GRANT DOUGLAS

Practice Leader - Mobile Security LONDON, UK

DETAILS

London, UK
hello@hexplo.it

NATIONALITY
British

DRIVING LICENSE
Yes

LINKS

Recent Talks

Blog

LinkedIn

HOBBIES

Development, Travel, Chess, Video Games, Capture the flag, Reverse Engineering

PROFILE

I'm a driven and enthusiastic security consultant with a strong passion for all things mobile. I've been working in software security for almost seven years and previously studied Ethical Hacking at the University of Abertay, Scotland. I am London based but have enjoyed global travel for customers and internal business. I have strong skills in application security, particularly concerning iOS, Android, MDM/MAM, RASP, API testing, threat modeling, reverse engineering, code review, and more.

Additionally, I have designed and developed both internal and publicly available tooling which has been referenced in books such as iPhone Forensics and The Mobile Application Hacker's Handbook. My free time is usually spent with my wife, gaming, or writing code. On occasion, I enjoy participating in Capture the Flag's and bug bounties, and have received prizes/bounties from companies such as Facebook & Security Innovation

EMPLOYMENT HISTORY

Mobile Security Practice Director at Synopsys, Inc, London, UK

January 2019 – Present

Early in 2019 I assumed the role of practice director for Synopsys' mobile security services. This is the result of seven years of service, driving both my own personal development and supporting the growth of others via internal tooling, strategy contributions and leading large and sophisticated mobile consulting engagements of various team sizes.

As practice director, my responsibilities include building out and expanding the organization's current mobile security offerings and putting together and executing on a roadmap that works for various stakeholders throughout the organization including senior management, sales, marketing and consulting. This involves a continuous review of our intellectual property, consulting aids, sales materials, internal & external mobile security tooling, and more. All of this is key to the enrichment of quality, scale, and efficacy as the business continues to grows in size.

Associate Principal Consultant at Synopsys, Inc, London, UK

January 2018 – January 2019

As an Associate Principal Consultant, I am recognized both internally and externally as a highly technical subject matter expert in a particular domain. For myself, this domain is mobile security and I have developed and honed my skills over the last 10 years. I have designed, managed and delivered on various mobile security engagement types including application hardening reviews and designs (RASP, obfuscation, reverse engineering, malware, tampering), threat modeling of highly complex mobile solutions, mobile app penetration testing, API/Web service penetration testing, secure code review, authoring both security testing guidelines and secure development guidelines, Mobile Device Management (MDM) & Mobile Application Management (MAM) configuration review and effectiveness assessments, etc.

I have also authored multiple internal and external tools which have exposure in books such as iPhone Forensics and the Mobile Application Hacker's Handbook. My specific area of passion and focus is in application hardening - particularly concerning RASP, MDM/MAM, reverse engineering, and threat modeling. I have a particular interest and focus on business-critical apps, and work predominately with financial services & retail. I am also a proficient speaker having delivered multiple webinars, training sessions, and presentations to customers. In addition, I am also the author and instructor for multiple full day mobile security training courses that we deliver to customers around the world

Senior Security Consultant at Synopsys, London, UK

September 2016 – January 2018

As a senior consultant, I developed and honed strong leadership and technical skills in multiple areas of security, particularly in mobile. I was a key member of the mobile practice, working on internal tooling and driving company-wide strategic changes for mobile security assessments. I was and still am involved in formally mentoring and leading junior through senior members of the team.

Security Consultant at Synopsys Inc (Cigital prior to acquisition), London, UK

May 2013 – September 2016

As a security consultant I regularly participated in both off-site and on-site security assessments for clients. This included mobile penetration testing, code reviews in many languages, client presentations, risk analysis, MDM assessments, and much more. Topics included web security, thick clients, documentation review, instructor led training, source code review, mobile security, and more.

INTERNSHIPS

Summer Intern at NCR Corporation, Dundee, Scotland

June 2012 – September 2012

During my internship with NCR I spent several months performing vulnerability assessments and penetration testing of Automated Teller Machines (ATM). As a result, I was sponsored by NCR for my dissertation at university. The dissertation was titled a critical evaluation of ATM endpoint security, however is bound by NDA.

EDUCATION

University of Abertay, Dundee, Scotland

September 2009 – May 2013

Degree: BSc (hons) Ethical Hacking & Countermeasures

I graduated with a first class honours and the topics studied included: software development (C#/Java), database models & design, web application development (PHP), networking, mobile development (Android), computer and network security, penetration testing, exploit development, digital forensics, and multiple hacking modules.

NOTABLE PUBLIC RESEARCH

MEMSCAN

URL: https://github.com/hexploitable/memscan

Description

MEMSCAN is a macOS/iOS memory scanner which runs out-of-process on jailbroken devices. Via this technique it's possible to read and write memory to another process with a very high likelihood of not being detected. This is a useful utility for performing memory analysis but also for assisting reverse engineers in location particular code objects in memory, such as critical functions.

MEMSCAN was featured in books such as The Mobile Application Hacker's Handbook & Learning iOS Forensics.

TouchID Security

URL: https://synopsys.com/blogs/software-security/integrating-touch-id-into-ios-applications/

Description

I was one of the first security researchers to discuss the different approaches to securing applications using Touch ID upon release. I have written multiple posts on the topic and co-authored the first Touch ID bypass in the form of a tool called SuccessID which allowed penetration testers and developers to simulate all of the success/error codes on jailbroken iOS devices. Such bypasses are frequent now and are commonly available in most security tooling (e.g. Objection)

Certificate Pinning Research

Description

In late 2017 I identified a certificate pinning bypass in an open source communications library owned and maintained by Facebook. The library was in use by many of the App Store's most popular apps.

The timeline of events is illustrated below:

1. I reported the bug via Facebook's Whitehat program (facebook.com/whitehat) in March 2017.
2. 5 days later, Facebook respond with confirmation of the bug and reported that the team were investigating a fix.
3. In August 2017, Facebook responds with a solution and asks for acknowledgment of the issue being considered closed .
4. In September 2017, a bounty is paid, and my handle (@hexploitable) was added to their hall of fame.

REFERENCES

References available upon request