Markus Gaasedelen

[address redacted]
Troy, New York, 12180

https://mark.us
markus.gaasedelen@gmail.com

Education

Rensselaer Polytechnic Institute 08/2011 – 05/2015

- B.S. Computer Science
  - GPA: 3.67 / 4.00

Work Experience

RET2 Systems, Inc. – *Co-founder, Senior Researcher* 09/2017 – Present

- Co-founded an applied security research firm to explore a broad range of systems-level topics
- Launched a gamified educational platform for learning practical binary exploitation skillsets
- Developed three award-winning reverse engineering tools embraced by thousands of security researchers
- Participated in PWN2OWN 2018 with a zero-day exploit chain for the Apple Safari Web Browser

Microsoft Corporation – *Security Software Engineer II* 07/2015 – 08/2017

- Root-caused hundreds of reported security issues in Microsoft software using WinDbg
- Produced technical reports documenting impact and remediation for each analyzed vulnerability
- Reverse engineered 5+ in-the-wild zero-days targeting the Windows kernel using IDA Pro
- Prototyped record-replay debugging of Windows kernel by integrating Microsoft TTD into Hyper-V

Trail of Bits, Inc. – *Security Research Intern* 12/2014 – 02/2015

- Refactored a C++ based semantic binary analysis framework known as CodeReason
- Established a working knowledge of Valgrind's intermediate representation language, VEX
- Created demos which leveraged the framework to discover ROP gadgets that met specified constraints
- Assisted with the release and maintenance of CodeReason which is now available on GitHub

Raytheon SI Gov. Solutions – *Vulnerability Research Intern* 06/2014 – 08/2014

- Source reviewed and fuzzed the SSH protocol implementations of PuTTY and OpenSSH
- Refined a proof-of-concept crash into a working exploit demo for an existing PuTTY CVE
- Discovered several exploitable memory corruption issues in the SSH server of an embedded ARM device
- Scripted binary analysis tasks in IDA and GDB to evaluate the attack surface of other remote services

MIT Lincoln Laboratory – *Security Research Intern* 06/2013 – 08/2013

- Developed a Python-based framework to excise malware from PDF files into portable 'patches'
- Forged a deep understanding of the PDF file format and its various internal structures
- Generated new PDF malware samples with my patch files to evaluate the robustness of anti-virus detection
- Built a JavaScript obfuscator to explore methods of masking malicious PDF elements from detection

Teaching Experience

RET2 WarGames – *Co-creator, Professional Trainer* 09/2017 – Present

- Designed a cutting-edge interactive x64 binary exploitation curriculum accessible via the web
- Wrote JavaScript that delivers progress-based feedback as students reach challenge milestones
- Mentored hundreds of students 1-on-1 to debug their exploits and fully realize low-level systems concepts
- Deployed the curriculum in commercial and academic settings, including RPI, ASU, West Point, DoD [link]

Modern Binary Exploitation – *Co-creator, Lecturer* 01/2015 – 05/2015

- Led a team of six to create the first university curriculum focusing on x86 binary exploitation
- Served as a lecturer to a class of 50+ students that enrolled in the Spring 2015 offering at RPI
- Constructed interactive lectures detailing C-based vulnerability patterns and modern exploit mitigations
- Curriculum amassed 4,600 stars on GitHub [link] and later adapted by Georgia Tech, Brown, GMU

RPISEC – *Club President, RPI Computer Security Club* 09/2012 – 05/2015

- Elected president of RPISEC from 2013 - 2015, active member of the club since 2012
- Led interactive weekly seminars to get other students interested and excited about security
- Competed in countless security CTFs including CSAW, Plaid, DEFCON, Boston Key Party, ISTS
- Rallied an enthusiastic student club into one of the most successful CTF teams in the USA

(Selected) Projects

Tenet – *A Trace Explorer for Reverse Engineers* 04/2021 – Present

- Developed Tenet to experiment with exploring execution traces using interactive visualizations
- Used Tenet to analyze real-world vulnerabilities discovered through snapshot-based fuzzers
- Incorporated several novel UI interactions to fluidly navigate between related states of program execution
- Published to GitHub in 2021 under the MIT License, where the project has collected over 800 stars [link]

Lucid – *A Microcode Explorer for the Hex-Rays Decompiler* 08/2020 – 09/2020

- Developed Lucid to help IDA plugin developers explore the Hex-Rays decompilation pipeline
- Engineered with an acute focus on usability to create a responsive, memorable user experience
- Boosted developer comprehension of the Hex-Rays microcode, fostering innovative new extensions
- Published to GitHub in 2020 under the MIT License, where the project has collected over 250 stars [link]

EthRays – *A Decompiler for Ethereum Smart Contracts* 01/2018 – 06/2018

- Developed EthRays as the first truly robust interactive decompiler for the EVM bytecode
- Integrated the decompiler into Binary Ninja, a flexible GUI-based binary analysis platform
- Reverse engineered dozens of sourceless on-chain Ethereum smart contracts to ensure correctness
- First team out of hundreds to successfully exploit a smart contract during DEFCON Quals 2018

Lighthouse – *A Coverage Explorer for Reverse Engineers* 02/2017 – Present

- Developed Lighthouse to visualize coverage for previously opaque binary-only fuzzing tasks
- Cited broadly by industry researchers for its role in helping uncover hundreds of CVEs
- Employed dynamic binary instrumentation such as Intel Pin, DynamoRIO, and Frida to collect coverage
- Published to GitHub in 2017 under the MIT License, where the project has collected over 1,500 stars [link]

Sol[IDA]rity – *Collaborative Reverse Engineering for IDA Pro* 05/2015 – 07/2016

- Developed Solidarity to facilitate real-time collaboration on reverse engineering tasks
- Formulated an extensive client/server Python infrastructure to synchronize disassemblers
- Explored methods of cultivating camaraderie and task awareness through non-verbal UX interactions
- Presented publicly on the project and its motivations at REcon 2016 in Montreal, Canada

Industry Presentations

- **The Layman's Guide to Zero-day Engineering**, 2018, Chaos Communication Conference
- **Building Cyber Armies at Scale**, 2018, ANYCON
- **Sol[IDA]rity: Collaborative Reverse Engineering**, 2016, REcon Montreal

(Selected) Research Writing

- **Fuzzing Modern UDP Game Protocols With Snapshot-based Fuzzers**, 2021 [link]
- **Extending the Hex-Rays Decompiler to Support Intel AVX Instructions**, 2020 [link]
- **In Transactional Memory, No One Can Hear You Scream**, 2019 [link]
- **A Methodical Approach to Browser Exploitation**, 2018 [link]
- **Practical Decompilation of Ethereum Smart Contracts**, 2018 [link]
- **Dangers of the Decompiler: Sampling of Anti-Decompilation Techniques**, 2017 [link]
- **Solving FireEye's Flare-On Six via Side Channels,** 2014 [link]
- **Depackaging the Nintendo 3DS CPU**, 2014 [link]

Awards and Honors

- **Pwnie Awards 'Epic Achievement' Nominee**, 2021 [link]
- **1st Place Hex-Rays Plugin Contest**, 2021 [link]
- **2nd Place Hex-Rays Plugin Contest**, 2020 [link]
- **Pwn2Own Competitor**, 2018 [link]
  - CVE 2018-4192, CVE 2018-4193
- **10th Place DEFCON CTF Finals** (RPISEC), 2018 [link]
- **2nd Place Hex-Rays Plugin Contest**, 2017 [link]
- **20th Finisher of FireEye's Flare-On** (1,500+ Competitors), 2015 [link]
- **Rensselaer Glenn Martin Mueller '64 Prize**, 2015
  - *"A graduating RPI computer science major who is deemed to be the most entrepreneurial."*
- **Member of Upsilon Pi Epsilon CS Honor Society**, 2014 – 2015
- **3rd Place CSAW CTF Finals** (RPISEC), 2014 [link]
- **23rd Finisher of FireEye's Flare-On** (1,000+ Competitors), 2014
- **Facebook DEFCON Scholarship**, 2014
- **4th Finisher of Microsoft BlueHat Challenge** (2,000+ Competitors), 2013
- **10th Place CSAW CTF Finals** (RPISEC), 2013 [link]