Surya Bakshi (sbakshi3@illinois.edu)

July 21, 2018

2^{nd} Year Graduate student in ECE.
810 W Stoughton St Urbana, IL 61801 - (516) 424 3656

Education

- **University of Illinois at Urbana-Champaign** — Urbana, IL
  ***Advisor: Andrew Miller**, Master of Science in ECE* — *2016 - Present*
  - Focus on cryptocurrencies, decentralized systems, security
- **University of Illinois at Urbana-Champaign** — Urbana, IL
  Bachelor of Science in ECE — *2012-2016*
  - Coursework: distributed systems, OS design, algorithms, computer architecture

Experience

- **Graduate Researcher at Decentralized Systems Lab** — Urbana
  Advisor: Andrew Miller — *2016 - Present*
  - Measurement of Bitcoin topology and influential miners
  - Decentralized systems security, smart contracts
- **Truebit**
  Researcher — *2018 - Present*
  - Doing research into securing and designing the Truebit incentnive layer and token mechanics. More broad work into cryptoeconomic problems as well as implementation of incentive layer.
- **ExoWear**
  Software Engineer — *2016*
  - Start-up in medical technology that provides a Bluetooth device to help monitor physical rehabilitation
  - Worked on developing the core product and managed other engineers
- **Undergraduate Researcher at Depend Research Group** — Urbana
  *Undergraduate Researcher, **Advisor**: Zbigniew Kalbarczyk* — *2015-2016*
  - Attack testbed that simulates different attacks from web applications to DDoS, remote code execution, SSL vulnerabilities
- **Akuna Capital** — Champaign, IL
  Software Developer Intern — *2015*
  - C++ gateways that send buys/sells to exchange and handle book keeping

Research

- **TwistedPair: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees**
  *G. Fanti, **S. Bakshi**, S. B. Venkatakrishnan, A. Miller, B. Denby, S. Bhargava, P. Viswanath*
  In submission at SigMetrics 2018

- **Erays: Reverse Engineering Ethereum's Opaque Smart Contracts**
  *Y. Zhou, D. Kumar, **S. Bakshi**, J. Mason, A. Miller, M. Bailey* *2018*
  In submission USENIX 2018 *2nd Round*

Projects - Github: https://github.com/sbaks0820

- **Battleship State Channel** IC3 Bootcamp
  Solidity, Truffle, Ethereum *2018*
  - Project from the IC3 Bootcamp, a Battleship game implemented as a state channel. Uses a combination of the Sprites, Pisa, Perun and L4 state channel construction.
- **microRaiden Off-chain Payment Monitoring**
  Solidity, Ethereum, Raiden, Python *2018*
  - Implementation of a **privacy-preserving** monitoring protocol for off-chain payment channels on Ethereum
  - **Paper with formal definitions and proofs incoming**
- **hackthiscontract.io**
  Solidity, Smart Contract Security *2017*
  - Interactive challenges for hacking vulnerable smart contracts and ERC20 tokens
  - Creating games where layered vulnerabilities allows adversaries to violate contract invariants
- **Dandelion++**
  Fork of Bitcoin Core and BIP *2017*
  - Implementation of Dandelion++ protocol that adds privacy at the p2p level of Bitcoin
  - Article about it on CoinDesk, a BIP-proposal on the Bitcoin Dec mailing list and a paper submission coming soon
- **Python-Bitcoinlib**
  Contributor, Bitcoin, Privacy *2017*
  - Contribution for segwit support in popular Python Bitcoin library managed by Peter Todd
- **Fair Lottery Smart Contract**
  Serpent Programming Language, Ethereum *2016*
  - Smart contract that implements a cryptographically fair lottery with a python simulator
- **Echo Dot Permissions Model**
  Java, Python Flask, AWS, Alexa Skills *2016*
  - Interacts with Alexa Skills and Microsoft Cognitive API to provide access control based on speaker recognition
- **Attack Testbed**
  Python, JavaScript, Docker *2015*
  - Docker testbed that allows easy creation, simulation, monitoring and replaying of attacks ranging from the application layer down to the network layer
  - Abstract paper: "Security Testbed: Scalable Infrastructure for Interactive Attack Replay and Testing of Security Monitoring Tools"
- **GalapagOS**
  C, x86 assembly *2015*
  - Light Linux-based operation system that runs on x86 assembly with a virtual memory support, scheduling, system calls, multiple terminals, drivers

Continued on next page

Continued from previous page

- **5-Stage Pipelined Processor**
  Verilog *2016*
  - Pipeline processor with branch prediction, multi-layered LRU caches, leap-frogging
- **FPGA Brick Breaker**
  System Verilog, C *2015*
  - FPGA brick breaker with verilog vga monitor, keyboard driver support