NOVA SOUTHEASTERN UNIVERSITY

4th Annual College of Computing, AI, and Cybersecurity Research Symposium, Nova Southeastern University (NSU)

CYBERSECURITY KEYNOTE PRESENTATION

Privacy and Security Matters Related to College Students' App Usage

Examining third-party data harvesting, location tracking, and mobile security paradigms in higher education.

Dr. Richard Maiti, Ph.D., MBA

Associate Professor of Computer Science | Kentucky State University

NSU Ph.D. Alumnus Class of 2016

PRESENTER BACKGROUND

NSU Graduate (2016)

About the Researcher: Dr. Richard R. Maiti

NSU Academic Root

Ph.D. in Information Systems (2016)

Nova Southeastern University College of Engineering and Computing.

Cybersecurity Focus

Prior Mobile & Social Media Work

Published privacy research in IEEE SoutheastCon 2021 & DevSecOps in CSCI 2024.

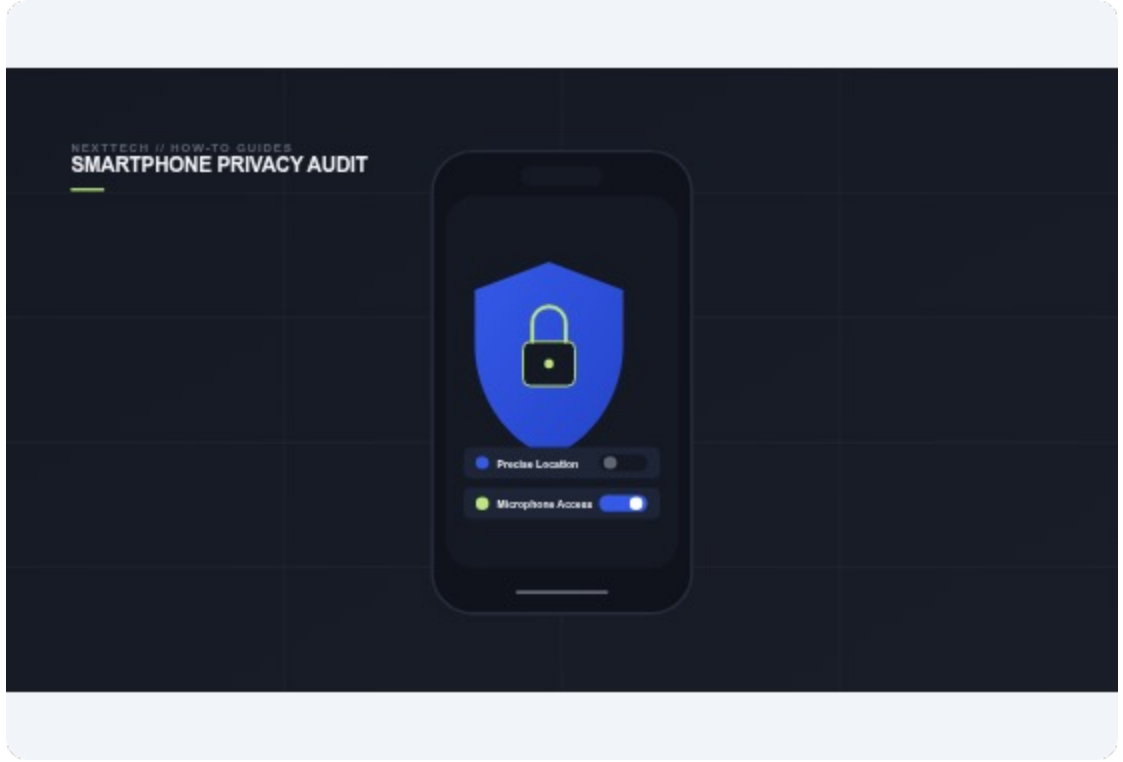
Credentials & Grants

Stanford & NSF PI Grants

Stanford Advanced Computer Security Certificate; Principal Investigator on NSF/USDA grants.

RESEARCH BACKGROUND

Ubiquitous Mobile Apps in Higher Education



Academic Infrastructure

Seamless campus integration via required mobile learning tools.

Social Interconnectivity

Constant exposure through communication and lifestyle platforms.

Extending Prior Work

Building on Mhlanga, Maiti & Hammer (2021) mobile vulnerability paradigms.

ECOSYSTEM TAXONOMY

The Multi-Layered Student App Landscape



Learning Systems

LMS portals and course tools.



Social Networks

Group chats and video apps.



Campus Utilities

Dining and transit services.



Fintech & Deals

Peer payments and discount apps.

RISK ANALYSIS

Primary Privacy & Security Threats

Data Harvesting

Excessive PII aggregation via third-party SDKs.

Location Tracking

Persistent GPS tracking during non-academic hours.

Credential Overreach

OAuth Single-Sign-On token exposure across services.

EMPIRICAL OBSERVATION

Student Risk Awareness Deficit

84%

Students accept app permissions without reviewing terms or privacy agreements.

68%

Students reuse academic portal credentials for third-party mobile web services.

TECHNICAL ASSESSMENT

Vulnerability Vectors in Student Apps

Over-Privileged SDKs

Third-party analytics scripts quietly logging background activity.

Insecure Local Caches

Unencrypted authentication tokens stored in app sandboxes.

Shadow IT Applications

Unvetted student club utilities operating outside institutional oversight.

INVESTIGATION FRAMEWORK

Methodology & Permission Audit Phase

01

Survey Sampling

Auditing collegiate app installation habits.

02

Permission Mapping

Evaluating Android and iOS manifest files.

03

Traffic Analysis

Inspecting third-party egress telemetry.

04

ATT&CK Alignment

Mapping risks to MITRE Mobile Matrix.

STRATEGIC SOLUTIONS

Multi-Tiered Mitigation Strategy

App Vetting Rules

Establishing campus software safety standards.

Student Cyber Hygiene

Promoting least-privilege permission management.

DevSecOps Standards

Enforcing secure eBPF third-party library rules.

Curricular Literacy

Integrating privacy education into orientation.

FUTURE WORK

Future Research Directions

Machine Learning Models: Real-time egress anomaly detection in campus app networks.

Zero-Trust Frameworks: Micro-segmenting institutional student credentials.

Longitudinal Tracking: Monitoring policy changes vs. student compliance behavior over time.



CONCLUSION

Summary & Core Takeaways

Usability Balance

Harmonizing academic mobile convenience with robust privacy preservation.

Proactive Institutional Policy

Shifting higher ed IT from reactive incident response to continuous vetting.

Empowered Student Hygiene

Fostering transparent consent awareness across higher education ecosystems.

References

Federal Trade Commission. (2024, September 19). *FTC staff report finds large social media and video streaming services engaged in vast s surveillance*. U.S. Federal Trade Commission. https://www.ftc.gov/news-events/news/press-releases/2024/09/ftc-staff-report-finds-large-s social-media-video-streaming-companies-have-engaged-vast-surveillance

Hammer, B. (2014). *A picture is worth a thousand words, but are they the words that matter? An analysis of the effects of image c comments on social networking sites* [Doctoral dissertation, Nova Southeastern University]. NSUWorks. https://nsuworks.nova.edu/gscis_etd/172/

Internet Safety Labs. (2026, August 24). *What we need to know about EdTech, data, and student privacy*. National Education Policy Center. h https://nepc.colorado.edu/blog/what-we-need

Mhlanga, M. X., Maiti, R. R., & Hammer, B. (2021). Privacy and security matters related to the use of mobile devices and social media. In *Proceedings of IEEE SoutheastCon 2021* (pp. 1–6). IEEE. https://doi.org/10.1109/SoutheastCon45413.2021.9401838

Pew Research Center. (2025, April 22). *Teens, social media, and mental health report*. Pew Research Center Methods & User Demographics. https://www.pewresearch.org/internet/2025/04/22/teens-social-media-mental-health/

U.S. Department of Education. (2020). *Family Educational Rights and Privacy Act (FERPA) compliance guidelines for student a applications*. Privacy Technical Assistance Center.



Questions & Discussion

Thank you for your time. Open for 5 minutes of Q&A.

Dr. Richard Maiti, Ph.D.

richard.maiti@kysu.edu • 502-597-6125

Associate Professor, Kentucky State University • NSU Ph.D. Class of 2016