Charles Perine

Boise, ID

https://charlesperine.com
https://www.linkedin.com/in/charlesperine

SKILLSET

- Security Research
- Network Security
- Computer Security
- Application Security
- Penetration Testing
- Reverse Engineering
- Red Teaming
- Embedded System Security
- Control System Security

WORK EXPERIENCE

- **Trend Micro** — Irving, TX
  Threat Researcher — *Oct 2018 - Feb 2024*
  - Led multiple research projects, managing time-lines, research direction, and team coordination
  - Conducted security assessments, uncovering vulnerabilities in multiple devices and notifying ZDI
  - Developed a method to identify customers of cloud services
  - Built, maintained, and monitored hyper-realistic factory honeypots, establishing a fictitious company to enhance realism and capture cyber threats
  - Collaborated on several research projects, leading to the creation of white papers, blog content, conference presentations, and media coverage
  - Tested Databricks and Retrieval-Augmented Generation (RAG) technologies to support a research project, optimizing data processing and information retrieval
- **Revolutionary Security** — Blue Bell, PA
  Senior Security Consultant — *Oct 2017 - Sept 2018*
  - Performed programmatic and technical threat model for product development organizations
  - Managed and executed pentesting and vulnerability assessments to evaluate and enhance the security of both corporate networks and industrial control systems
  - Executed vulnerability assessment of sub-GHz radio networks and hardware
- **Leidos (formerly Lockheed Martin - IS&GS)** — Valley Forge, PA
  Information Assurance Engineer — *Oct 2012 - Oct 2017*
  - Led pentesting engagements and vulnerability assessments to verify the security of corporate, industrial control, point of sale and Internet service provider systems
  - Mentored junior consultants in industrial control system assessment methodologies
  - Discovered multiple 0day vulnerabilities in industrial control systems
  - Communicated complex technical details effectively to C-level management
- **General Electric** — Van Buren Township, MI
  Lead Analyst - Security Assessments — *Mar 2011 - Oct 2012*
  - Performed software and hardware security assessments for intra-company organizations
  - Led root-cause analysis investigations in response to product security incidents
  - Directed small, agile, global assessment teams
  - Trained analysts in fuzzing, reversing, and exploitation of control and embedded systems
- **Digital Bond, Inc.** — Sunrise, FL
  Security Consultant — *Jan 2008 - Mar 2011*
  - Performed security assessments of Industrial Control Systems, Smart Grid, and Corporate Networks
  - Generated custom Meterpreter scripts for complex ICS attacks
  - Produced and instructed a protocol fuzzing, exploitation development, and firmware analysis curriculum

TECHNICAL EXPERIENCE

- 10+ years experience with *nix based operating systems
- 10+ years experience with Industrial Control System security
- 5+ years security research
- Familiar with the following programming languages: C/C++, IA32, Perl, Python, SQL, Shell scripting

EDUCATION

- **California State University - Hayward** — Hayward, CA
  Bachelor of Science in Computer Science — *Aug 2004 - Aug 2006*
- **Las Positas College** — Livermore, CA
  Associate of Science in Computer Science — *Sep 2001 - Aug 2004*
- **REcon - Philippe Langlois** — Montreal, ON
  Mobile and Telecom Applied Hacking and Reverse Engineering — *Jun 2016*
- **REcon - Joe Grand** — Montreal, ON
  Hardware Hacking — *Jun 2015*
- **REcon - Saumil Shah** — Montreal, ON
  Exploit Laboratory — *Jun 2014*
- **Immunity, Inc.** — Miami, FL
  Unethical Hacking — *Nov 2008*
- **SANS** — Monterey, CA
  SEC 503: Intrusion Detection In-Depth — *May 2007*

Papers

- "A Survey of Cloud-Based GPU Threats and Their Impact on AI, HPC, and Cloud Computing" Trend Micro, Mar 2024
- "Distributed Energy Generation Gateway (In)Security" Trend Micro, Jan 2024
- "MQTT and M2M: Do You Know Who Owns Your Machine's Data?" Trend Micro, Oct 2023
- "Examining Security Risks in Logistics APIs Used by Online Shopping Platforms" Trend Micro, Sep 2022
- "Attacks From 4G/5G Core Networks: Risks of the Industrial IoT in Compromised Campus Networks" Trend Micro, Sep 2020
- "Lost in translation: when industrial protocol translation goes wrong" Trend Micro, Aug 2020
- "Caught in the act: Running a realistic factory honeypot to capture real threats" Trend Micro, Jan 2020

Presentations

- *Attacks From the 4G/5G Core* — S4 2022
- *Faking a Factory: Creating and Operating a Realistic Honeypot* — Blackhat Asia 2020
- *Good to Bad: When Industrial Protocol Translation Goes Wrong* — Critis 2020