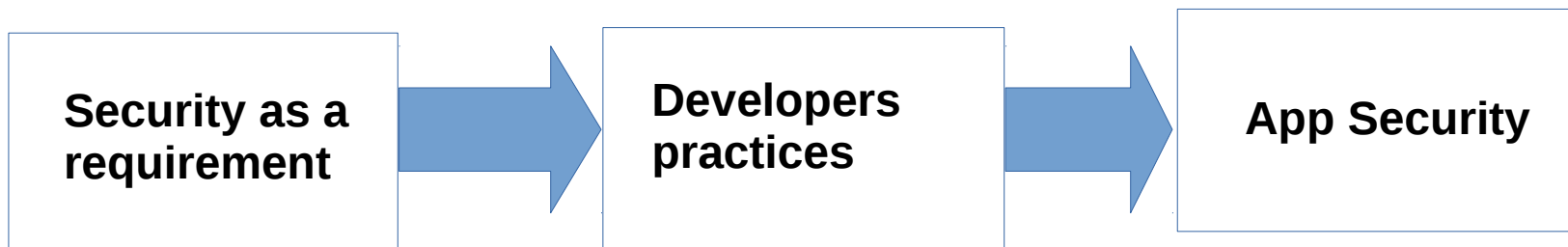


“From Needs to Actions to Secure Apps? The Effect of Requirements and Developer Practices on App Security”

Presented by: Lamees Elhiny

Objective

Finding if security as a requirement and a practice can lead to the development of more secure Apps



How to measure or evaluate Developer Practices?

- A survey was done for experienced Android developers to evaluate:
 - How they planned for App security
 - Whether they consulted security experts or not
 - The security checks done while developing the App
 - Assurance techniques used
 - Security updates performed

This study investigates the relation between developers' behavior in terms of security practices and its effect on developing more secure Apps by finding answers to TWO Questions **RQ1** and **RQ2**



RQ1---> Does the need for privacy lead to better developer practices?

- A group of professional android developers were chosen
- A survey focusing on security practices was conducted among the developers
- A well documented approach was taken on every step of the survey



RQ1 Findings and Statistics

Android Developers (Total 330)	Security Practices
<= 22%	Regularly access security professionals
<= 53%	Use basic assurance techniques
<= 30%	Run security updates for apps less than once a year
<= 15%	Perform minor changes due to new GDPR legislation

RQ1 Findings and Statistics(cont.)

 Need for security in requirements --->  Assurance techniques applied

 Need for security in requirements <--->  Security experts<----->

 Assurance techniques<--->  Security updates

RQ2---> To what degree developers practices lead to more secure Apps?

- Android Apps developed by the professional developers who took the survey were analyzed to find security defects
- The results of the survey (Survey Scores) were compared with detected App security defects

RQ2 Findings

- **No relation** was proven between different **developers practices** (security as a demand, assurance techniques used, and frequent security updates) and **the number of security issues** in the Apps
- The big surprise was **more cryptographic APIs** issues were reported in Apps in which **security professionals** were involved

Survey Description

- In May 2019, a transparent online survey was conducted for Google Play Android professional developers (**345 developers participated**)
- The survey was **pretested** and got **modified** to cover two more research questions:

RQ3---> What is the percentage of Android developers having access to security professionals?

RQ4---> How frequent assurance techniques were used?

Survey Description (cont.)

- The survey covered five prominent assurance techniques:
 - Threat Assessment
 - Configuration Review
 - Automated Static Analysis
 - Code Review
 - Penetration Testing

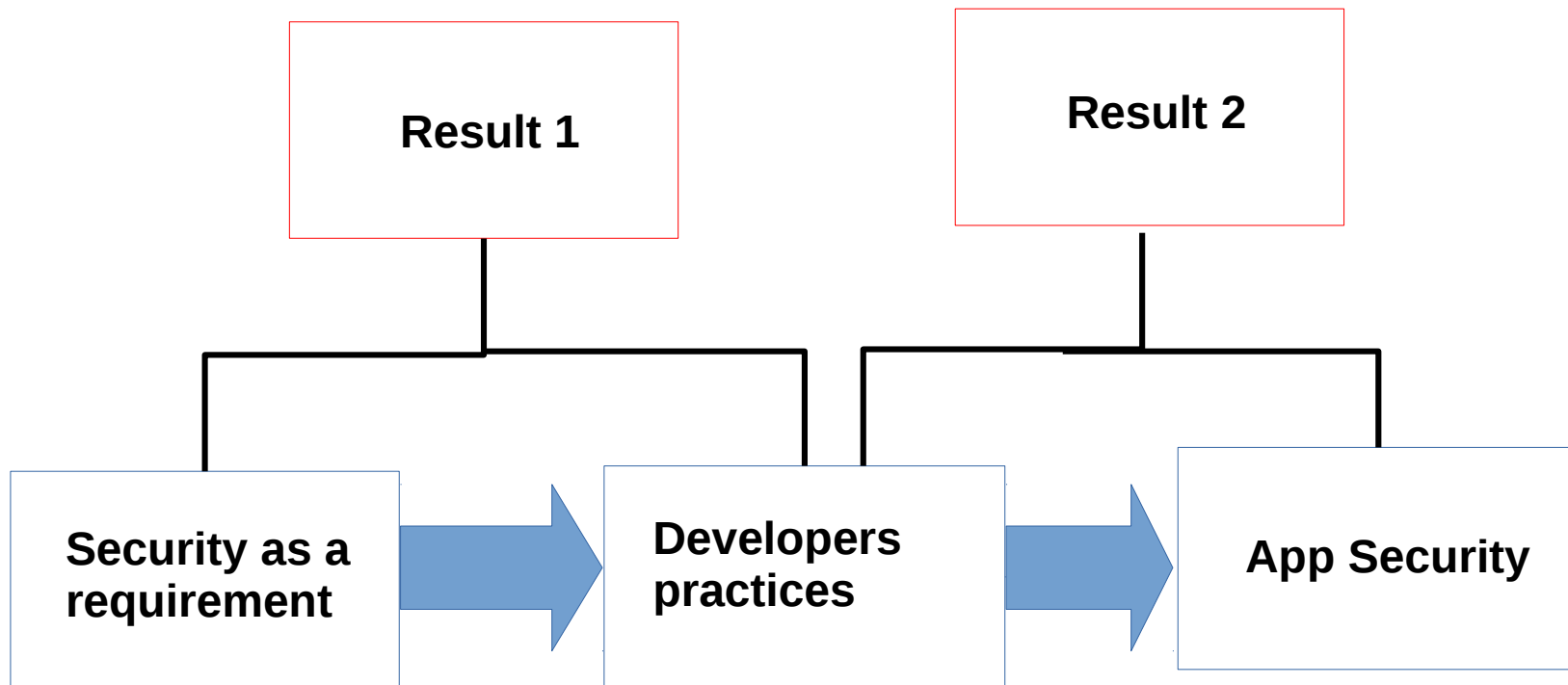
Application Analysis Methodology

- App binary was downloaded for each survey participant
- The Apps got tested using mature tools available to Android developers
- The issues for each App were counted and a given score was calculated

Application Analysis Methodology (cont.)

- The analysis covered three main aspects:
 - *SSL Security*
 - using correct ssl connections when remotely communicating
 - Tools: **curl**, **openssl**
 - *Cryptographic API Misuse*
 - Make sure that Java Cryptographic APIs are used properly
 - Tools: **CogniCrypt**
 - *Privacy Leaks*
 - To detect harmful data flow in the code that might violate privacy
 - Tools: **FlowDroid**

Results And Statistics



Result 1: “Linear Analysis of Developer Survey Scores”

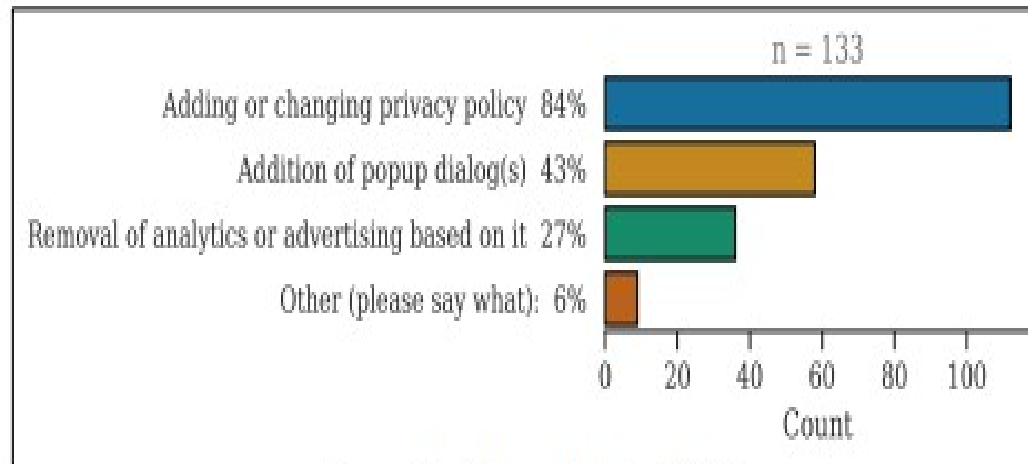


Figure 12: Changes Due to GDPR

Result 1 (cont.)

Table 1: Pearson R Results (R, P) for Developer Survey Security Scores

Dependent:	Independent:	Expertise Support	Requirements	Developer Knowledge	Assurance Technique Use
Assurance Technique Use		0.56, 3.9e-25	0.37, 1.5e-11	0.27, 8.6e-07	
Security Update Frequency		0.16, 0.0085	0.25, 2e-05	0.03, 0.61	0.41, 5.7e-13

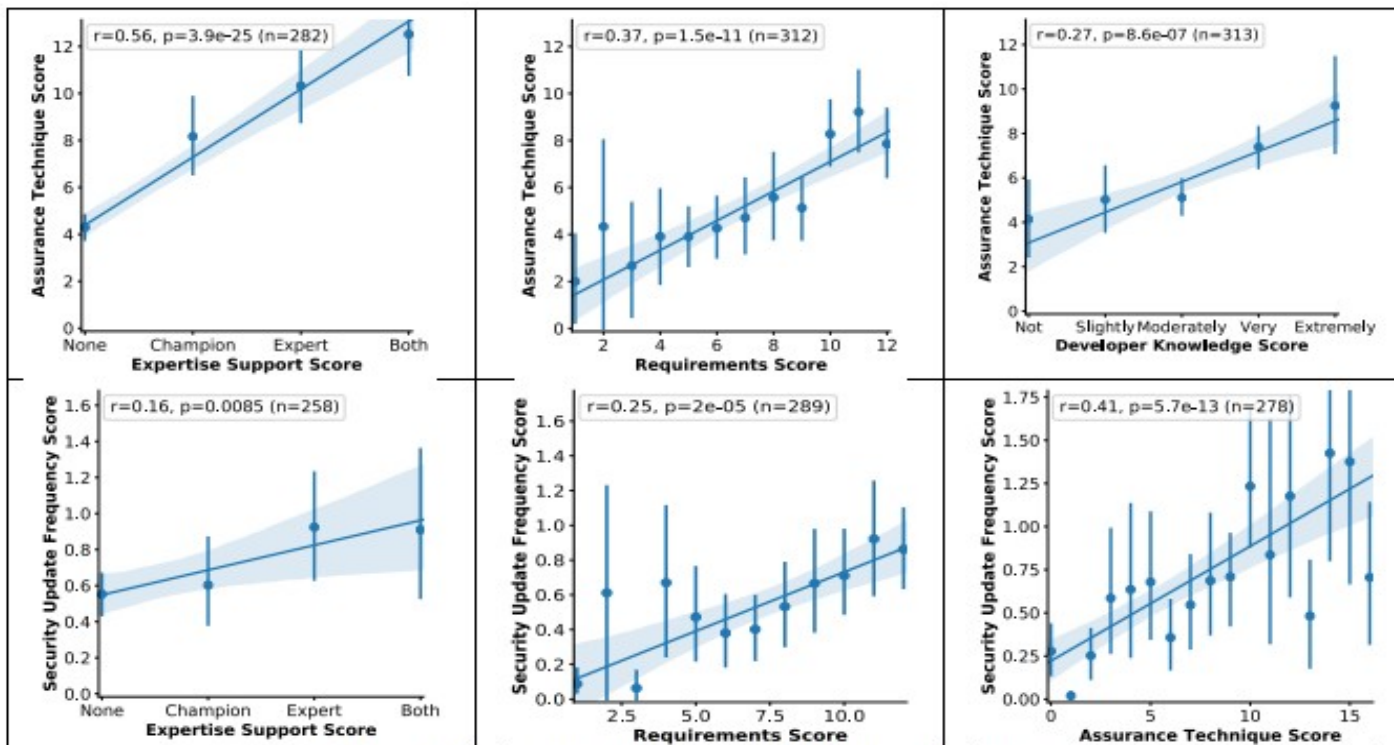


Figure 13: Cross-plots of the Scores with Significant Correlations

Result 2: “Linear Analysis of App Analysis Score”

Table 2: Pearson R Results (R, P) Correlating App Security Measurements with Developer-based Factors

Dependent:	Independent:	Expertise Support	Requirements	Developer Knowledge	Assurance Technique Use
Cryptographic API Misuse		-0.17, 0.016	-0.06, 0.37	-0.09, 0.17	-0.13, 0.047
Privacy Leak		-0.09, 0.20	-0.01, 0.85	0.02, 0.81	0.02, 0.81
SSL Security		-0.14, 0.049	0.01, 0.93	-0.02, 0.76	-0.08, 0.20

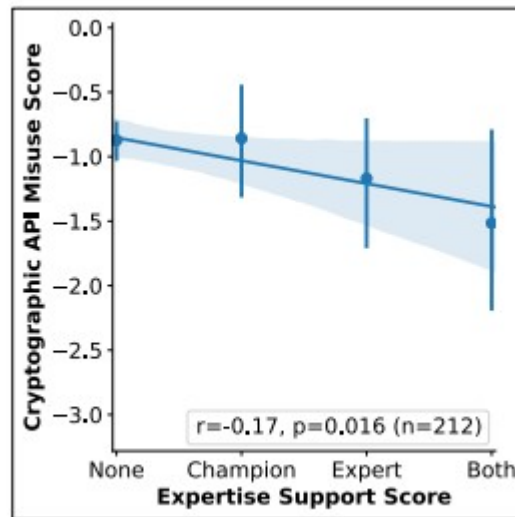


Figure 14: Worse Cryptosecurity with Expert Involvement?

Discussion

- Positive findings in Result 1, **60%** of developers involved consider *security* and *privacy* extremely important
- Security experts led to more *assurance techniques* used and *security updates*
- In general, *security as a requirement* led to more *security practices*
- However, **GDPR** legislations were not strong enough to improve app security and practices

Discussion

- Security practices are costly, not supposed to be used unless required
- Result 2 could **not correlate** developers practices to App Security; could be due to:
 - Involving libraries in analysis
 - Limited capabilities of tools
- Also, *Cryptographic APIs issues* resulted from *professionals involvement* is due to the use of **more Cryptographic APIs** when they get involved

References

[Weir-USENIX20] Weir, Charles, Ben Hermann, and Sascha Fahl, From Needs to Actions to Secure Apps? The Effect of Requirements and Developer Practices on App Security, In the 29th USENIX Security Symposium, pp. 289-305, 2020.

Thank You!