Oliver Jensen

Computer Science Department ■ University of Texas ■ 1 University Station C0500 ■ Austin, TX 78712
email: ojensen@cs.utexas.edu ■ cell: +1 512 609 0502

Education

University of Texas at Austin, Austin, TX **2010 – Present**
Ph.D. (in candidacy)
Computer Science
Honors: MCD Fellowship

University of Texas at Austin, Austin, TX **2010 – 2013**
Master of Science
Computer Science

Colgate University, Hamilton, NY **2005 – 2009**
B.A. Magna Cum Laude
Computer Science and Mathematics (double concentration)

Honors

- High Honors in Computer Science (2009, Colgate University)
- Edward P. Felt '81 Memorial Prize in Computer Science (2009, Colgate University)
- Raider Academic Honor Roll for Varsity Athletes (4 years, 2006 – 2009, Colgate University)
- Dean's Award for Academic Excellence
  (8 semesters, Fall 2005 – Spring 2009, Colgate University)
- Epsilon Pi Upsilon National Honor Society for Computer Science (2009, National)
- Phi Eta Sigma National Honor Society (2006, National)

Research Interests

- Security and Privacy
- Protocol Design (NFC, Mobile Payments)
- Offensive and Defensive Technologies

Relevant Skills

Programming Languages:

- Python
- Rust
- C
- Java

Platforms:

- Linux
- UNIX
- Windows

Web Application Development:

- Flask, Django, PHP
- HTML5, JavaScript
- SQL, Database Structure
- CSS, SCSS

Other:

- Security Assessments / Penetration Tests
  (application and platform security)
- Research
- LaTeX
- Digital mischief

Work Experience

Praetorian, Inc. **Summer 2016**
Intern *https://www.praetorian.com*
Manager: Anthony Marquez (anthony.marquez@praetorian.com)
Engaged in security assessments for several high-profile clients, including a bank, a space telescope institute, an IoT device manufacturer, and others. Manged and participated in the building a crowd-sourced IoT mapping project targeting non-Internet-connected IoT devices (https://iotmap.io/). Wrote and open-source released a tool to assist with HTTP command injection attacks (https://github.com/praetorian-inc/pyshell).

Google, Inc. **Summer 2015**
Software Engineering Intern *Team: Gmail Security*
Manager: Danesh Irani (danesh@google.com)
Created the client-side HTML sanitizer JsVir for consolidated use across Google products. The many disparate sanitizers in previous use were each broken or vulnerable in some way. Based on the Caja sanitizer, JsVir leverages modern browser technologies built into HTML5. It is undergoing QA for large-scale use across Google, and through the open-source release procedure.

Google, Inc. **Summer 2014**
Intern Engineering Software * *Team: Infrastructure Security / Red Team*
Manager: David Tomaschik (davidtomaschik@google.com)
Created an educational tool to help teach the basics of web-security (e.g. XSS, CSRF, SQLi, etc) to the world. Also created and open-sourced a chrome extension Tamper Chrome to allow inspection and modification of any Chrome request. (*Found that I could alter my official job title.)

Google, Inc. **Summer 2013**
Software Engineering Intern *Team: Incident Response*
Manager: Kristinn Gudjonsson (kiddi@google.com)
Implemented changes to PLASO, an open-source digital forensics tool, greatly increasing speed of common operations. Created PLASM, an output processor for PLASO, which tags, groups, and clusters PLASO output by occurrence and frequent neighbors on an augmented forensic timeline.

Google, Inc. **Summer 2012**
Software Engineering Intern *Team: Adwords API*
Manager: Dan Halem (dhalem@google.com)
Augmented the Adwords API to support non-writing “shadow” versions, such that two versions of the API could be run simultaneously, and the results verified against each other. Also engaged in an internal penetration testing project, under Matt Moore (mattmoore@google.com).

Google, Inc. **Summer 2011**
Software Engineering Intern *Team: Adwords API*
Manager: Dan Halem (dhalem@google.dom)
Created a logs-parsing system capable of aggregating and displaying Adwords data from disparate sources, providing the Adwords team with a view on how 3rd party Adwords resellers affect sales.

Research Experience

University of Texas at Austin **Fall 2013 – Present**
Ph.D. Advisor: Mohamed Gouda *https://cs.utexas.edu/~gouda*
Exploring protocols currently employed by credit cards, in various settings such as NFC and Chip-and-Pin, identifying weaknesses in these protocols, and proposing alternative solutions guarding against these weaknesses.

University of Texas at Austin **Fall 2013 – Spring 2014**
Laboratory for Advanced Systems Research *https://cs.utexas.edu/~lasr*
Supervisor: Lili Qiu
Successfully demonstrated eavesdropping on sensitive NFC communication, harvesting credit card information near NFC-enabled paystations. Worked on developing a protocol for NFC communication which prevents eavesdropping through a self-jamming signal, requiring only the replacement of paystations / readers, and not the credit-cards / tags.

University of Texas at Austin **Fall 2012 – Spring 2013**
Supervisor: Vitaly Shmatikov *https://cs.utexas.edu/~shmat*
Successfully cracked the “rolling code” voice scrambling scheme used by the NFL until August 2012. Continued work on cracking their current digitally encrypted system. Explored Oblivious RAM, and methods for extending its fundamental concepts to a 3-party database system for use in SPADE (Secure and PrivAte Database Execution).

University of Texas at Austin **Spring 2012**
Learning Agents Research Group *https://cs.utexas.edu/~ai-lab*
Supervisor: Peter Stone
Explored instances and causes of Braess' Paradox in the context of vehicular traffic networks for autonomous vehicles using the AIM (Autonomous Intersection Management) protocol. Demonstrated that use of micro-tolling could successfully mitigate such instances in real time.

University of Texas at Austin **Fall 2011**
Laboratory for Advanced Systems Research *https://cs.utexas.edu/~lasr*
Supervisor: Lili Qiu
Conducted thorough measurements of power usage of laptop and mobile network cards in a wide variety of conditions and settings. Through analysis of this data, constructed a power consumption model used to algorithmically manage wireless cards in mobile devices to increase battery life without significantly affecting user experience**.**

Colgate University **Spring 2009**
High-Honors Thesis *http://cs.colgate.edu*
Supervisor: Vijay Ramachandran
Authored the thesis Traceroute Data Integrity and Route Concealment investigating the motives, means, and practice of traceroute data falsification. Collected traceroute data to globally disparate hosts over a period of several months, in order to map out global network paths and seek out opportunities to angage in (and evidence of current) tampering, modification, and other means of covertly conceal true routes.

Entrepreneur Experience

MycenaCave.com **2013 – Present**

Founder, Lead Developer, Owner *https://www.mycenacave.com*

Mycena Cave is an online community and social gaming website, encouraging self-expression through creative writing and digital art. It embodies a digital collectibles aspect, allowing players to represent and customize their creations. The team consists of two co-owners and 21 paid staff.

Whimventory.com **2009 – 2016**

Founder, Developer, Owner *http://www.whimventory.com*

An online “universal wishlist” service. Written in PHP on the CodeIgniter framework and leveraging the jQuery JavaScript library, it provides a simple, clean, and universal interface for adding any product for sale on the Internet to a unified wishlist.

Teaching Experience

University of Texas at Austin **Fall 2014, Spring 2015, Fall 2015, Spring 2016**

Instructor

CS 361S: Network Security and Privacy *https://www.cs.utexas.edu/~ojensen/courses/cs361s*

This course focuses on basic concepts in network and application security. It aims to introduce students to the fundamental techniques used in implementing secure network communications, and to give them an understanding of common threats and attacks, as well as some practical experience in attacking and defending networked systems. Class sizes have ranged from 40 to 80 students.

University of Texas at Austin **Fall 2010 – Present**

Teaching Assistant:

- CS 305J: Introduction to Computing
- CS 307: Foundations of Computer Science
- CS 315H: Data Structures and Algorithms (Honors)
- CS 371P: Object Oriented Programming
- CS 378: The Computational Brain

Hobbies

Colgate Men's Varsity Crew (rowing), Eagle Scout, playing the violin. I also enjoy hacking, backpacking and snowboarding. Languges: English (native), French (once-fluent), German (conversational), Spanish (conversational)

Publications

Architecture of a Mobile Payment System **(in progress)**
Oliver Jensen, Mohamed Gouda

Securing NFC Credit Card Payments from Malicious Retailers **2016**
Oliver Jensen, Tyler O'Meara, Mohamed Gouda
In Proceedings of The International Conference of Networked Systems (NETYS)

A Secure Credit Card Protocol over NFC **2016**
Oliver Jensen, Mohamed Gouda, Lili Qiu
In Proceedings of The International Conference on Distributed Computing and Networking (ICDCN)

Model-Driven Energy-Aware Rate Adaptation **2013**
Muhammad Owais Khan, Vacha Dave, Yi-Chao Chen, Oliver Jensen, Lili Qiu, Apurv Bhartia, Swati Rallapalli
In Proceedings of the International Symposium on Mobile Ad Hoc Networking and Computing (MobiHoc)

Publication Abstracts

Architecture of a Mobile Payment System
In progress. In this work we build conceptually from the 2016 papers to define an augmented contactless (NFC) credit card protocol and supporting architecture. We leverage electronic wallet smart-phone applications and define our interfaces such that we may leverage existing infrastructure (not requiring any Point of Sale to be replaced or upgraded) and such that any credit card may be utilized (as opposed to solely those which support contactless transactions). Further, we retain all security properties from the previous two papers (protection from both malicious third parties and malicious retailers), as well as providing a property known as "unlinkability": retailers become unable to correlate purchases from the same credit card. In so doing, we advance both the security and privacy of credit card payments as a whole, while sidestepping roadblocks to implementation such as the need to upgrade infrastructure.

Securing NFC Credit Card Payments from Malicious Retailers
The protocol by which "contactless" (NFC) credit cards operate is insecure. Previous work has done much to protect this protocol from malicious third parties, e.g. eavesdroppers, credit card skimmers, etc. However, most of these defenses rely on the retailers being honest, and on their Points of Sale following the credit card protocol faithfully. In this paper, we extend the threat model to include malicious retailers, and remove any restrictions on the operation of their Points of Sale. In particular, we identify two classes of attacks which may be executed by a malicious retailer: Over-charge attacks exploiting victim customers, and Transparent Bridge attacks exploiting victim retailers. We then extend the protocol from previous work in order to defend against these attacks, protecting cardholders and honest retailers from malicious retailers.

A Secure Credit Card Protocol over NFC

NFC (“Near Field Communication”) is a short-range wireless communication channel. The current NFC credit card protocol allows a contactless credit card to communicate wirelessly with a Point-of-Sale in order to perform a purchase. This protocol is vulnerable to four common attacks: eavesdropping, skimming, relay attacks, and compromised Points-of-Sale. The attacker’s objective is twofold: stealing sensitive information, and performing unauthorized. We use stepwise refinement to design a secure NFC credit card protocol which defends against all four of these attacks. The resulting protocol does not use heavyweight cryptographic operations, instead using only inexpensive primitives such as pre-computed hashes, indexing, and XOR operations. Moreover, it explores the lower-bound of computation required on the card to mount an effective defense against these four classes of attacks. As such, the energy and computational requirements of the credit card in our protocol are kept to a minimum

Model-Driven Energy-Aware Rate Adaptation

Rate adaptation in WiFi networks has received significant attention recently. However, most existing work focuses on selecting the rate to maximize throughput. How to select a data rate to minimize energy consumption is an important yet under-explored topic. This problem is becoming increasingly important with the rapidly increasing popularity of MIMO deployment, because MIMO offers diverse rate choices (e.g., the number of antennas, the number of streams, modulation, and FEC coding) and selecting the appropriate rate has significant impact on power consumption.

In this paper, we first use extensive measurement to develop a simple yet accurate energy model for 802.11n wireless cards. Then we use the models to drive the design of an energy-aware rate adaptation scheme. A major benefit of a model-based rate adaptation is that applying a model allows us to eliminate frequent probes in many existing rate adaptation schemes so that it can quickly converge to the appropriate data rate. We demonstrate the effectiveness of our approach using trace-driven simulation and real implementation in a wireless testbed.