Graham Sutherland

gsuberland@gmail.com

Keywords

IoT, electronic design, side-channel attacks, industrial, operational technologies, marine, x86 platform, Windows kernel & internals, Windows binary applications, cryptography, reverse engineering, penetration testing, code review, threat modelling, C#, JS, Python, PHP, C++, C, x86 assembly, Delphi, Java

Requirements

Position must allow full-time work from home in Nottingham, England.

About me

My key skill areas include hardware and IoT, connected vehicle and marine operational technologies, and Windows applications and internals. I have a strong background in electronics including signal integrity, EMI, and related physics, which allows me to tackle advanced security assessments where physical and side-channel attacks are in scope, or where custom electronics design is required. I am highly adaptable to learning new technologies and excel at developing new security assessment capabilities. I am at my best when tackling unusual and novel problems in areas where little existing knowledge or research exists. I have received strong praise for the quality of my written communication in reports and documentation. I hold a UK passport and driving license.

Employment

Senior Security Researcher **2018-11 to Present**
LRQA Nettitude

Performed internal and external security research and customer engagements with a focus on marine operational technologies, industrial environments, IoT, hardware, x86 platforms, and cryptography. Scoped and delivered complex projects involving emerging technologies and industry verticals with little or no existing published research or guidance. Built advanced IoT assessment capabilities, including techniques for tamper resistance bypass and side-channel attacks. Designed bespoke electronic devices to support customer engagements and internal research requirements. Wrote internal safety standards and procedures for hardware research activities. Published research through official company channels.

Senior Information Security Consultant **2013-03 to 2018-10**
Cisco Advanced Security Services / Portcullis

Performed penetration tests on a wide variety of targets across all industry verticals, working individually, as part of a team, and as a team lead. Developed and lead the Hardware Assessment, Cryptography Review, Windows Binary Application Assessment, and Web Services Assessment capabilities, acting as a key point of contact and training leader for these assessment types. Acted as a coordinator for security research efforts within the EMEAR region alongside Cisco Talos. Designed a connected vehicle and IoT lab and helped manage the procurement of necessary tools and materials. Helped shape the internal SSL/TLS security standards document used as a benchmark for all Cisco products worldwide. Spoke at both internal and external conferences on behalf of the company.

Software Developer **2012-04 to 2013-02**
Fast React Systems Ltd

Hired as a C# developer in a small team, moved into maintaining two large ERP products written in Delphi. Learned Delphi 7 and Delphi 2009 from scratch in a fast-paced agile development environment. Developed methods for interoperation and marshalling between .NET code and Delphi code, by reverse engineering internal object representations and compiler behaviours. Patched 3rd party libraries to fix bugs without access to source.

Software Developer **2011-09 to 2012-03**
Centiq Ltd

Worked in a small development team to produce a Windows-based system monitoring agent, written in C#, to integrate with an existing web service written in PHP. Produced documentation and an installer.

Provided basic penetration testing on internal systems and infrastructure, as well as a security review of the custom web service.

Volunteer Student Lecturer **2009-10 to 2009-12**
Leicester DeMontfort University

Pioneered a set of programming classes and lectures open to any students at DMU, providing additional tutoring to anyone who wished to come along. Attendees ranged from HND to masters students.

Web Developer **2007 to 2009**
Twisted Pair Design

Self-employed as a web design and development freelancer. Consulted with clients to design and build bespoke web applications. Wrote scopes of work and contracts for projects.

Certifications and Training

- ISO/IEC 62443 (ISA 99) Industrial Automation and Control Systems Security
- Software Exploitation via Hardware Exploitation (SExViaHEx) training by Xipiter
- CREST Registered Tester (Lapsed)
- Capable of attaining security clearance

Education

BSc in Computing, Leicester DeMontfort University. A Levels in physics, chemistry, and maths. GNVQ3 in Java Programming.

Community and Talks

I am one of the highest reputation users on Security StackExchange, with more than 1000 answers reaching over 9 million people.

I have spoken at quite a few conferences over the years:

- Netticon 2021 - *Unprivileged Driver Detection*
- Netticon 2021 - *From MSMQ to RCE*
- Netticon 2020 - *Evading EDR and AV with the world's worst pen drive* (data remenance in nonvolatile system components)
- Capital One Security Days 2019 - *Adopting TLS 1.3*
- BSides Leeds 2019 - *Hardware isn't hard* (updated)
- Securi-Tay 2019 - *Hardware isn't hard*
- Securi-Tay 2018 - *An Introduction to Binary Application Assessments*
- 44CON 2017 - *Secrets of the Motherboard* (x86 motherboard security issues)
- Securi-Tay 2017 - *SSL/TLS Hipsterism: Finding implementation bugs outside the mainstream*
- 44CON 2016 - *Saving Nostalgia* (reverse engineering and modifying Z80 hardware platforms)
- Securi-Tay 2016 - *Am I Living In A Box?* (novel VM and sandbox detections)
- DC4420 2015 - *VM detection via ACPI tables*
- 44CON 2015 - *Get in the ring0: Understanding Windows drivers*
- Securi-Tay 2015 - *We don't take kindly to your types around here!* (deserialisation bugs across languages)
- EMF Camp 2014 - *Minimal effort web application security*
- BSides London 2014 - *Breaking Binary Protocols and Bad Crypto*
- Securi-Tay 2014 - *Breaking bad crypto without breaking your brain*
- Securi-Tay 2013 - *Feed me a cat!* (embedded systems security)

Beyond work

Outside of work I enjoy stage lighting and lasers, DJing, tinkering with electronics, and making interactive art pieces. I have a strong interest in optics and colourimetry. I am a member of the Nullsector team at EMF Camp, where I help with custom electronics design, buildup and teardown, running the lasers, and developing the COVID safety infrastructure. I am also an organiser at NOVA Demoparty, a demoscene event that brings creative coders, artists, and musicians together to create interesting things on platforms of any age.