David Isaac Wolinsky
Novi Financial, a subsidary of Facebook
E-mail: isaac.wolinsky@gmail.com
Web: http://www.davidwolinsky.com
Phone: (352) 283-4066

Wednesday 10th March, 2021

Interests Computer systems, cyber-security, anonymity, networking, distributed computing.

Education

Ph.D. in Electrical-Computer Engineering, August 2011, University of Florida, Advisor: Renato J Figueiredo
Thesis: "Design and Implementation of User-friendly, Self-configuring, and Scalable Virtual Private Networks"
M.S. in Electrical-Computer Engineering, May 2007, University of Florida, Advisor: Renato J Figueiredo
Thesis: "Design Space Exploration of Virtual Machine Appliances for Wide-Area Distributed Computing,"
B.S. in Electrical-Computer Engineering, May 2005, University of Florida

Work Experience

Novi Financial, a subsidary of Facebook — Menlo Park, CA
Diem Blockchain – Software Engineer — July 2019 – present

- Selected as one of four core maintainers of the Diem blockchain
- Actively defining the framework for integrating with Diem as a payment network inclusive of blockchain synchronization, handling of payments / transactions, and off-chain exchanges
- Worked across several organizations to architect the Diem governance model and genesis procedures and built a set of tools to facilitate the genesis process
- Identified the (minimal) security critical components of the Diem blockchain and isolated them into separate execution containers with negligible performance impact
- Established (crypto) key management principles and frameworks for the Diem blockchain validators

Facebook — Menlo Park, CA
Ads Growth – Software Engineer and Manager — August 2015 – July 2019

- Led a team of 7 engineers as a hybrid tech lead / manager
- Drove the architecture and development of communication platforms that increased the total number of active advertisers by over 6%
- Eliminated Facebook advertiser marketing dependency on third-party communication platforms by building a rich e-mail platform saving the company millions of dollars a year, eliminating third-party access to consumer data, and making Facebook GDPR unsubscribe compliant (easily worth millions in fines per year)
- Worked across the company with ML experts to infuse our advertising communication products with ML to substantially improve reach (over 2x) and effectiveness (nearly 50% increase of active advertisers)

Yale University — New Haven, CT
Research Scientist / Lecturer — June 2011 – August 2015

- Taught Operating Systems and advanced systems seminar
- Designed and developed the first strong anonymity network that scaled to 1000s of users, Dissent
- Designed the first system to systematically address intersection attacks in anonymity systems, Buddies
- Designed and developed an OS that protects from accidental leakage of private information, Nymix
- Investigated means for avoiding correlated failures in cloud computing, INDaaS
- Developed privacy preserving biometric authentication software, Private Eyes
- Developed deniable, forward secure group authentication software, DAGA
- Mentored 6 PhD students, 2 masters students, 4 interns, and many undergraduate projects

University of Florida — Gainesville, Florida
System Administrator / Research Assistant — May 2006 – June 2011

- Teacher's assistant for digital computer architecture, virtual computing, computer system design
- Designed and developed a distributed, decentralized volunteer grid, Grid Appliance
- Designed and developed a decentralized virtual private network, Brunet / IPOP
- Maintained a multi-university distributed computing grid, Archer
- Developed teaching modules for cloud computing including Hadoop and MPI using Grid Appliance
- Mentored 4 PhD students, 3 masters students, and 3 high school students

Dell — Round Rock, Texas
Intern with the Server Performance and Analysis Lab — May 2005 – August 2005

- Led an investigation into the Xen virtual machine monitor
- Experimented with early prototype Intel VT (hardware virtualization) processors
- Compared performance between Xen using paravirtualization and hardware virtualization
- Developed a secure web browser using virtual machines for Summer 2005 Technology Fair

Dell Integrated Products and Process Design (IPPD) — Gainesville, Florida
Team Lead — August 2004 to May 2005

- Built a simulator for WMI (Windows Management Instrumentation) in C++
- Transitioned resulting software to Dell who used it for internal projects
- Led a team of 5 students

Software Development Skills

- Substantial experience with C, C++, C#, Hack (PHP), Python, React (JavaScript), and Rust.
- Significant experience with Bash, Go, Haskell, HTML DOM, Java, Latex, and (My)SQL.
- Web, cluster, and grid management skills scaling from single to hundreds of resources
- Development in and management of Linux, Mac, and Windows environments
- Experience deploying large-scale distributed systems on DeterLab, EC2, and PlanetLab.
- Cluster management experience using Terraform, Kubernetes, and Docker.
- Significant use of profilers (e.g., Valgrind) and debuggers (e.g., gdb)
- Extensive experience with unit and integration testing as well as test deployments

Selected Projects

- Diem Blockchain - 07/19 to present - A proof of authority blockchain written in Rust provides the backend for the Diem Payment Network.
- Dissent - 06/11 to 09/14 - A C++ framework and run-time for large-scale, accountable group anonymity. Supports groups over 5,000 using a variety of different communication methods (Dissent CCS'10, Dissent OSDI'12, Verdict USENIX Security '13, Buddies CCS'13).
- Nymix - 11/12 to 10/14 - An operating system designed to protect users from accidentally leaking private information. Isolates user applications, data, and communication through virtualization. Local system supports Amnesiac system with persistent data stored anonymously to the cloud.
- Anonymity Simulator - 10/12 to 04/13 - A python library for acquiring data sets from IRC (Internet Relay Chat) and Twitter. As well as a data parser and simulator for evaluating intersection resistance in group anonymous communication systems.
- Grid Appliance - 05/06 to 09/11 - Ad hoc Distributed, decentralized grid system using virtual, physical, and cloud resources. Utilizes Condor for batch job scheduling and IPOP / Brunet for virtual networking. Configuration and security handled through a web interface.
- IPOP – IP over P2P - 05/06 to 09/12 - Lead developer – Structured P2P, completly decentralized virtual networking stack written in C#, 7,000 lines of code. Supports DHCP, multicast, ARP, transparent subnet gateway, network address translation, and firewalls. Built on top of Brunet. Used to build "GroupVPN" and "SocialVPN". Note: source code has been integrated into Brunet.
- Brunet - 05/07 to 09/12 - Structured P2P framework written in C#, 41,000 lines of code. Supports completely decentralized NAT traversal via hole punching and relays, DHT, edge and overlay security, xmlrpc bridge, private overlay bootstrapping, and a built-in Simulator. My contributions were support for relays, DHT, security, bootstrapping from existing overlays, and a built-in simulator.

Selected Research Papers

1. Ewa Syta, Iulia Tamas, Dylan Visher, **David I Wolinsky**, Philipp Jovanovic, Linus Gasser, Nicolas Gailly, Ismail Khoffi, Bryan Ford, "Keeping authorities "honest or bust" with decentralized witness cosigning", IEEE Symposium on Security and Privacy (SP), 05/2016
2. Ennan Zhai, Ruichuan Chen, **David I Wolinsky**, and Bryan Ford, "Heading Off Correlated Failures through Independence-as-a-Service", USENIX Symposium on Operating Systems Design and Implementation (OSDI), 10/2014
3. **David I Wolinsky**, Ewa Syta, and Bryan Ford, "Hang With Your Buddies to Resist the Intersection Attack", ACM Conference on Computer and Communications Security (CCS), 11/2013

4. **David I Wolinsky**, Panoat Chuchaisri, Kyungyong Lee, and Renato Figueiredo, "Experiences with Self-Organizing Decentralized Grids Using the Grid Appliance", International Journal of Cluster Computing, 06/2013
5. **David I Wolinsky**, Henry Corrigan-Gibbs, Bryan Ford, and Aaron Johnson, "Dissent in Numbers: Making Strong Anonymity Scale", USENIX Symposium on Operating Systems Design and Implementation (OSDI), 10/2012
6. Kyungyong Lee, **David I Wolinsky**, and Renato J Figueiredo, "PonD : Dynamic Creation of HTC Pool on Demand Using a Decentralized Resource Discovery System", ACM International Symposium on High-Performance Parallel and Distributed Computing (HPDC), 06/2012
7. **David I Wolinsky** and Renato J Figueiredo, "Experiences with Self-Organizing Decentralized Grids Using the Grid Appliance", ACM International Symposium on High Performance Distributed Computing (HPDC), 06/2011
8. **David I Wolinsky**, Pierre St. Juste, P Oscar Boykin, and Renato Figueiredo, "Addressing the P2P Bootstrap Problem for Small Overlay Networks", IEEE International Conference on Peer-to-Peer Computing (P2P), 08/2010
9. Pierre St Juste, **David I Wolinsky**, P Oscar Boykin, Michael Covington, and Renato J Figueiredo, "SocialVPN: Enabling Wide-Area Collaboration with Integrated Social and Overlay Networks", Journal of Computer Networks, 08/2010
10. **David I Wolinsky**, Yonggang Liu, Pierre St. Juste, Girish Venkatasubramanian, Renato J Figueiredo, "On the Design of Scalable, Self-Configuring Virtual Networks", SuperComputing, 11/2009

Selected Talks

1. "Tracking Resistance in PriFi", EuroSys Program Committee Workshop, 01/2015
2. "Enforcing Anonymity and Improving Pseudonymity in Tails", Tails Hackfest 2014, 07/05/14
3. "Hang With Your Buddies to Resist the Intersection Attack", ACM Conference on Computer and Communications Security (CCS), 11/2013
4. "Strong, Scalable Anonymity with Dissent", USENIX Symposium on Operating Systems Design and Implementation (OSDI), 10/2012
5. "Experiences with Self-Organizing, Decentralized Grids Using the Grid Appliance", IEEE High Performance Distributed Computing (HPDC), 06/2011
6. "Addressing the P2P Bootstrap Problem for Small Overlay Networks", IEEE International Conference on Peer-to-Peer Computing (P2P), 08/2010
7. "Archer - A Community Distributed Computing Infrastructure for Computer Architecture Research and Education", Universities of Northeastern, Minnesota, and Texas at Austin, 09/[14,16,18]/09
8. "Autonomic Condor Clouds", Condor Week, 04/2009
9. "IPOP - IP over P2P Virtual Networking for Grid Computing", Open Science Grid All Hands, 03/2009