George Corser

2974 Vido Drive, Saginaw, MI 48603 • www.georgecorser.com • gpcorser@svsu.edu • 989.780.3168

Scholarship Statement

Research Interests

My primary research interests are **network security** and **digital privacy**. I also study information and application security, cyber crime, and cyber security education. My recent publications have examined network firewall security and economic motivations of cyber criminals. My dissertation work focuses on privacy protection protocols for location based services in wireless vehicular networks. Long term, I intend to research technical solutions to network security and digital privacy problems, examining technical performance, privacy protection levels and economic and social implications. I intend to collaborate with computer science researchers in network security, application security, encryption and digital forensics, but also with social science researchers in business/economics, philosophy/ethics, law/criminal justice and education.

Research Grant Experience

- Principal Investigator (PI), SVSU, Faculty Led Undergraduate Research Grant, $1000, Awarded 12/18/2014. Leading one student in the preparation of diagrams and data as the foundation of a research paper on vehicle network privacy and safety to be published with undergraduate student Alejandro Arenas as co-author. Paper was accepted at IEEE ICNC 2016.
- Principal Investigator (PI), SVSU, Faculty Research/Professional Growth Grant, $3200, Awarded 3/9/2015. Leading one student in the preparation of vehicle networks analysis software.
- Team Leader, NSF, Research Experience for Undergraduates (REU), Oakland University, summer 2013. Led two teams of undergraduate researchers and helped prepare final NSF report. Published two IEEE conference papers with undergraduate co-authors, Patrick D'Errico and Warren Ma. One journal paper was accepted with two other undergraduate co-authors, Mathias Masasabi and Lars Kivari.
- Team Leader, NSF, Research Experience for Undergraduates (REU), Oakland University, summer 2015. Led one team of undergraduate researchers.

Current Research

My recent work has focused on protecting **location privacy in vehicle networks**. This involves researching existing vehicular network standards and measuring the performance of new protocols in simulations. Generally, I seek to identify to what extent digital privacy is possible. Addressing this question requires understanding something about privacy, for example how it is defined and measured in a digital environment. It also requires a broad understanding of computer technology, including hardware and software architectures, network layers and protocols, encryption and other security techniques.

The problem of digital privacy is both important and complicated, confounding both laymen and technologists. While societies try to decide what *should* be kept private, researchers try to determine

what *can* be kept private. Technical solutions to the digital privacy problem will shape society to the extent that technological feasibility determines social acceptability. Already some have proclaimed "privacy is dead" [1,2] and therefore presumably society must change to accept this reality. I suggest reports of privacy's death are premature. The technical problem of privacy has not been studied sufficiently enough to make such a proclamation, nor has the social value of privacy been studied sufficiently enough to abandon it so cavalierly.

Two of my most recent papers and my dissertation research focus on the problem of protecting location privacy against collusion and deanonymization in vehicular networks. There are four methods of protecting privacy [3], hiding events, obfuscation, anonymization and adding dummy events. Hiding events will not always work in vehicle networks because safety is the primary purpose of such systems. Missing transmissions might create safety problems. Obfuscation will not always work when vehicles must provide continuous precise location information to location based services. Anonymization will not always work because it can be defeated by deanonymization, specifically correlating wireless network transmissions with map databases like Google Maps.

That leaves the fourth method, adding dummy events. This technique remains largely un-researched in vehicular network environments, though there have been published a few proposals [4,5,6,7,8,9]. My early research suggests that, to protect privacy, location based services, LBSs, may be designed so that users relay dummy queries through other vehicles to camouflage true locations.

In a computerized culture we often cannot control information about ourselves [10]. We often cannot even restrict access. Our best alternative may be to introduce misinformation, to deceive rather than to restrict those who would infringe upon our privacy. My most recent proposal is called PARROTS, Position Altered Requests Relayed Over Time and Space, a privacy protocol which protects LBS users' location information from LBS administrators even (1) when the LBS requires continuous precise location data in a vehicular ad hoc network, (2) when LBS administrators collude with administrators of vehicular wireless access points (a.k.a. roadside units, or RSUs), and (3) when precise location data can be deanonymized using map databases linking vehicle positions with vehicle owners' home/work addresses and geographic coordinates. Defense against deanonymization requires concealment of endpoints, the effectiveness of which depends on the density of LBS users and the endpoint protection zone size. Simulations using realistic vehicle traffic mobility models have shown improvements in privacy protection under varying endpoint protection zone sizes. I call this approach ***privacy-by-decoy***.

Vision and Future Plans

Short term, I would like to publish new technical solutions to digital privacy problems. This will undoubtedly involve research in wireless networking, system administration, encryption, information storage and retrieval, and location based services. Long term, I intend to identify and develop interdisciplinary research relationships. I would like to write a book similar to *Privacy in Context* [11] which would break the digital privacy problem into the layers of the Zachman Framework [12]. Such a work would architecturally organize digital privacy definitions, metrics, motivations, ethics, methods, mechanisms and attack vectors using as examples a few basic privacy models which are implementable on a computer, especially privacy-by-decoy models. It would require extensive interdisciplinary collaboration.

Integration with Teaching

Both short and long term I intend to complement my teaching with my research. Where possible I already update course material with wireless vehicle network examples. Security in general, and privacy in particular, are hot topics even in the lay press, so they often provide motivation for students studying otherwise dry networking concepts. Networking lessons can expose vulnerabilities for malicious hacking. Students love this sort of thing,

I have also had success developing a YouTube channel and I would like to build a new, similar video resource. I would like to call it Open Source Cybersecurity Academic Repository, or OSCAR. It would consist of videos demonstrations, lab instructions and short quizzes that cybersecurity educators all over the world could share, similar to how programmers share code on SourceForge. I am developing the system now in my course, CIS-355 (Server Side Web Development).

Funding

Expanding cybersecurity education is initiative #8 of the US President's The Comprehensive National Cybersecurity Initiative, CNCI [16]. The NSF continues to fund multi-million dollar cyber security and privacy research projects [13,14]. While I do not anticipate an award in that dollar range, the NSF's Secure and Trustworthy Cyberspace (SaTC) program [15] represents a prime target for funding continuing interdisciplinary digital security research. I expect funding prospects to be better than average for research in the areas of network security and digital privacy.

References

[1] Glanville, J. (Ed.). (2011). *Privacy Is Dead*. SAGE Publications.

[2] Rauhofer, J. (2008). Privacy is dead, get over it! 1 Information privacy and the dream of a risk-free society. *Information & Communications Technology Law*,*17*(3), 185-197.

[3] Shokri, R., Freudiger, J., & Hubaux, J. P. (2010). A unified framework for location privacy. *3rd Hot Topics in Privacy Enhancing Technologies (HotPETs)*.

[4] Chow, R., & Golle, P. (2009, November). Faking contextual data for fun, profit, and privacy. In Proceedings of the 8th ACM workshop on Privacy in the electronic society (pp. 105-108). ACM.

[5] Kido, H., Yanagisawa, Y., & Satoh, T. (2005, July). An anonymous communication technique using dummies for location-based services. In Pervasive Services, 2005. ICPS'05. Proceedings. International Conference on (pp. 88-97). IEEE.

[6] Krumm, J. (2009). Realistic driving trips for location privacy. In Pervasive Computing (pp. 25-41). Springer Berlin Heidelberg.

[7] Lu, H., Jensen, C. S., & Yiu, M. L. (2008, June). Pad: Privacy-area aware, dummy-based location privacy in mobile services. In Proceedings of the Seventh ACM International Workshop on Data Engineering for Wireless and Mobile Access (pp. 16-23). ACM.

[8] You, T. H., Peng, W. C., & Lee, W. C. (2007, May). Protecting moving trajectories with dummies. In Mobile Data Management, 2007 International Conference on (pp. 278-282). IEEE.

[9] Yang, Q., Lim, A., Ruan, X., & Qin, X. (2010, December). Location privacy protection in contention based forwarding for VANETs. In Global Telecommunications Conference (GLOBECOM 2010), 2010 IEEE (pp. 1-5). IEEE.

[10] Moor, J. H. (1997). Towards a Theory of Privacy I1', in the Information Age.*Computers and Society*, *27*(3), 27-32.

[11] Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

[12] Zachman, J. A. (1996). Concepts of the framework for enterprise architecture.*Zachman International*.

[13] Brown, B. (2012, September 27). *Exploring cybercriminal minds, safeguarding privacy among $50m worth of new NSF research projects*. Retrieved from http://www.networkworld.com/news/2012/092712-national-science-foundation-cybersecurity-262841.html

[14] Spice, B. (2013, August 20). Press release: Carnegie Mellon leads NSF project to help people understand web privacy policies. Retrieved from http://www.cmu.edu/news/stories/archives/2013/august/aug20_webprivacypolicies.html

[15] Epstein, J. (2013, January 3). *Report on the NST "Secure and Trustworthy Cyberspace" PI meeting*. Retrieved from https://freedom-to-tinker.com/blog/jeremyepstein/report-on-the-nsf-secure-and-trustworthy-cyberspace-pi-meeting/

[16] http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative. (n.d.). Retrieved from http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative