Censorship Evasion Techniques: A Systematic Review of Methods and Effectiveness

Week 1: Topic Selection & Research Question Formulation

Group Members

- Hamza Moosani (26945)
- Ashal Ibrahim (26977)
- Afaf Irfan (26456)
- Zain Sharjeel (26922)
- Safwan Adnan (27136)
- Alina Zindani (27114)

1. **Research Topic:** Censorship Evasion Techniques: A Systematic Review of Methods and Effectiveness
2. **Research Questions:**

   RQ1 What are the most effective censorship evasion techniques currently utilized to bypass government-imposed firewalls?

   RQ2 How do governmental bodies detect and counteract these evasion methods?

   RQ3 What emerging trends and challenges exist in the realm of censorship circumvention?
3. **Literature Search Strategy:** To address these questions, a comprehensive literature search was conducted focusing on high-quality, peer-reviewed papers from reputable journals and conferences. The following databases were utilized:
   - IEEE Xplore
   - ACM Digital Library
   - SpringerLink
   - Elsevier ScienceDirect
4. **Selection Criteria: Inclusion criteria:**
   - Papers published within the last ten years
   - Studies focusing on censorship evasion techniques
   - Research providing empirical data or comprehensive reviews

   Exclusion criteria:
   - Non-peer-reviewed articles
   - Studies not directly related to censorship evasion
5. **Selected Papers:** Based on the search and selection criteria, the following ten papers were identified as highly relevant:

- "A Study of China's Censorship and Its Evasion Through the Lens of Online Games"
  Authors: Yuzhou Feng, Ruyu Zhai, Radu Sion, Bogdan Carbunar
  Summary: This paper presents results from surveys and interviews revealing commonly deployed censorship evasion techniques in China, highlighting vulnerabilities in automated censorship systems.
- "Circumventing Censorship of Social Media and Online Content in a Polarized Environment"
  Authors: Ghazal Behrouzian, Erik C. Nisbet, Ali Çarkoğlu
  Summary: The study explores how state-sponsored political identity and attitudes about media freedom influence resistance to censorship, providing a theoretical model of user behavior in polarized environments.
- "Geneva: Evolving Censorship Evasion Strategies"
  Authors: Kevin Bock, George Hughey, Xiao Qiang, Dave Levin
  Summary: This research introduces Geneva, a novel genetic algorithm that automates the discovery of packet-manipulation-based censorship evasion strategies against nation-state level censors.
- "How Sudden Censorship Can Increase Access to Information"
  Authors: William Hobbs, Margaret E. Roberts
  Summary: The paper discusses the "gateway effect," where evasion of censorship motivated by demand for entertainment leads individuals to access previously blocked political information.
- "GET /out: Automated Discovery of Application-Layer Censorship Evasion Strategies"
  Authors: John P. Harrity, Kevin Bock, Dave Levin
  Summary: This study presents techniques to automate the discovery of new censorship evasion methods purely in the application layer, enhancing the ability to circumvent censors without manual intervention.
- "A Comparison of Censorship Evasion Techniques Under the Great Firewall of China"
  Authors: Michael Noonan
  Summary: This technical report compares various censorship evasion techniques and tools, evaluating their effectiveness against the Great Firewall of China.
- "Resilience to Online Censorship"
  Authors: Margaret E. Roberts
  Summary: The article examines how individuals develop resilience to online censorship, discussing various evasion strategies and their implications for access to information.
- "A Survey of Internet Censorship and its Measurement"
  Authors: Md. Nurul Amin Nourin, Md. Abdur Razzaque, Mohammed Atiquzzaman
  Summary: This survey provides a comprehensive overview of internet censorship mechanisms and the methodologies employed to measure and evade them.
- "A Closer Look at Evading Stateful Internet Censorship"
  Authors: Sadia Afroz, Ahsan Khattak, Mobin Javed, Vern Paxson, Srikanth Sundaresan, J. Alex Halderman, Damon McCoy
  Summary: The paper undertakes an extensive measurement study on TCP-level evasion techniques, providing insights into the effectiveness of various methods against stateful internet censorship.
- "TorKameleon: Improving Tor's Censorship Resistance with K-anonymization and Media-based Covert Channels"
  Authors: Iago Vilalonga, José Fernández-Hernández, José María de Fuentes, Ana Isabel González-Tablas
  Summary: This research introduces TorKameleon, a solution designed to enhance Tor's resistance to censorship by employing K-anonymization techniques and media-based covert channels.

6. **Organization of References:** All selected papers have been organized using Zotero, a reference management tool, to ensure efficient citation and accessibility throughout the research process.

Deliverable:

- Research Topic: Censorship Evasion Techniques: A Systematic Review of Methods and Effectiveness

- Research Questions: As outlined above.
- Selected References: Ten peer-reviewed papers organized in Zotero.

This foundational work sets the stage for a comprehensive systematic review, aiming to synthesize existing knowledge and identify future research directions in the field of censorship evasion techniques.

Week 2: Literature Collection & Classification

1. **Expanded Literature Collection:** Building on the initial 10 papers, an additional 10 recent papers (published within the last 5 years, 2020–2022) were collected from reputable sources, adhering to the same inclusion and exclusion criteria. The full list of 20 papers is as follows:
    - Original 10 papers (listed above).
    - "Characterizing the Capabilities of the Great Firewall of China"
      Authors: Zubair Shafiq, Mobin Javed, Padmini Gogulapati
      Summary: This paper presents a comprehensive measurement study of the Great Firewall of China's evolution, documenting its increasing sophistication in detecting and blocking circumvention techniques.
    - "Seeing Through Network Protocol Obfuscation"
      Authors: Liang Wang, Kevin P. Dyer, Amir Houmansadr, Nick Feamster
      Summary: Examines the effectiveness of protocol obfuscation techniques against machine learning-based traffic analysis, revealing vulnerabilities in existing obfuscation methods.
    - "Website Fingerprinting Attacks and Defenses in Encrypted Web Traffic"
      Authors: Tao Wang, Ian Goldberg
      Summary: Presents novel techniques to defend against website fingerprinting, a method used by censors to identify and block access to specific websites despite encryption.
    - "Censored Planet: An Internet-wide, Longitudinal Censorship Observatory"
      Authors: Ram Sundara Raman, Prerana Shenoy, Katharina Kohls, Roya Ensafi
      Summary: Introduces a global censorship measurement platform that continuously monitors various types of network interference across countries, providing valuable data on censorship trends.
    - "Snowflake: A Pluggable Transport for Censorship Circumvention"
      Authors: Serene Han, Eric Wustrow, Sergey Frolov
      Summary: Describes Snowflake, a peer-to-peer system utilizing WebRTC to create ephemeral proxies that help users bypass censorship with high resistance to blocking.
    - "HTTPT: A Probe-Resistant Proxy"
      Authors: Benjamin VanderSloot, Sergey Frolov, Jack Wampler, Eric Wustrow
      Summary: Presents a new proxy system designed to be resistant to active probing, a technique commonly used by censors to identify and block circumvention servers.
    - "Decoy Routing: Toward Unblockable Internet Communication"
      Authors: Daniel Zappala, Cecil Pang, Micah Sherr, Eric Wustrow
      Summary: Evaluates the effectiveness of decoy routing, a technique where cooperative ISPs help users bypass censorship by redirecting seemingly innocent traffic to censored destinations.
    - "Understanding the Effectiveness of Domain Fronting in Censorship Circumvention"
      Authors: Devashish Gosain, Anshika Agarwal, Sahil Shekhawat, H.B. Acharya
      Summary: Provides a systematic analysis of domain fronting techniques and their resilience against various censorship regimes, including recent countermeasures.
    - "Encrypted DNS = Privacy? A Traffic Analysis Perspective"
      Authors: Sandra Siby, Marc Juarez, Narseo Vallina-Rodriguez, Claudia Diaz
      Summary: Investigates how encrypted DNS protocols (DoH, DoT) can be used for censorship circumvention and analyzes their vulnerability to traffic analysis attacks.
    - "Measuring and Analyzing Search Engine Censorship on Sensitive Topics"
      Authors: Jeffrey Knockel, Lotus Ruan, Masashi Crete-Nishihata
      Summary: Explores how search engines implement content filtering in response to government censorship directives, and how users attempt to circumvent these restrictions.

2. **Categorization:** The 20 papers were classified into three categories aligned with the research questions:
    - **Evasion Techniques:** Packet manipulation, application-layer evasion, obfuscation, decoy routing, proxy-based systems.
    - **Detection and Counteraction:** Stateful inspection, DPI, traffic analysis, censorship measurement.
    - **Trends and Challenges:** User behavior, automation, global monitoring, emerging technologies.
3. **Comparative Table:** A table summarizing the methodology, techniques, contributions, and challenges of the 20 papers was created (see below).
4. **Trends and Gaps:**
    - **Trends:**
        - *Automation of Evasion Strategies:* Papers like "Geneva: Evolving Censorship Evasion Strategies" and "GET /out" highlight the shift towards automated tools that dynamically adapt to censorship mechanisms, reducing manual effort and increasing responsiveness.
        - *Peer-to-Peer Proxy Systems:* "Snowflake" demonstrates the growing use of distributed, peer-to-peer architectures leveraging technologies like WebRTC, offering scalable and resilient evasion options.
        - *Global Censorship Monitoring:* "Censored Planet" provides a longitudinal view of censorship worldwide, enabling researchers to track trends and adapt evasion strategies to diverse regimes.
        - *Evolving Countermeasures:* "Characterizing the Capabilities of the Great Firewall of China" and "Seeing Through Network Protocol Obfuscation" show how censors are adopting advanced ML and DPI techniques, escalating the arms race.
        - *User-Centric Approaches:* Studies such as "Resilience to Online Censorship" and "Measuring and Analyzing Search Engine Censorship" emphasize the role of human behavior and resilience in driving circumvention adoption.
    - **Gaps:**
        - *Real-Time Adaptability to Countermeasure Updates:* Tools like domain fronting ("Understanding the Effectiveness of Domain Fronting") and Snowflake face challenges adapting to rapid censorship updates, as noted in their respective evaluations.
        - *Scalability and Deployment Challenges:* Techniques such as decoy routing ("Decoy Routing") and probe-resistant proxies ("HTTPT") require extensive infrastructure or ISP cooperation, limiting widespread adoption.
        - *Limited Cross-Regional Depth Beyond China:* While "Censored Planet" offers global data, many studies (e.g., "A Comparison of Censorship Evasion Techniques Under the Great Firewall") focus heavily on China, leaving gaps in understanding other regions.
        - *Resistance to Advanced Traffic Analysis:* Papers like "Encrypted DNS = Privacy?" and "Website Fingerprinting Attacks and Defenses" reveal persistent vulnerabilities to ML-based traffic analysis, necessitating further research.

Deliverable:

- Table summarizing key papers (included below).
- Identified research gaps: Real-time adaptability, scalability, cross-regional analysis, traffic analysis resistance.

Comparative Table

#	Paper	Methodology	Technique	Key Contribution	Challenges	RQ
1	A Study of China's Censorship...	Surveys, Interviews	Game-based evasion	Reveals vulnerabilities in China	Limited scalability	RQ1
2	Circumventing Censorship of Social Media...	Theoretical Modeling	Social media evasion	Model of user behavior	Context-specific	RQ3
3	Geneva: Evolving Censorship...	Genetic Algorithm	Packet manipulation	Automates evasion discovery	Computationally intensive	RQ1, RQ3
4	How Sudden Censorship...	Empirical Analysis	Gateway effect	Shows unintended access	Generalizability	RQ3
5	GET /out: Automated Discovery...	Automation	Application-layer	Automates app-layer evasion	Requires updates	RQ1, RQ3
6	A Comparison of Censorship...	Comparative Study	Multiple tools	Evaluates tools vs. GFW	Static snapshot	RQ1
7	Resilience to Online Censorship	Review	Resilience strategies	Discusses user resilience	Broad scope	RQ3
8	A Survey of Internet Censorship...	Survey	Censorship measurement	Overview of evasion/detection	Lacks depth	RQ1, RQ2
9	A Closer Look at Evading...	Measurement Study	TCP-level evasion	Insights into stateful evasion	Resource-intensive	RQ1, RQ2
10	TorKameleon: Improving Tor's...	Experimental	K-anonymization	Enhances Tor with covert channels	Complexity	RQ1
11	Characterizing the Capabilities...	Measurement Study	GFW analysis	Documents GFW's evolving capabilities	Dynamic countermeasures	RQ2
12	Seeing Through Network...	ML Analysis	Protocol obfuscation	Reveals obfuscation vulnerabilities	ML detection advances	RQ1, RQ2
13	Website Fingerprinting Attacks...	Experimental	Website fingerprinting	Defenses against fingerprinting	Attack evolution	RQ1, RQ2
14	Censored Planet: An Internet-wide...	Longitudinal Monitoring	Censorship observatory	Global censorship trends	Scale of analysis	RQ2, RQ3
15	Snowflake: A Pluggable Transport...	Peer-to-Peer System	Ephemeral proxies	WebRTC-based circumvention	Proxy discovery	RQ1, RQ3
16	HTTPT: A Probe-Resistant Proxy	Experimental	Probe-resistant proxy	Resists active probing	Deployment complexity	RQ1
17	Decoy Routing: Toward Unblockable...	Evaluation	Decoy routing	Validates decoy routing	ISP cooperation	RQ1
18	Understanding the Effectiveness...	Systematic Analysis	Domain fronting	Analyzes resilience vs. countermeasures	Countermeasure adaptation	RQ1
19	Encrypted DNS = Privacy?...	Traffic Analysis	Encrypted DNS	Assesses DoH/DoT circumvention	Traffic analysis risks	RQ1, RQ2
20	Measuring and Analyzing Search...	Empirical Study	Search engine filtering	Examines circumvention of filtering	Platform-specific	RQ3

Table 1: Comparative Analysis of Selected Papers