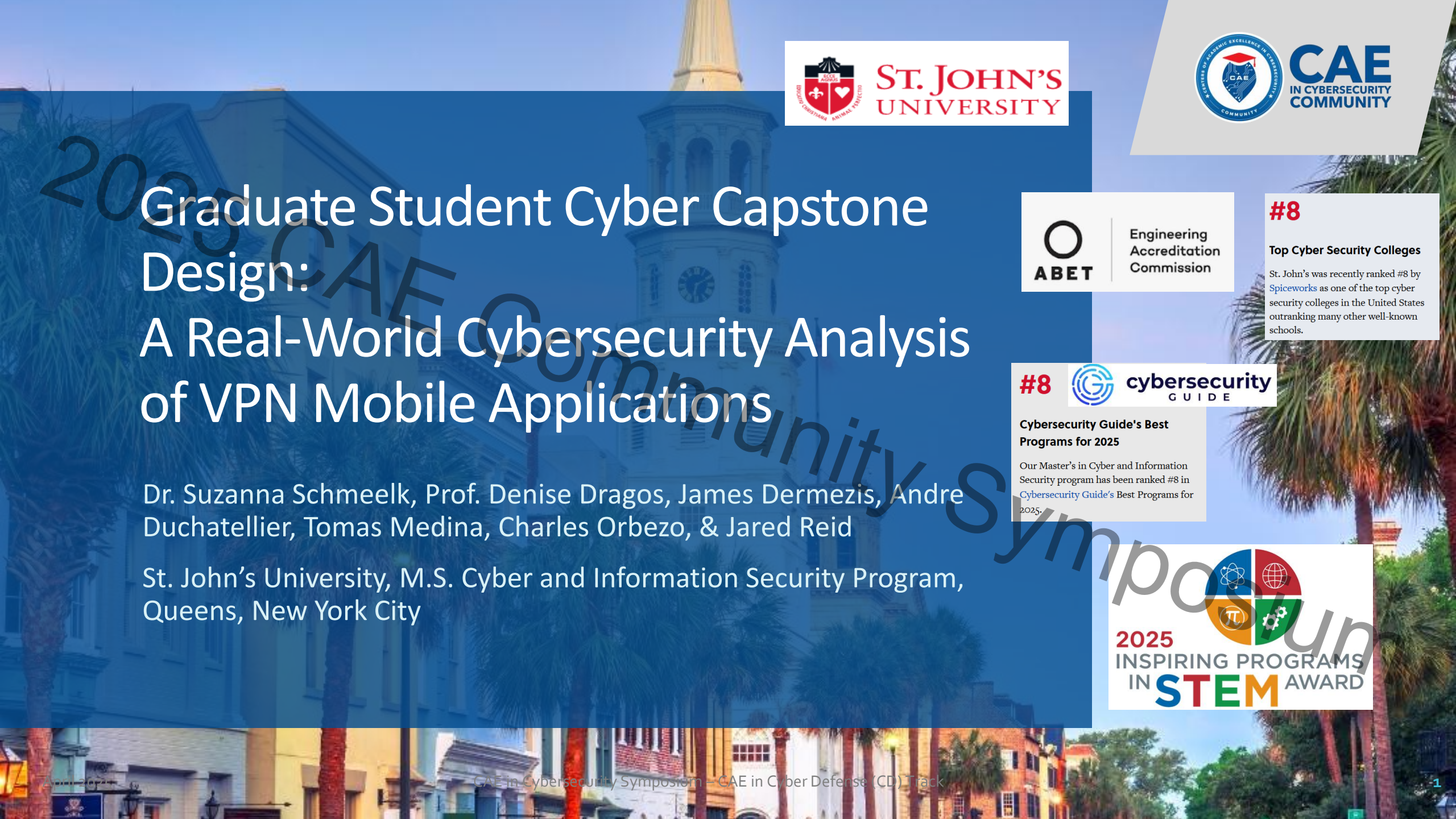


Graduate Student Cyber Capstone Design: A Real-World Cybersecurity Analysis of VPN Mobile Applications

Dr. Suzanna Schmeelk, Prof. Denise Dragos, James Dermezis, Andre Duchatellier, Tomas Medina, Charles Orbezo, & Jared Reid

St. John's University, M.S. Cyber and Information Security Program, Queens, New York City

Website: https://www.stjohns.edu/academics/programs/ms-cyber-and-information-security

Prof. Denise Dragos (Program Designer/Co-Founder)

- Education Experience
  - DPS in Computing Program (Current), Pace University
  - MS, Information Systems, Pace University
  - BS, Computer Science, Pace University
  - Criminal Justice, Nassau County Community College

- Industry Experience & Research
  - NYPD Computer Crimes Squad
  - KPMG's U.S. Forensic Advisory Services Manager
  - **Research:** Digital Forensics, Network Security, Intrusion Detection, Malware, Social Justice, and Curriculum development

Dr. Suzanna Schmeelk (Program Director/Co-Founder)

- Education Experience
  - DPS in Mobile Security, Pace University
  - Ed.D. in Mathematics Education, Rutgers University
  - M.S. Cybersecurity
  - + 4 M.S./M.B.A. Cyber-focused Advanced Degrees
  - B.S. Computer Science, Minor in Mathematics
- Industry Experience + Research
  - The City of New York
  - Bell Laboratories
  - Yahoo!, eBay
  - Sloan Kettering
  - **Research:** Secure Scripting, Risk Management, Machine Learning, Network Security, Healthcare Informatics Privacy/Security, Social Justice, and Curriculum development

A Graduate Research Capstone Course

1. Faculty-led Semester course
2. Graduate research students
    1. Work in small-groups and select a timely topic
        1. Many groups are heterogeneous groups of students
        2. Research paper and research readings captains
    2. Work and collect all aspects of the research project and deliver on (bi)weekly deliverables to LMS
    3. At key intervals of course, students incrementally transition their findings into LaTex (Overleaf) with conference/journal template
    4. All data analyzed is collected into LMS at key intervals
    5. Final products of the course include a dataset, paper, and presentation
3. Graduate research students are optionally provided an IRB-Approved survey about the course at end of course to gain insights for the next iterations of the course and curricular research.

Reporting on one capstone project results

, James Dermezis, Andre Duchatellier, Tomas Medina, Charles Orbezo, & Jared Reid

Abstract

A Virtual Private Network (VPN) is a logical network that uses encryption and tunneling to allow users to access networks privately and securely.

VPN usage has been increasing, with 46% of Americans using VPN's in 2024.

Since VPN's are security tools, it stands to reason that the VPN's themselves should be secure.

This analysis will explore and evaluate the security of 27 VPN applications based on their use of data collection, logging, random number generators, and permissions.

Applications will be analyzed by scanning their APK files with Mobile Security Framework (MobSF).

Background/ Introduction: Usage statistics

A 2024 study found that 46% of Americans use VPN's.

- This is a 7% increase from 2023.

The majority of VPN users are college-educated

The largest age demographic of VPN users are adults from the age of 45-60.

NordVPN is currently the most popular VPN, making up 27% of the market, although many competitors exist.

The number of individuals who use paid VPN services and the number of individuals who use free VPN's are roughly equal.

- Paid VPN applications refere to those that charge either a one-time fee or a subscription to use.
- VPN applications that monetize using advertisements and/or in-app purchases are considered "free".

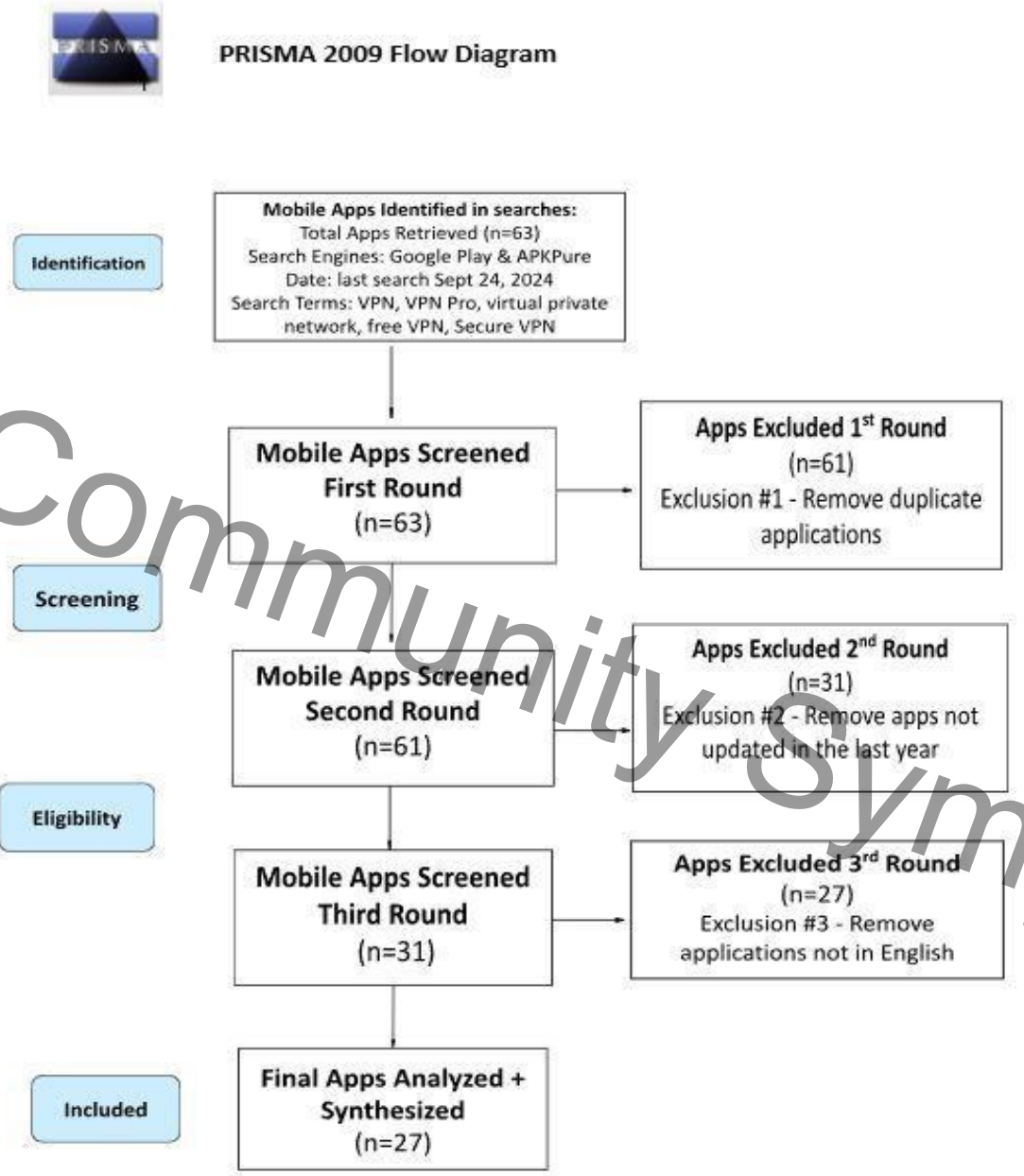
Literature Review in different related domains of research

VPN Research (focus on security)

Static Analysis (focus on mobile)

Mobile Application Security

Methodology



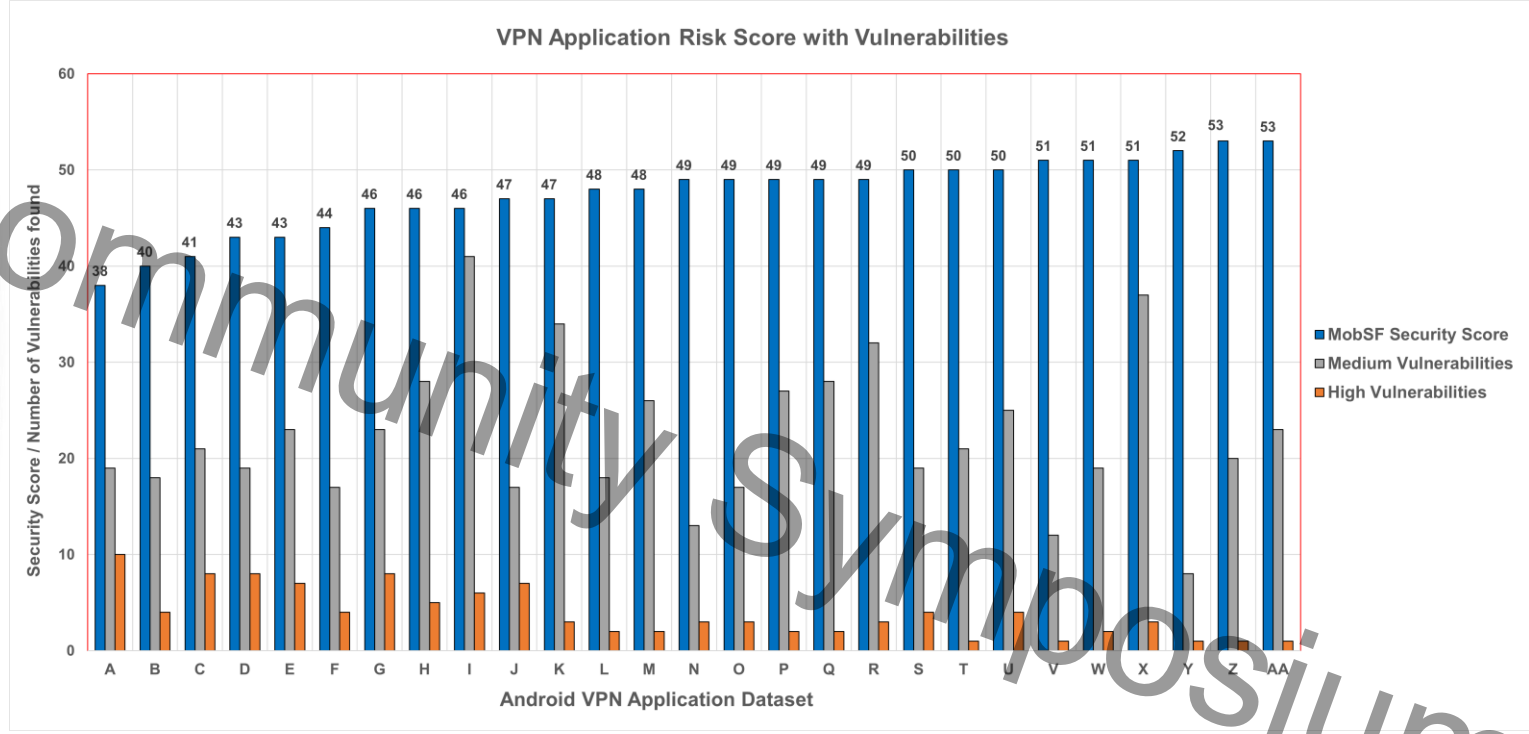
Methodology

(Best Practices for Developers)

- Category #1: Clear Text Traffic
- Category #2: Sensitive Information Logging
- Category #3: Insecure RNGs
- Category #4: Permissions
- Category #5: Exported Components

Findings & Results

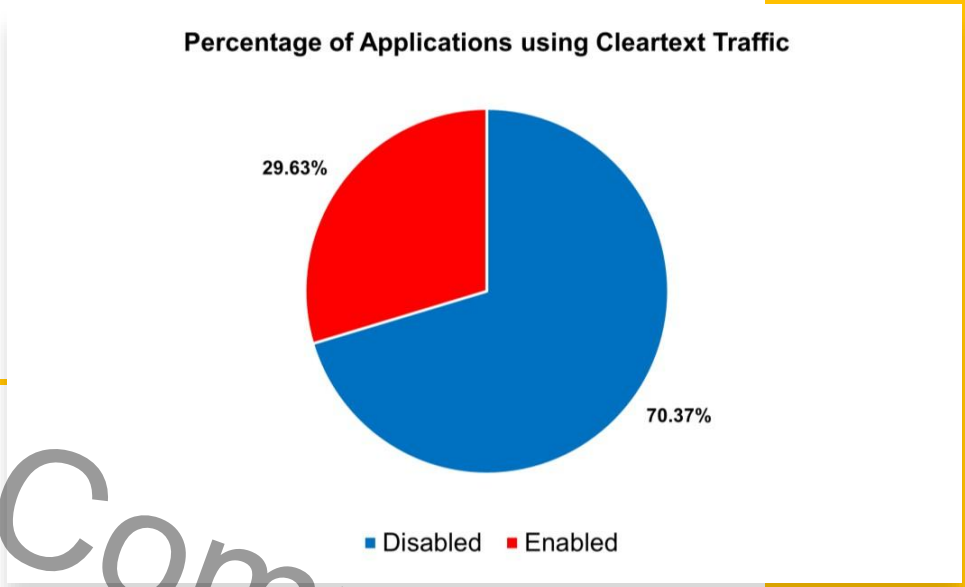
- 96% (26 out of 27) of the VPN applications in our dataset were given a risk score of B by MobSF.
- One application in our dataset was given a risk score of C.
- The average numerical security score given by MobSF was about 47.5/100.
- MobSF identified an average of 22.4 medium and 3.9 high vulnerabilities per application across our dataset.

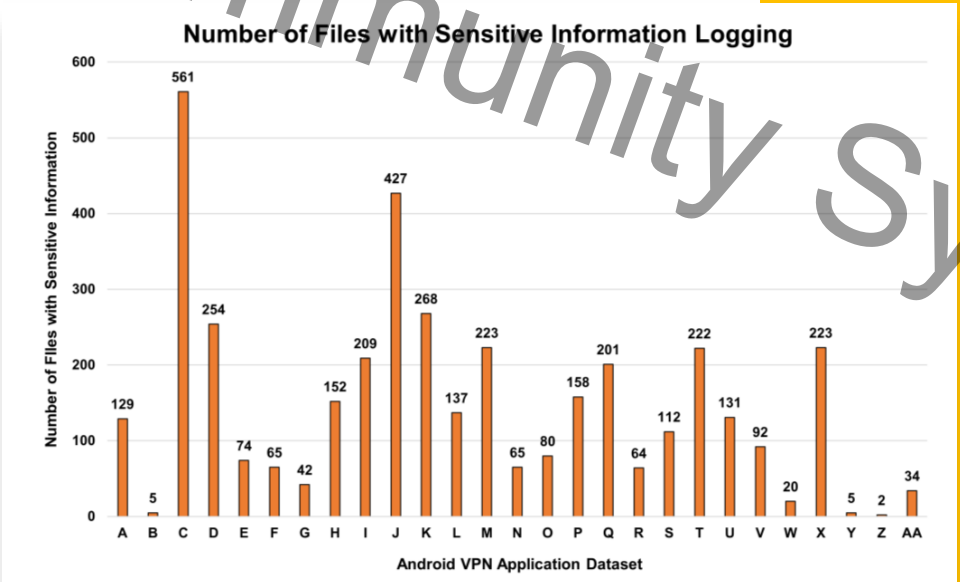


Findings & Results

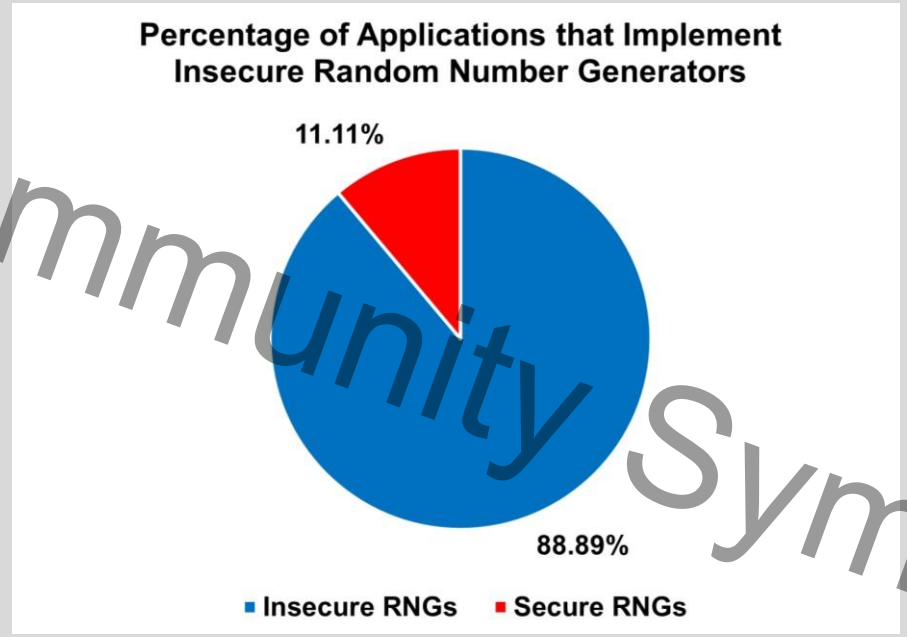
Category #1
Cleartext

Category #2
Sensitive Info Logging





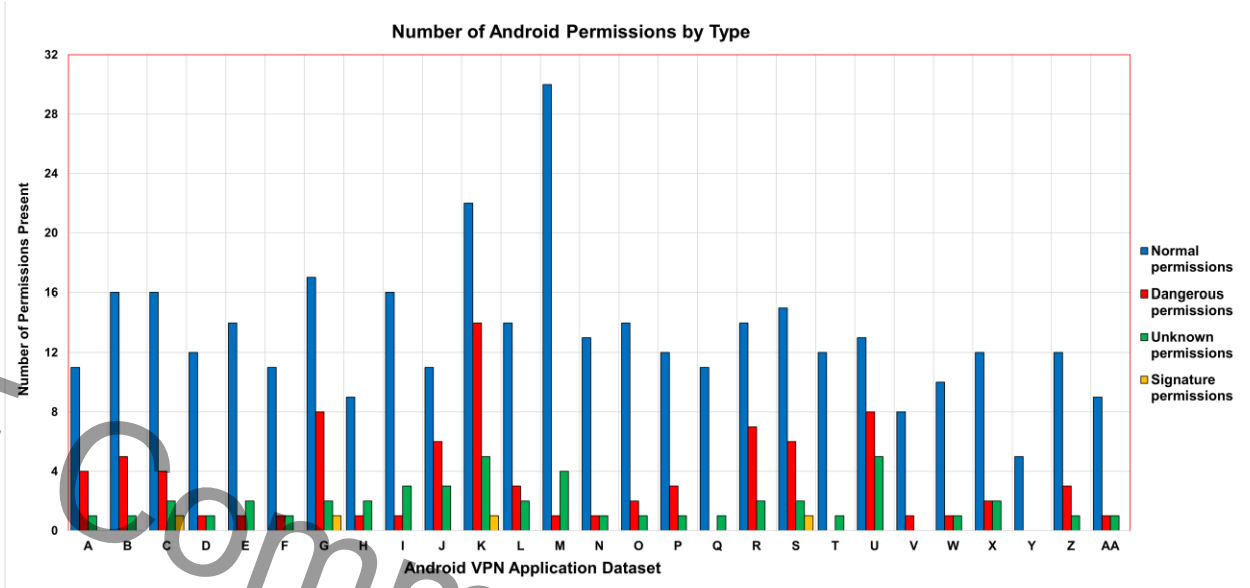
Category #3: Insecure Random Number Generators

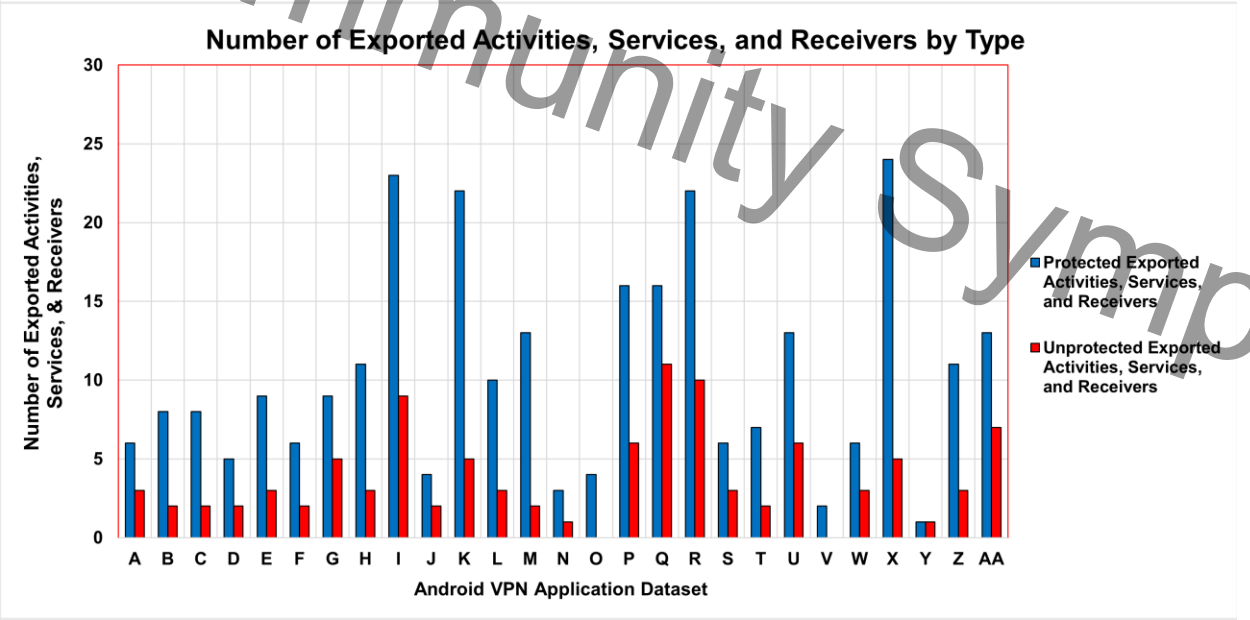


Findings & Results

Category #4: Android Permissions

Category #5: Exported Components





Limitations and Future Research

- Static analysis is limited in scope
- MobSF does not use detailed descriptions.
- MobSF reports provide little to no insight on the user experience. For example, while MobSF lists an application's permissions, the transparency of said permisions can only be determined by using the application.
- Future studies could elaborate on these findings.

Conclusion

- VPN applications have decent security, but there is room for improvement.
- MobSF gave the majority of applications a "B" rating. Noapplications received an "A" rating.
- Nearly all VPN applications had the following vulnerabilities:
  - Use of dangerous permissions unrelated to functionality.
  - Use of insecure random number generators.
  - Logging of sensitive data
- At the bare minimum, a VPN only requires access to network-related functions, so many
  of these vulnerabilities are avoidable.
- All data was collected with publicly available tools. Therefore, it stands to reason that both threat actors and developers can easily learn of these vulnerabilities.

Bibliography & Analysis Data Quality Assurance

- Total Citations: 33
- [1]J. Klein, "A Journey Through Android App Analysis: Solutions and Open Challenges," *Proceedings of the 2021 International Symposium on Advanced Security on Software and Systems*, May 2021, doi: https://doi.org/10.1145/3457340.3458298.
- [2]B. Mishra *et al.*, "Privacy Protection Framework for Android," *IEEE Access*, vol. 10, pp. 7973–7988, 2022, doi: https://doi.org/10.1109/access.2022.3142345.
- [3]G. Xu *et al.*, "Research on Cryptographic Misuse Detection for Android Applications Based on Dynamic and Static Combination," *Research on Cryptographic Misuse Detection for Android Applications Based on Dynamic and Static Combination*, Nov. 2023, doi: https://doi.org/10.1145/3603273.3634708.
- [4]M. Ikram, N. Vallina-Rodriguez, S. Seneviratne, M. A. Kaafar, and V. Paxson, "An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps," *Proceedings of the 2016 ACM on Internet Measurement Conference - IMC '16*, 2016, doi: https://doi.org/10.1145/2987443.2987471.
- [5]S. Seraj, Siavash Khodambashi, M. Pavlidis, and Nikolaos Polatidis, "MVDroid: an android malicious VPN detector using neural networks," *MVDroid: an android malicious VPN detector using neural networks*, Apr. 2023, doi: https://doi.org/10.1007/s00521-023-08512-1.

Ensuring bibliography and analysis data quality is critical because:

- It **establishes credibility**: Research backed by high-quality sources and data gains trust.
- It **enhances reliability**: Accurate, complete, and consistent data leads to valid conclusions.
- It **avoids misinformation**: Poor-quality sources or flawed data can result in erroneous findings.
- It **facilitates reproducibility**: Proper citations and quality data allow others to verify and replicate the work.