization techniques against our Onion service.
- Conduct thorough testing and record the obtained results.

Week 6: Data Analysis and Documentation

- Analyse the data collected during the experimentation phase.
- Document the results, observations, and any challenges encountered.

Week 7: Report and Recommendations

- Prepare comprehensive reports for each deanonymization technique analysed.
- Formulate strategic recommendations to improve Onion service security against the identified vulnerabilities.

Resources

1. **Tor Project:** Official website with information about the Tor network and Onion services.
2. **Research Papers and Articles:** Academic publications and cybersecurity literature on deanonymization techniques.
3. **Experimentation Environment:** Virtual machines or controlled networks for secure and accurate testing.

Budget

As this project will be a general case study, we will not face any budget spending. Other than the cost of printing, we do not expect to see any potential costs for this project.

Conclusion

By undertaking this survey on Tor/Onion Hidden Service Deanonymization Techniques, our Cybercrime Investigation project aims to contribute valuable insights to the field of cybersecurity. We seek to deepen our understanding of the threats posed to Onion services and formulate effective strategies to safeguard against deanonymization attacks. Our exploration of the complexities of the Dark Web and the vulnerabilities associated with Onion services will foster a deeper understanding of the digital landscape, contributing to a safer online environment.

References

[1] S. Farrell and H. Tschofenig, "Security and privacy threat analysis for the Internet of Things (IoT)," Internet-Draft, draft-farrell-iotsi-threat-01, 2014.