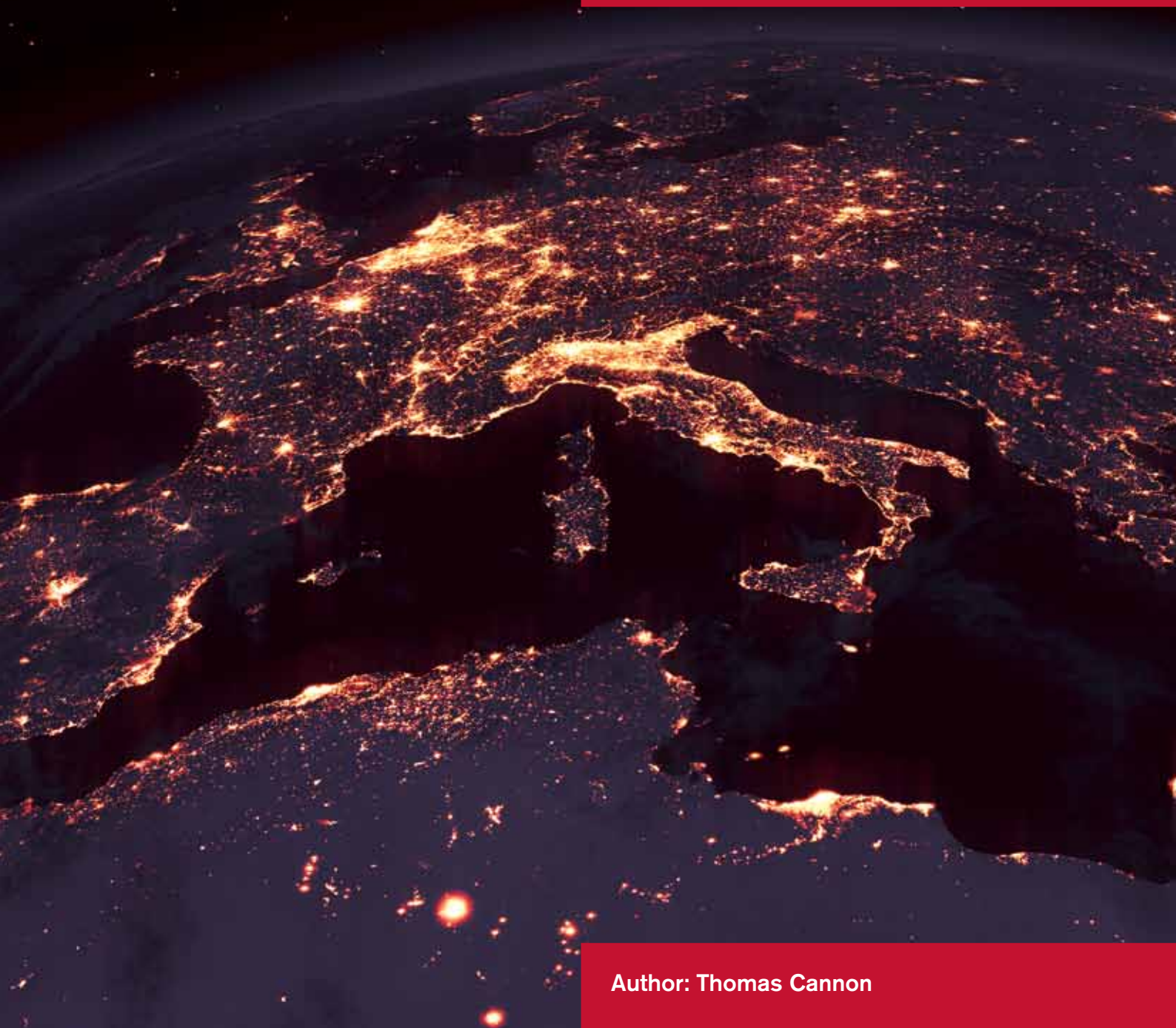
nccgroup
freedom from doubt

RESEARCH INSIGHTS

How we are breaking in: Mobile Security



Author: Thomas Cannon

CONTENTS

AUTHOR

THOMAS CANNON

Thomas has worked in the Information Security industry for over eight years holding a variety of roles. Prior to joining NCC Group, Thomas held the position of Director of R&D for mobile security firm NowSecure where he performed cutting edge research into mobile device exploitation. Thomas has led mobile security engagements for phone manufacturers, Government, banking, medical and the US Army. Thomas is active in the mobile security community, contributing to books, certification development, speaking engagements at DEF CON and launching an open source mobile security Linux distribution.

INTRODUCTION

The proliferation of the personal and business use of mobile devices has created a strong demand for mobile security assurance. Mobile apps and devices can suffer from many of the same vulnerabilities as traditional systems but also require new approaches to security testing and risk assessment. Some of the unique risks mobile introduces are:

- They can be exposed to hostile network environments (such as public WiFi)
- They remove data from the physical confines of a home or data centre and are at high risk of theft
- They typically are not protected with complex passcodes or two-factor authentication because it hampers usability
- They offer always-connected computing power with sensors such as camera, microphone, GPS, facilitating surveillance and remote access
- They are a new fast-changing platform with new attack techniques that developers are not experienced in protecting against

Given the amount of new risks that mobile introduces on top of traditional risks, it is perhaps not surprising to find a wide range of issues in a typical mobile assessment. This Research Insights aims to illustrate some of the common issues NCC Group finds within mobile.

How We Are Breaking In: Mobile Security

COMMON ISSUES IN MOBILE			
Data	**At Rest**	No Encryption	No encryption – Apps do not encrypt sensitive data, relying on OS controls to prevent access. This puts data at risk from malware and physical access in the event of a lost or stolen device.
		Not Erased	It is typical for apps to delete a sensitive, unencrypted file but leave it available to recovery with a forensic tool. NCC Group performs forensic techniques to see what data an app leaves behind.
		Poor Access Control	Apps which store data as world readable or on the SD Card (Android) make data available to any other app or malware.
	Transport	Improper SSL Handling	Apps which do not properly check the certificate of the server they are connecting to, or allow redirects to non-SSL connections, allowing Man in The Middle attacks
		No Certificate Pinning	SSL was designed for clients to securely connect to servers which are not known in advance, requiring trust of a central certificate authority to verify identity. Mobile apps usually know the backend server they are going to connect to, so can validate the certificate itself, protecting against rogue CAs or stolen certificates.
	Cached	UI Caching	An example would be a banking app for Android which displays a list of transactions and the user then logs out. Because Android does not actually terminate the app by design, that information can still be stored on the transaction screen and it is possible to directly invoke the screen to see the last data displayed there.
		Thumbnail Images	iOS devices take a screenshot when switching away from an app and if it is not disabled for sensitive screens it can include that data in the image.
		Browser	When using an embedded browser in an app it can cache data in the app's cache directory by default.
	Memory	Sensitive data not erased after use	Mobile devices are at higher risk of theft or loss and therefore NCC Group emulate a threat scenario where an attacker has access to a device and dumps the memory (RAM). This can reveal login credentials, encryption keys and other sensitive data.

It is clear from the output of mobile assessments over the last few years that data protection is not improving in mobile apps.

COMMON ISSUES IN MOBILE CONT...			
	Permissions	Incorrectly set or handled	Android apps can communicate with each other in a standard way to share data or invoke functionality. Such access is usually controlled via permissions but some apps set permissions incorrectly or export functionality unintentionally. This can result in data manipulation or leakage.
	Logs	Logging sesitive data	Logging data to the system log or including it in crash logs when the app crashes.
			There are some areas in mobile which are similar to both web and desktop regarding validation of data input.
	SQLite data	Database injection techniques	Mobile apps often store data in SQLite databases and are subject to SQL Injection. On Android there is a standard way to share data via inter-process communication and this is often mapped to queries of the app's data store. By supplying a malformed request, malware can sometimes cause a target app to execute SQL commands and reveal or manipulate data.
	Path validation	Traversal attacks	Apps which accept file names or paths as input do not always check for dangerous characters such as ".." which can be used to access or write to files which the attacker would not otherwise have permission to do.
	Exploit mitigation	ASLR and PIE not enabled	To better protect against issues such as buffer overflows due to malformed data, apps should be compiled with protection such as Position Independent Executable (PIE) and Address Space Layout Randomisation (ASLR).
	Reverse engineering	Lack of code obfuscation	It takes more effort for an attacker to reverse engineer an obfuscated app which is otherwise quite trivial on mobile platforms. While not directly protecting against vulnerabilities obfuscation does reduce the risk of a vulnerability being found and exploited.

CONCLUSION

It can be seen that the common issues on mobile are heavily biased towards data protection. Whereas traditional infrastructure assessment may be biased towards protecting against gaining entry in the first place, mobile testing has to assume the attacker already has some level of access. Access can be gained via malware installation, physical access or access to the network the device is connected to.

It is clear from the output of mobile assessments over the last few years that data protection is not improving in mobile apps. Mobile device manufacturers are improving their devices to help mitigate this problem with features such as:

- Fingerprint readers
- Full device encryption by default
- Explicitly requiring enablement of higher risk features
- Providing hardware backed secure data stores

Nevertheless, it is the responsibility of developers to ensure they protect their users and data regardless of platform security features.

Additionally NCC Group has seen new features of mobile platforms open up categories of issues that developers are failing to defend against. With mobile devices storing an ever increasing amount of sensitive data about our lives and work it is more important than ever to ensure it is being adequately protected.

With mobile devices storing an ever increasing amount of sensitive data about our lives and work it is more important than ever to ensure it is being adequately protected.

CONTACT US

0161 209 5200
response@nccgroup.trust
@nccgroupplc
www.nccgroup.trust

United Kingdom

Manchester - Head office
Manchester Technology Centre
Oxford Road
Manchester
M1 7EF

Cheltenham
Eagle Tower
Montpellier Drive
Cheltenham
GL50 1TA

Milton Keynes
Suite 526-528
Elder House
Eldergate
Milton Keynes
MK9 1LR

Edinburgh
37 York Place
Edinburgh
EH1 3HP

Leatherhead
Kings Court
Kingston Road
Leatherhead
KT22 7SL

Glasgow
The Beacon
176 St Vincent Street
Glasgow
G2 5SG

London
Floor 4
Tavistock House North
London
WC1H 9HR

Europe

Switzerland
Ibelweg 18A
CH-6300 Zug
Switzerland

The Netherlands
Veemkade 396
1019 HE Amsterdam
The Netherlands

Germany
Heimeranstrasse 37
D-80339 Munchen
Germany

Denmark
Tranevej 16-18
DK-2400 Kobehavn NV
Copenhagen
Denmark

North America

San Francisco
Suite 1020
123 Mission Street
San Francisco
CA 94105

Texas
4029 South Capital of Texas Hwy
Suite 100
Austin, TX 78704

New York
39 W. 14th St.
Suite 202
New York
NY 10011

Chicago
53 W.Jackson
Suite 464
Chicago, IL 60604
USA

Seattle
720 3rd Avenue
Suite 2101
Seattle

Sunnyvale
111 West Evelyn Avenue
Suite 101/103
Sunnyvale, CA 94086

Asia Pacific

Australia
2.08/56 Bowman street
Pyrmont NSW 2009
Australia

www.nccgroup.trust
@nccgroupplc