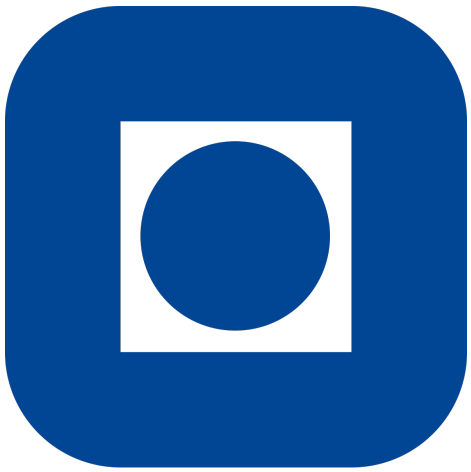
Project Plan Group R5

Andreas Handal Hellesnes, Lars Meland, Ole André Hauge, Sander Stamnes Karlsen, and Sylwia Harewska.



NTNU

September 20, 2021

Silk Road - A Case Study of Anti-forensic Techniques for Internet Crime

This document is a project plan for the term paper on "Silk Road - A Case Study of Anti-forensic Techniques for Internet Crime". It clarifies what methods will be used and contains a project description, project plan, and foreseen references for the topic.

The document is subject to change due to the early stage of the research. This includes, but is not limited to, the number of pages, references, meeting- and delivery times.

Project description

The project aims to describe, analyze and evaluate anti-forensics strategies used by users of the Dark Web to stay hidden and anonymous. This will be accomplished by focusing on one of the most popular websites on the Dark Web, at least by the public, namely the Silk Road website. Silk Road is a website that was initially created in February 2011 as an anonymous online marketplace for sales and distribution of illegal substances; primarily narcotics. The FBI and Europol have taken it down twice since its launch, and the creator has been arrested. The third version of the website is said to still be active.

The project will produce a paper that answers the research question:

> What anti-forensics methods are used to stay hidden and anonymous on the Silk Road Dark Web website and what are their efficacy, downsides, and how can they be used?

With this in mind, we want to learn more about how the website protects its users' privacy.

Expected result

Answering the question the paper will confirm whether the Silk Road website is still online, and provide an analysis and evaluation of the anti-forensics techniques that are in use, as well as the internal security policies employed by the admin to help ensure the security and anonymity of the users. The reader will gain a better understanding of anti-forensics strategies and how they are used by actors by examining how this is done in a real-life case. This includes knowledge about how they can be used, as well as their efficacy and downsides.

Methodology

The case study's general research strategy is based on a systematic literature review, which mostly consists of modern, western, and peer-reviewed publications, as well as news outlets. The literature comes from the disciplines of information technology, information security, computer science, political science, social science, and the law information. The IEEE referencing style is used for reference.

The *WEIRD-phenomenon* (western, educated, industrialized, rich, and democratic) may have an impact on the deductions within the sub-topics and restrict our conclusions (Azar, 2010, pp. 11). The group must be aware of this.

Project plan

- Introduction (1 page, 2 weeks) Ole André Hauge
    1. An overview of the topic covering anti-forensics and the Silk Road website.
    2. The relevance of the study and a presentation of research question.
- Methodology (1-2 pages, 2-4 weeks) Andreas Hellesnes
    1. An overview of what and how the results were found.
- Results (4-6 pages, 6-8 weeks) Lars Meland and Sylwia Harewska
    1. Case study - Silk Road
        (a) Identified techniques and policies
        (b) Examination of findings: efficacy, etc...
- Discussion (3-5 pages, 6-8 weeks) Sander Karlsen and Andreas Hellesnes
    1. Evaluation of techniques found in the case study.
        (a) How can they be used?
        (b) Pros and cons of techniques and policies
        (c) What are their effect?
        (d) What are their downsides?
- Conclusion (0.5-1 page, 2 weeks) Ole André Hauge

Project members

The group has decided to give Ole Hauge the role of the groups' coordinator. He will be responsible for the collaboration, meetings, follow-up on the progress, keep the red thread of the paper, structure and deliver the final documents and other deliverables. The coordinator is also responsible for writing the introduction and conclusion of the paper. The methodology chapter will be written by Andreas Hellenes, while Lars Meland and Sylwia Harewska will write the result chapter. Sander Karlsen and Andreas Hellenes will structure the discussion.

The group will have mandatory meetings on the weekends before important deadlines. The dates are given in table 1. More meetings can be added if needed by the group. The meetings intend to coordinate the implementation of each sub-topic, briefly review the content, identify the potential for improvement and adjust accordingly.

Nr	Date	Description
1	26.09.2021	Discuss the writing of the paper
2	24.10.2021	Discuss the presentation
3	14.11.2021	Prepare for presentation and final delivery

Table 1: Group Teams-meetings

The important dates, milestones, and deadlines for the group project are given in table 2.

Nr	Date	Description
1	23-24.11.2021	Presentation delivery
2	26.11.2021	Final paper delivery

Table 2: Important deadlines

The group will use Teams as the main platform for internal communication. With this platform, the members can chat, post about their sub-topics, share sources and ideas, request meetings, or have questions forwarded to the professor by the group coordinator. Furthermore, the group will use Overleaf as a text editor. The documents in Overleaf are shared and open to all group members, enabling the group to work simultaneously and have access to each other's work.

The group members are to deliver a short report by each Sunday to the group coordinator, who will turn it into an update post to inform the group about the overall progress, thus enabling support to those that might need assistance.

Foreseen References

1. Årnes, A. (2018) *Digital Forensics*. Norway: Wiley, 2018.
2. Kumar, A. and Rosenbach, E. (2019) *The Truth about the Dark Web*. [online] Available at: `https://www.imf.org/external/pubs/ft/fandd/2019/09/the-truth-about-the-dark-web-kumar.htm/` [Accessed 13 September 2021].
3. Lacson, W. and Jones, B. (2016) *The 21st Century DarkNet Market: Lessons from the Fall of Silk Road*. [online] Available at: `http://www.cybercrimejournal.com/Lacson&Jonesvol10issue1IJCC2016.pdf/` [Accessed 13 September 2021].
4. Mireca, M., Wang, V. and Jung, J. (2018) *The not so dark side of the darknet: a qualitative study*. [online] Available at: `https://d-nb.info/1168586542/34/` [Accessed 13 September 2021].
5. Zajácz, R. (2017) *Silk Road: The market beyond the reach of the state*. [online] Available at: `https://clas.uiowa.edu/commstudies/sites/clas.uiowa.edu.commstudies/files/Zajacz_SR16_proofs.pdf/` [Accessed 13 September 2021].
6. Myra Security (2021) *What is the Tor network?*. [online] Available at: `https://www.myrasecurity.com/en/tor-network//` [Accessed 13 September 2021].
7. Shim, T. (2021) *How to Access the Dark Web: Guide to Browsing Dark Web using TOR Browser*. [online] Available at: `https://www.webhostingsecretrevealed.net/blog/web-tools/tourist-guide-to-dark-web-accessing-the-dark-web-tor-browser-and-onion-websites/` [Accessed 13 September 2021].
8. Leyden, J. (2021) *Tor security: Everything you need to know about the anonymity network*. [online] Available at: `https://portswigger.net/daily-swig/tor-security-everything-you-need-to-know-about-the-anonymity-network/` [Accessed 13 September 2021].

9. Dipiero, C. (2017) *Deciphering cryptocurrency: Shining a light on the deep dark web.* University of Illinois Law Review. 1267-1299. [online] Available at: `https://www.illinoislawreview.org/print/vol-2017-no-3/deciphering-cryptocurrency/` [Accessed 17 September 2021].

10. Shekhtman, L. et. al. (2020) *Percolation framework reveals limits of privacy in Conspiracy, Dark Web, and Blockchain networks.* [online] Available at: `https://arxiv.org/abs/2007.05466` [Accessed 17 September 2021].

11. Hiller, J. et. al. (2019) *Tailoring Onion Routing to the Internet of Things: Security and Privacy in Untrusted Environments,* 2019 IEEE 27th International Conference on Network Protocols (ICNP), pp. 1-12, doi: 10.1109/ICNP.2019.8888033.

12. Elgzil, A. et. al. (2017) *Cyber anonymity based on software-defined networking and Onion Routing (SOR),* 2017 IEEE Conference on Dependable and Secure Computing, pp. 358-365, doi: 10.1109/DESEC.2017.8073856.

13. Goanta, C. (2020) *The Private Governance of Identity on the Silk Road*[online] Available at: `https://www.frontiersin.org/articles/10.3389/fbloc.2020.00004/full` [Accessed 17 September 2021].