Frank Y. Wang

frankw@mit.edu
(408) 893-1709
http://frankwang.org

Education

Massachusetts Institute of Technology — Sept 2012 -
Ph.D. in Computer Science
Advised by Prof. Nickolai Zeldovich

Stanford University — Sept 2008 - June 2012
B.S. in Computer Science with Honors and Minor in Mathematics
Advised by Prof. Dan Boneh
Thesis Title: Offloading Critical Security Operations to the GPU

Interests

Computer Security and Privacy, Systems, and Applied Cryptography

Research

Sept 2014- **Private Browsing**. Current Project with Nickolai Zeldovich and James Mickens.

2012 **Chrome Cache and Security**. Project under the guidance of Elie Bursztein and Ulfar Erlingsson. The current cache is addressed by URI, but with increased usage of CDNs and web proxies, content is being duplicated across many URIs, which means there is duplicate content in the cache. At Google, I designed and ran an experiment to understand and gather more details on the duplicated cache content of a real user.

2012-2013 **Understanding the Source of Web Vulnerabilities**. Project with Jason Bau, Elie Bursztein, and John Mitchell. We develop a web application vulnerability metric based on the combined reports of 4 leading commercial black box vulnerability scanners and evaluate this metric using historical benchmarks and our new sample of applications. We then use this metric to examine the impact of three factors on web application security: provenance (developed by startup company or freelancers), developer security knowledge, and programming language. Our study evaluates 27 web applications developed by programmers from 19 Silicon Valley startups and 8 outsourcing freelancers using 5 programming languages. We correlate the expected vulnerability rate of a Web application with whether it is developed by startup company or freelancers, the extent of developer security knowledge (assessed by a simple quiz), and the programming language used. We provide statistical confidence measures and find several results with statistical significance. For example, applications written in PHP are more prone to severe vulnerabilities, especially injection, and applications developed by freelancers tend to have more injection vulnerabilities. Our summary results provide guidance to developers that we believe may improve the security of future web applications.

2012 **Oblivious Encrypted Database**. Project with Prof. Dan Boneh, Craig Gentry, and Shai Halevi. In a private database query system, a client issues queries to a database and obtains the results without learning anything else about the database and without the server learning the query. While previous work has yielded systems that can eciently support disjunction queries, performing conjunction queries privately remains an open problem. In this work, we show that using a polynomial encoding of the database enables efficient implementations of conjunction queries using somewhat homomorphic encryption. We describe a three-party protocol that supports ecient evaluation of conjunction queries. Then, we present two implementations of our protocol using Pailliers additively homomorphic system as well as Brakerskis somewhat homomorphic cryptosystem. Finally, we show that the additional homomorphic properties of the Brakerski cryptosystem allow us to handle queries involving several thousand elements over a million-record database in just a few minutes, far outperforming the implementation using the additively homomorphic system.

2011 **Stegotorus**. Project with Prof. Dan Boneh and collaborators from Stanford Research Institute. Tor is an open network of Internet tunnels that helps improve Internet privacy and security. It was originally developed by the U.S. Navy to protect government communications. The main purpose is to prevent against traffic analysis, which allows attackers to infer connections between various sources on the Internet. Some attackers use sophisticated techniques to track communication patterns, and Tor provides user anonymity by "hiding" a person's network traffic among other people in the Tor network. This is of particular interest because it is commonly used to circumvent government censorship filters, which means packets have to seem random and not have a particular pattern. Currently, the encryption of the data is done through HTTPS. However, because HTTPS has a predictable handshake to initiate the connection, it is very easy for filters to block these connection packets because of the lack of randomness. Therefore, in order to encrypt and decrypt data, keys have to be exchanged before packets are sent, which is a difficult problem. I implemented a protocol that allows keys to be exchanged over the network while maintaining randomness.

2011 **Mobisocial**. Joint work with Prof. Dan Boneh and Prof. Monica Lam's lab. I helped integrate Identity-Based Encryption (IBE) into the Musubi application. Musubi is an application that creates a distributed social network to protect personal privacy. Current social networks, like Facebook, require that users belong to the same proprietary network, but Musubi has no sole proprietary owner of all data exchanged through the network so that no one owns all the data transferred throughout the network. More information regarding the Mobisocial project and Musubi can be found at `http://mobisocial.stanford.edu`.

2011 **Healthcare Security and Privacy**. Project under the guidance of Eric Lam and Prof. John Mitchell. HIPAA is a complex law that regulates communication between healthcare professions and patients, which is extremely difficult to enforce using existing systems. We prove that translating law into a set of rules interpretable by a logic program is possible, and then I helped develop a secure health information system using advanced cryptographic techniques, such attribute-based encryption, and logic programming. This system, given a set of rules created from HIPAA and credentials, automatically encrypts information securely such that only the individuals with the correct credentials (as specified by HIPAA) can read it.

2010-11 **GPU Security**. As part of my honors thesis under the guidance of Prof. Dan Boneh, I studied the security design behind GPU programming languages, such as CUDA and OpenCL. General computing with GPUs has taken off in the last few years because of their unique ability to perform parallel calculations very efficiently. More developers have started to take advantage of this processor to improve software performance. Similarly, security developers have considered using GPUs to offload calculations as a way to improve the speed and robustness of security software. In this thesis, I outline reasons why this process might not necessarily be secure and provide experiments I have performed to find security flaws in GPU offloading. In particular, we find that GPUs are open to denial of service attacks and leak data. More information can be found in my thesis on my website.

2010 **Location Privacy**. Joint work with Prof. Dan Boneh and Prof. Arvind Narayanan. We studied privacy-preserving tests for proximity: Alice can test if she is close to Bob without either party revealing any other information about each other's location. I implemented a system that performs this protocol without revealing location information. More details about this project and the source code for Android are available at `http://crypto.stanford.edu/locpriv/`.

2010 **Airplane Communication Security**. Joint work with Prof. Dan Boneh, Prof. Per Enge, and Sherman Lo. Distance measuring equipment (DME) is a form of navigation that uses land-based transponders to measure distance by timing propogation delay. This radio navigation system is typically used on airplanes as a secondary form of radar to complement GPS and is constantly discussed as a form of alternate navigation because it has signals stronger than GPS. The security problem with DME is that there is no form of authentication between the airplane and the DME. This means the airplane cannot confirm that the messages the airplane receives actually originate from the DME. It is possible to spoof the DME's message and provide incorrect navigation information to the airplane. We provide an approach using cryptography to solve this problem. We provide two DME authentication protocols. Both require little additional equipment and minor changes. More information about this project can be found at `http://crypto.stanford.edu/FAA`.

2009-10 **Simulating Catalytic Systems**. Joint work with Venkat Viswanathan and Prof. Heinz Pitsch. Low operating temperatures, quiet operation, and high theoretical efficiencies have made Polymer Electrolyte Membrane Fuel Cells a desirable power source. Specifically, we studied the sluggish oxygen reduction reaction (ORR) occurring at the cathode of the fuel cell. I helped develop a computational framework to better simulate different sized nanoparticles undergoing ORR. We used this tool to perform a computational analysis of the effect of particle size and support material on the electrocatalytic activity of platinum nanoparticles, finding an optimal particle size in the range of 2.5-3.5 nm, which agrees well with recent experimental work.

Publications

1. **Frank Wang**, James Mickens, Nickolai Zeldovich, and Vinod Vaikuntanathan. "Sieve: Cryptographically Enforced Access Control for User Data in Untrusted Clouds." To appear in proceedings of Networked Systems Design and Implementation (NSDI) 2016.
2. Dan Boneh, Craig Gentry, Shai Halevi, **Frank Wang**, and David J. Wu. "Private database queries using Somewhat Homomorphic Encryption." In proceedings of Applied Cryptography and Network Security (ACNS) 2013.
3. Zachary Weinberg, Jeffrey Wang, Vinod Yegneswaran, Linda Briesemeister, Steven Cheung, **Frank Wang**, and Dan Boneh. "StegoTorus: a camouflage proxy for the Tor anonymity system." In proceedings of ACM Conference on Computer and Communications Security (CCS) 2012.
4. Peifung E. Lam, John C. Mitchell, Andre Scedrov, Sharada Sundaram, and **Frank Wang**. "Declarative privacy policy: Finite models and Attribute-Based Encryption." In proceedings of 2nd ACM International Health Informatics Symposium, 2012.
5. Venkatasubramanian Viswanthan and **Frank Wang**. "Theoretical analysis of the effect of particle size and support on the kinetics of oxygen reduction reaction on platinum nanoparticles." Nanoscale, 2012, 4(16), 5110-5117.
6. Venkatasubramanian Viswanathan, **Frank Wang**, and Heinz Pitsch. "Dynamic Monte-Carlo based approach for simulating nanostructured catalytic and electrocatalytic systems." Computing in Science and Engineering, 2012, 14(2), 60-68.

Teaching

Teaching Assistant for MIT Computer Systems Security (6.858) — Fall 2012
Teaching Assistant for Stanford Introduction to Cryptography (CS 255) — Winter 2012

Awards

NSF Graduate Research Fellowship — Sept 2013 -
Jacobs Presidential Fellowship — Sept 2012 - June 2013
Massachusetts Institute of Technology

Industry Experience

Facebook, Security Engineer Research Intern — June - Aug 2013
Designing and building infrastructure for intrusion detection

Google, Software Engineering Intern — June - Aug 2012
Chrome security research project for Security Research under mentorship of Elie Bursztein and Ulfar Erlingsson.

Other Experience

Rough Draft Ventures, Partner — Sept 2014 - Current
Sidney Pacific, Board of Trustees — May 2015 - Current
Advise new officers, administer elections, and deal with major issues.

Sidney Pacific, Web Chair — Sept 2012 - May 2015
Maintain website and create new features.

Skills

C/C++, Python, Java, Android, PHP, SQL, Javascript