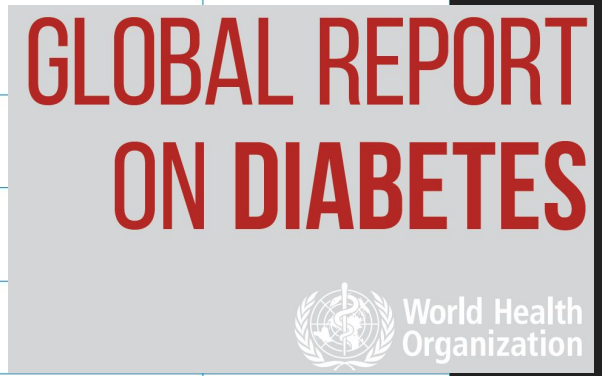
Security of diabetes monitoring apps

Research project 1
Security and Network Engineering
Edgar Bohte & Roy Vermeulen

Why diabetes?

TABLE 2. ESTIMATED PREVALENCE AND NUMBER OF PEOPLE WITH DIABETES (ADULTS 18+ YEARS)

WHO Region	Prevalence (%)	Number (millions)	Number (millions)	
	2014	2014	1980	2014
African Region	7.1%	25	4	25
Region of the Americas	8.3%	62	18	62
Eastern Mediterranean Region	13.7%	43		
European Region	7.3%	64		
South-East Asia Region	8.6%	96		
Western Pacific Region	8.4%	131		
Total[a]	**8.5%**	**422**	**108**	**422**



LOSS OF VISION

Diabetic retinopathy caused 1.9% of moderate or severe visual impairment globally and 2.6% of blindness in 2010 *(20)*.

CARDIOVASCULAR EVENTS

Adults with diabetes historically have a two or three times higher rate of cardiovascular disease (CVD) than adults without diabetes

END-STAGE RENAL DISEASE

Pooled data from 54 countries show that at least 80% of cases of end-stage renal disease (ESRD) are caused by diabetes, hypertension or a combination of the two

LOWER EXTREMITY AMPUTATIONS

Diabetes appears to dramatically increase the risk of lower extremity amputation because of infected, non-healing foot ulcers *(19)*.

The upside

People with diabetes can live long and healthy lives if their diabetes is detected and well-managed.

The role of blood glucose control in preventing the development and progression of complications has been proven in both type 1 and type 2 diabetes,

Self-monitoring of blood glucose is recommended for patients receiving insulin,

GLOBAL REPORT ON DIABETES

Smartphone app security

Our findings reveal that the majority of the analyzed applications do not follow well-known practices and guidelines, not even legal restrictions imposed by contemporary data protection regulations, thus jeopardizing the privacy of millions of users.

Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice

ACHILLEAS PAPAGEORGIOU[1], (Member, IEEE), MICHAEL STRIGKOS[1], EUGENIA POLITOU[1], (Member, IEEE), EFTHIMIOS ALEPIS[1], (Member, IEEE), AGUSTI SOLANAS[2], (Senior Member, IEEE), AND CONSTANTINOS PATSAKIS[1], (Member, IEEE)

We applied Stowaway to 940 Android applications and found that about one-third of them are overprivileged.

Android Permissions Demystified

Adrienne Porter Felt, Erika Chin, Steve Hanna, Dawn Song, David Wagner

Health data confidentiality

Healthcare data is substantially more valuable than any other data.

Uses extend to sophisticated fraud perpetrated by organized crime.

Ongoing publicity associated with large breaches may compromise patient trust which could result in less willingness to share data.

Cybersecurity in healthcare: A narrative review of trends, threats and ways forward

Lynne Coventry*, Dawn Branley

Next we consider threat agents. Some examples are:

- **Health insurance companies** who may seek to gain advantage by learning health information which is not normally part of their review procedures.

Security Testing for Android mHealth Apps

Konstantin Knorr David Aspinall

Diabetes data integrity

- Hyperglycaemia

Symptoms of hyperglycaemia include:

- tiredness
- blurred vision

Regularly having high blood sugar levels for long periods of time (over months or years) can result in permanent damage to parts of the body such as the eyes, nerves, kidneys and blood vessels.

NHS

- Hypoglycaemia

Early symptoms include weakness, lightheadedness, and dizziness. Headaches can occur from a lack of glucose, especially if you have diabetes.

You may also feel signs of stress, such as nervousness, anxiety, and irritability.

Untreated, severe low blood sugar can be very dangerous. It can result in seizures, loss of consciousness, or death.

healthline

Research question

- What is the current state of security in diabetes blood glucose monitoring apps?

1. How can an unauthorized third party derive data from the glucose monitoring apps?
2. Which data can be derived from these apps by an unauthorized third party?
3. How can an unauthorized third party alter the data in these apps?

Selecting apps

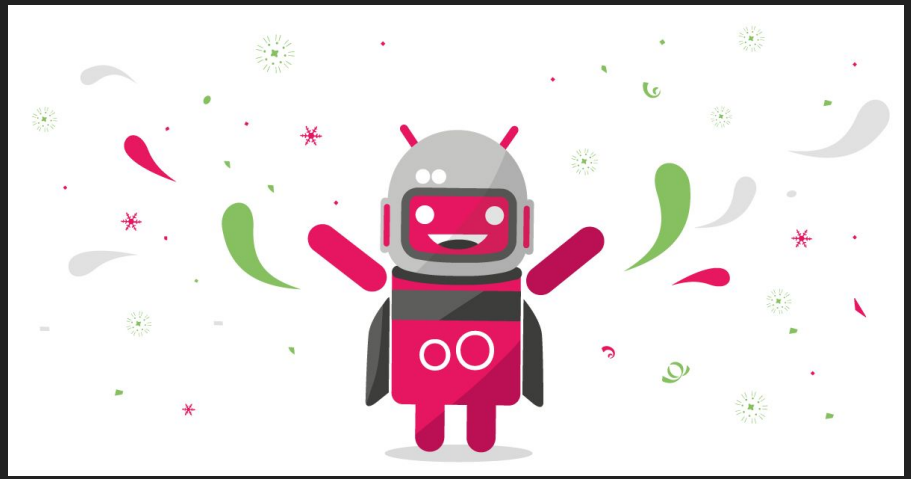
- 3 apps
- Only android apps
- Selected by popularity

Emulation

- Genymotion
- Android 8.0 Oreo

GENYMOTION
By Genymobile

a)



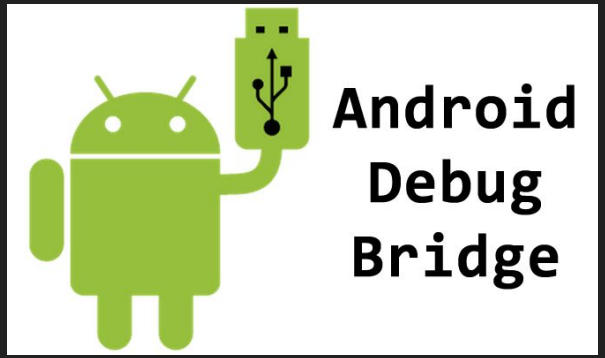
a)

Tools

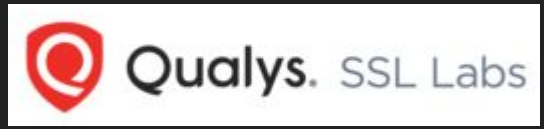
b)


MOBSF

c)


Android
Debug
Bridge

d)


Qualys. SSL Labs

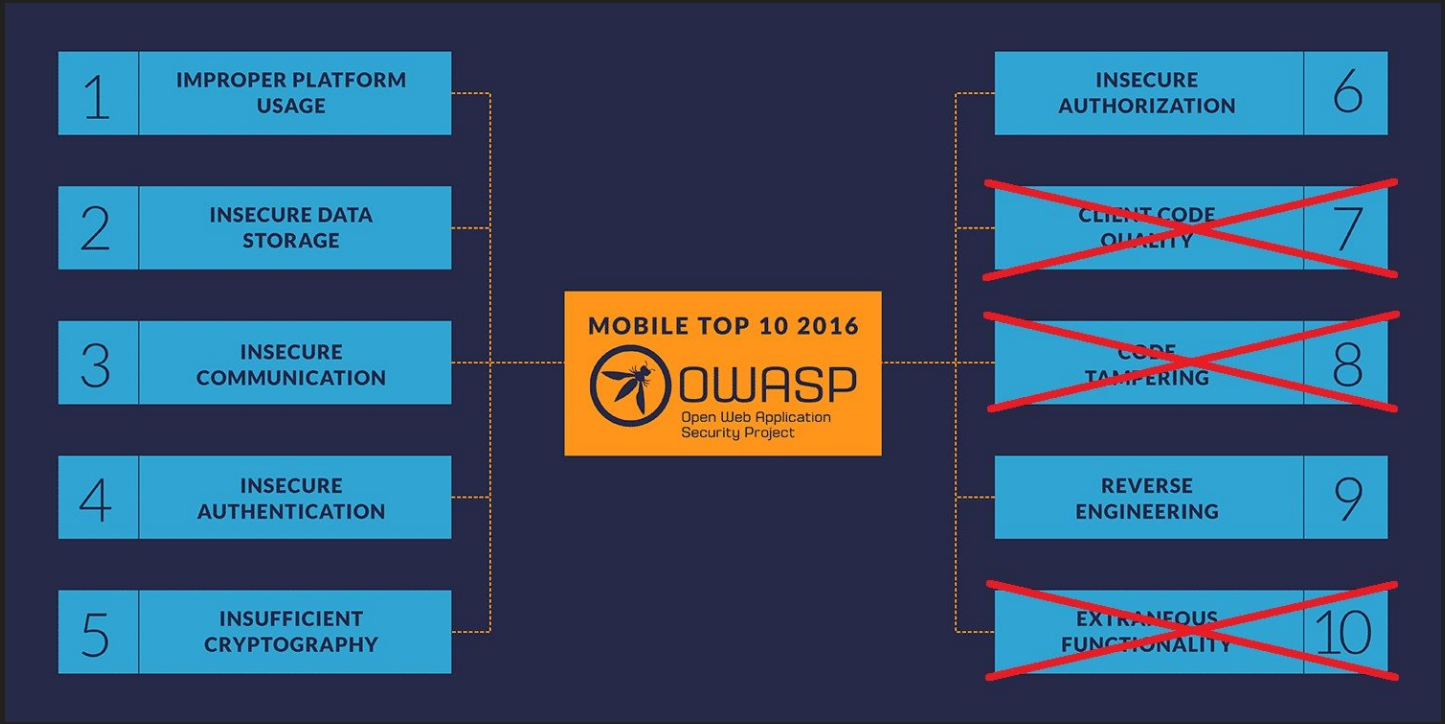
e)


Security
Report
drozer
Android Security Assessment Framework

f)


BURPSUITE

OWASP framework



o)

M1: Improper Platform Usage

	M1: Improper Platform Usage
App 1	
App 2	Activities every app can call
App 3	Activities every app can call

M2: Insecure Data Storage

	M2: Insecure Data Storage
App 1	Authentication is in logs
App 2	Database not encrypted
App 3	Glucose level in logs

M3: Insecure Communication

	M3: Insecure Communication
App 1	Uses HTTP connection
App 2	
App 3	

M4: Insecure Authentication

	M4: Insecure Authentication
App 1	Authentication token duration valid
App 2	Not able to log out
App 3	Authentication token generation

M5: Insufficient Cryptography

M6: Insecure Authorization

	M6: Insecure Authorization
App 1	Insecure link generation for sharing data
App 2	
App 3	Authorization check export archived data

Link generation

- Character space a-z A-Z 0-9
- 4 characters long
- http://example.link/**i1Db**
- http://example.link/**j1Db**

  .

  .

  .
- http://example.link/**91Db**
- http://example.link/**a2Db**

M6: Insecure Authorization

	M6: Insecure Authorization
App 1	Insecure link generation for sharing data
App 2	
App 3	Authorization check export archived data

M9: Reverse Engineering

	M9: Reverse Engineering
App 1	
App 2	
App 3	

Scoring overview

	M1	M2	M3	M4	M6	M9
App 1						
App 2						
App 3						

App 1 exploit

- Authentication token in logs
- Duration Authentication token stays valid

Access level	**Requirements**
read and write	malicious app or access physical device

App 2 exploit

- Get data via unencrypted database

Access level	**Requirements**
read and write	root

App 3 exploit

- Get unencrypted email and password
- Use them to get authentication code

Access level	Requirements
read and write	root

- Get data via export archived data

Access level	Requirements
read	Connect to server and an account

Conclusion

- What is the current state of security in diabetes blood glucose monitoring apps?
- Storage and authentication biggest problem
- Obtain medical data from all apps
- Modify medical data 2 out of 3 apps
- Most found vulnerabilities rely on physical access or malicious app

Future work

- Other OS (iOS)
- More apps (paid for apps)
- Invasive server testing
- Apps connecting to sensor

Thank you for your attention

image sources:

a) images by Genymotion (https://www.genymotion.com/)
b) image from kali linux tutorials (https://kalilinuxtutorials.com/mobsf-mobile-security-framework/)
c) image from android community (https://androidcommunity.com/how-to-getting-adb-on-your-pc-without-installing-full-android-sdk-20180307/)
d) image by Qualys (https://community.qualys.com/community/ssllabs)
e) image from effect hacking (http://www.effecthacking.com/2016/01/drozer-android-security-assessment-framework.html)
f) image from ehacking.net (https://academy.ehacking.net/p/burp-suite-web-penetration-testing)