Security Lancaster | Lancaster University

ARTIFACT EVALUATED usenix ASSOCIATION PASSED

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

USENIX Security - August 2020

Charles Weir
Lancaster University

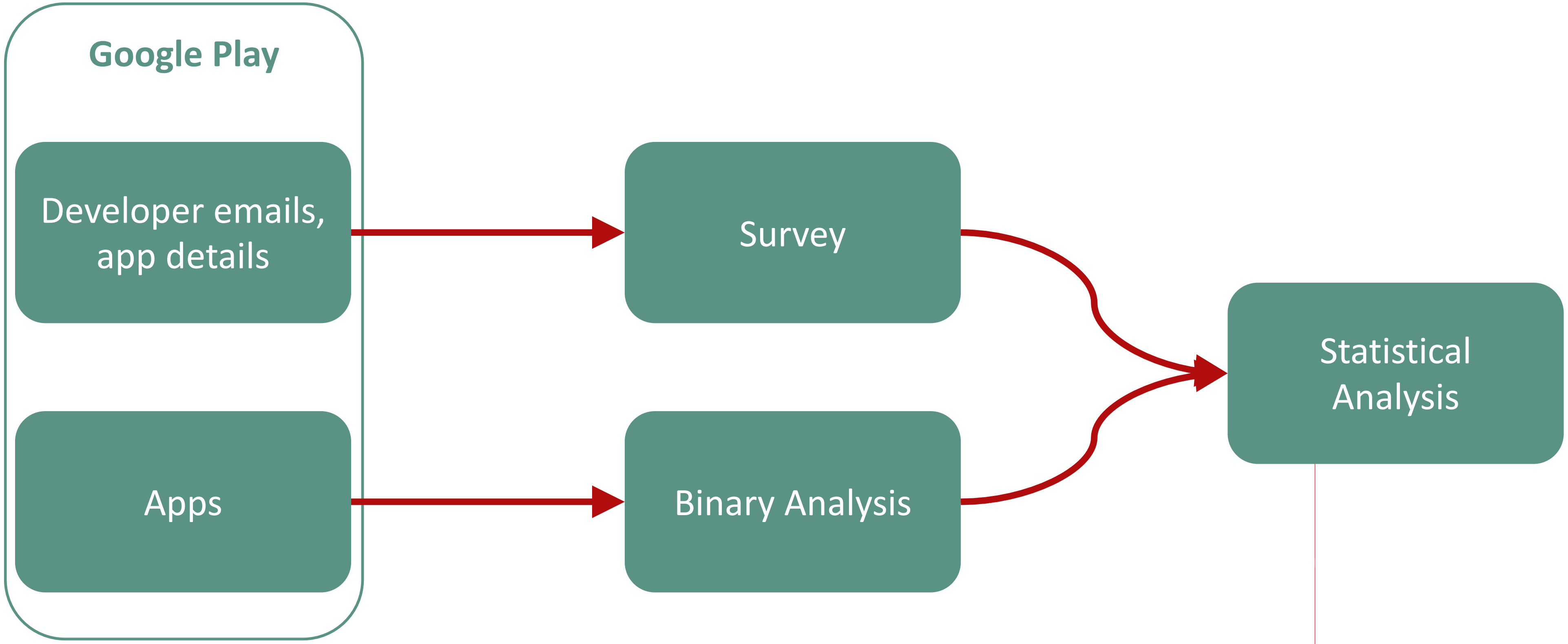
Ben Hermann
Paderborn University

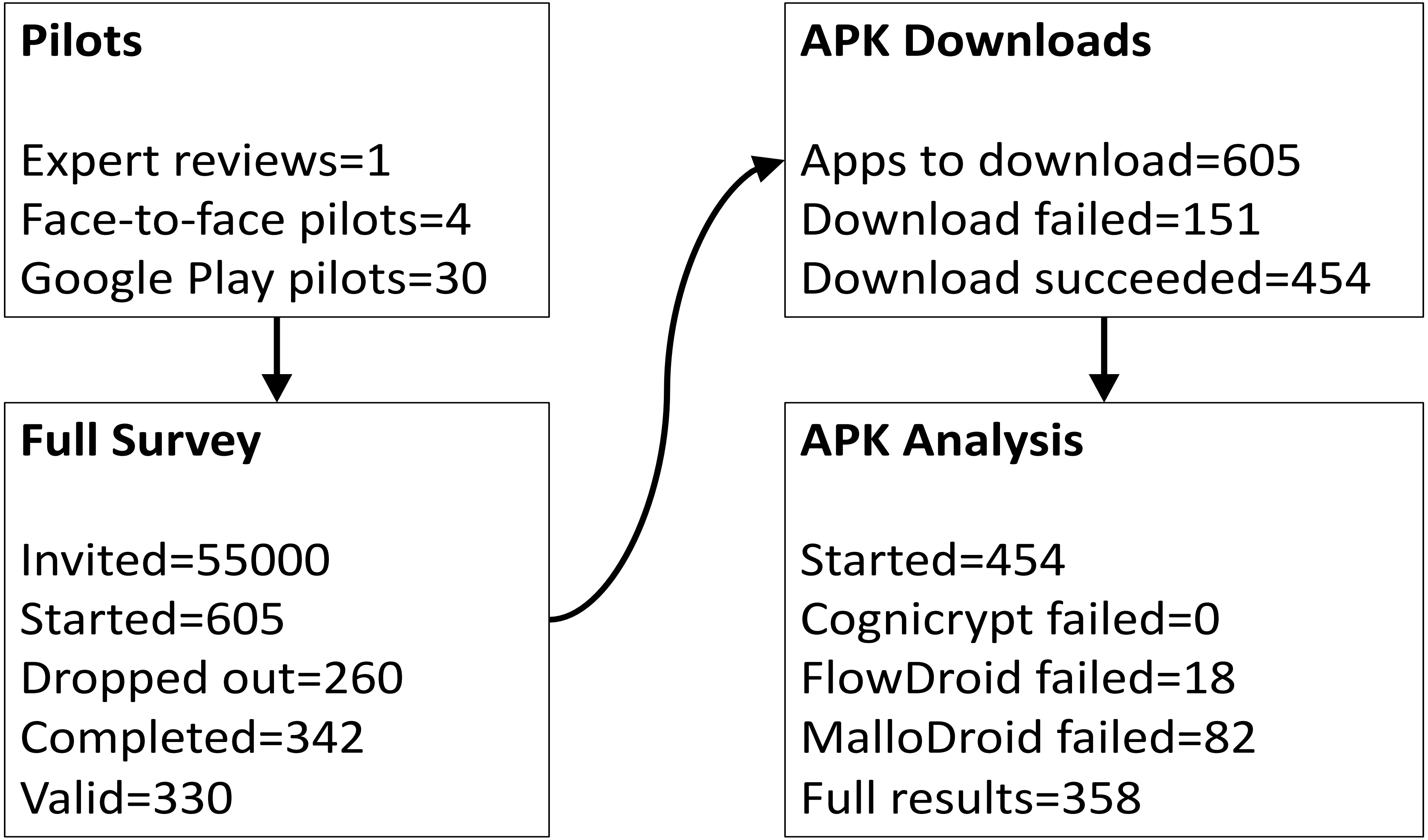
Sascha Fahl
L. University Hannover

Research Question

To what extent, and how,
does a perceived need for security and privacy
lead to security-enhancing activities …
in the development team?

Survey Concept





Developer Questionnaire

Pilots

Expert reviews=1
Face-to-face pilots=4
Google Play pilots=30

Full Survey

Invited=55000
Started=605
Dropped out=260
Completed=342
Valid=330

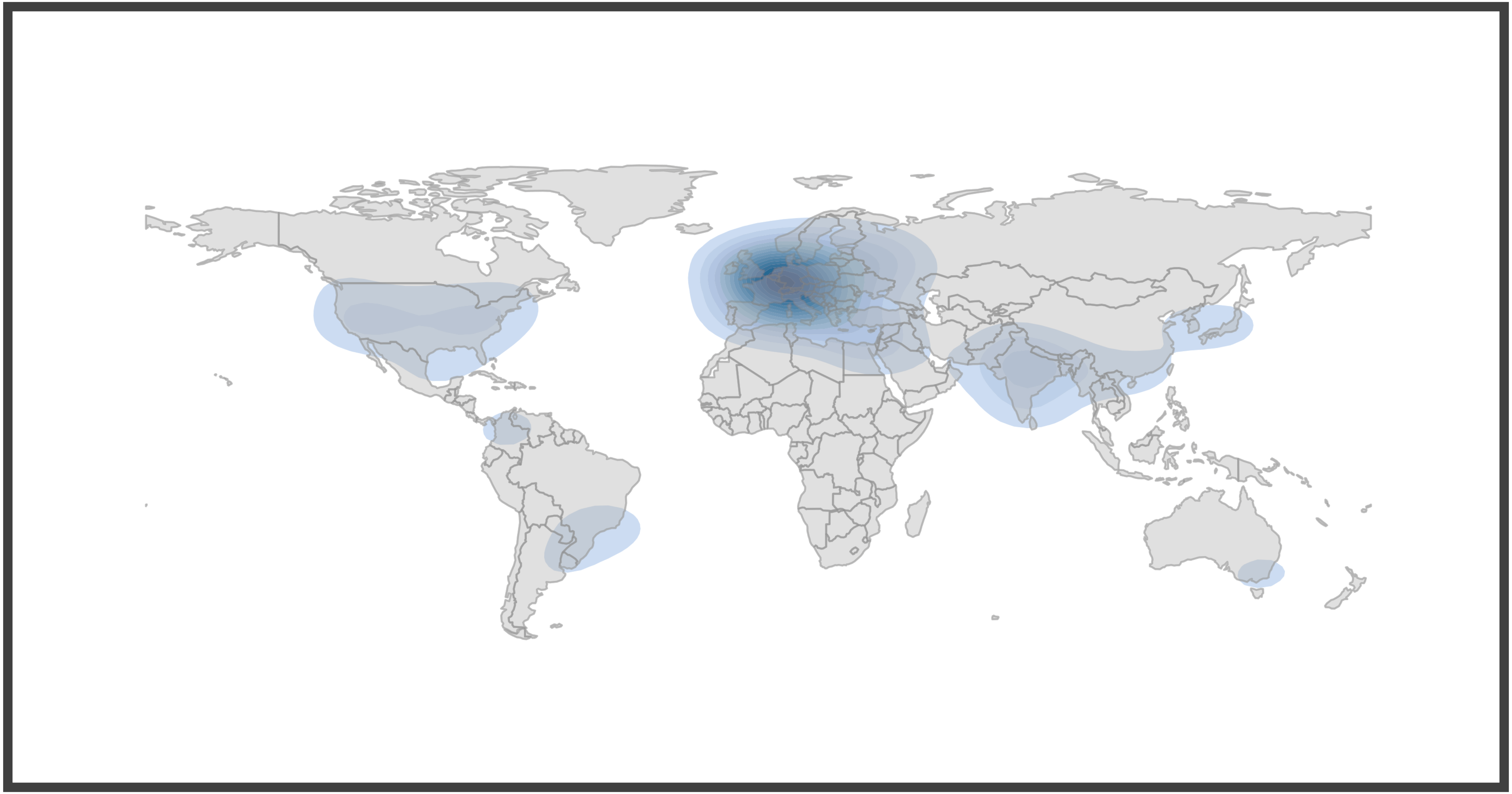
App Analysis

APK Downloads

Apps to download=605
Download failed=151
Download succeeded=454

APK Analysis

Started=454
Cognicrypt failed=0
FlowDroid failed=18
MalloDroid failed=82
Full results=358

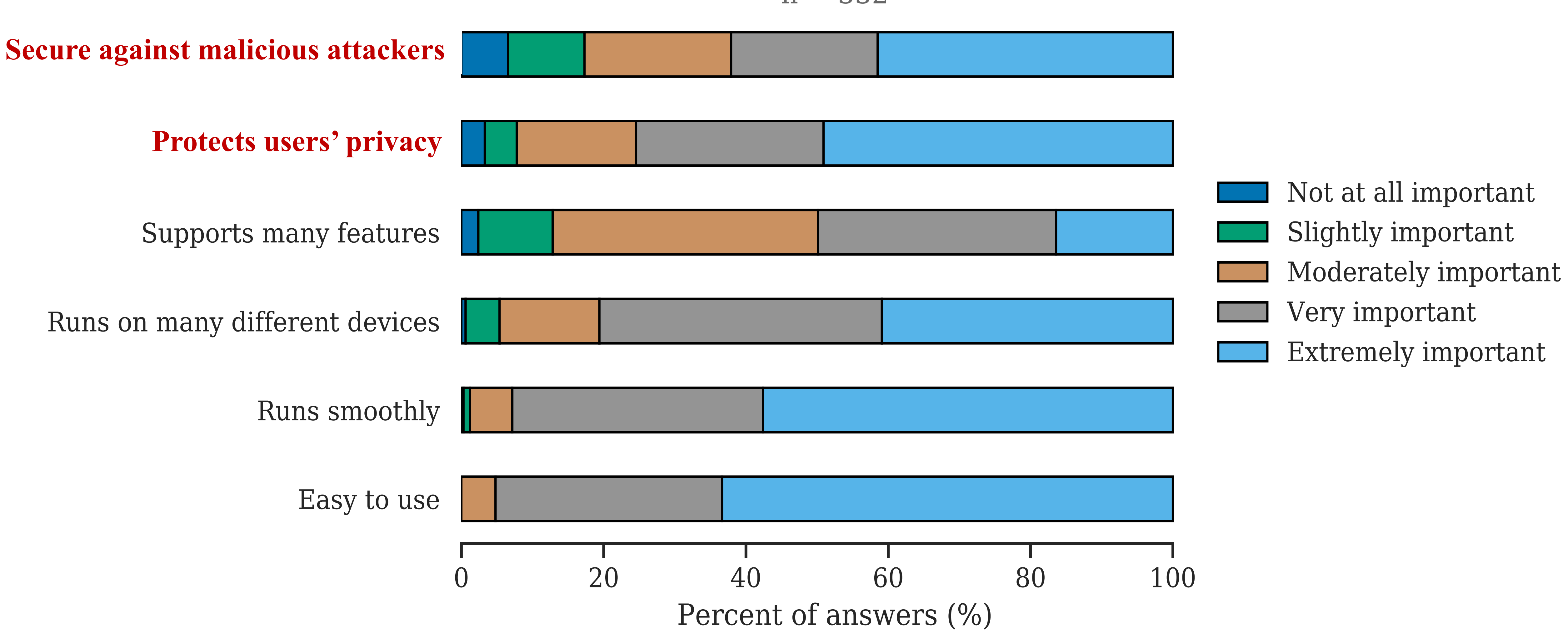


Discussing the Results

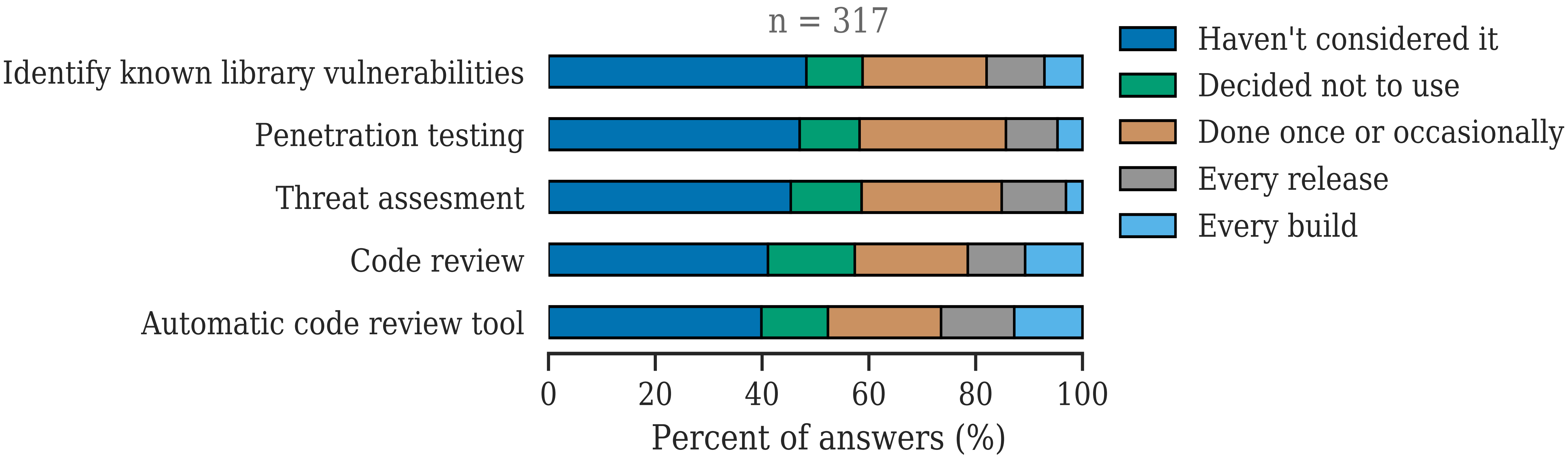
Description of the Survey Data

Relationships in the Survey Data

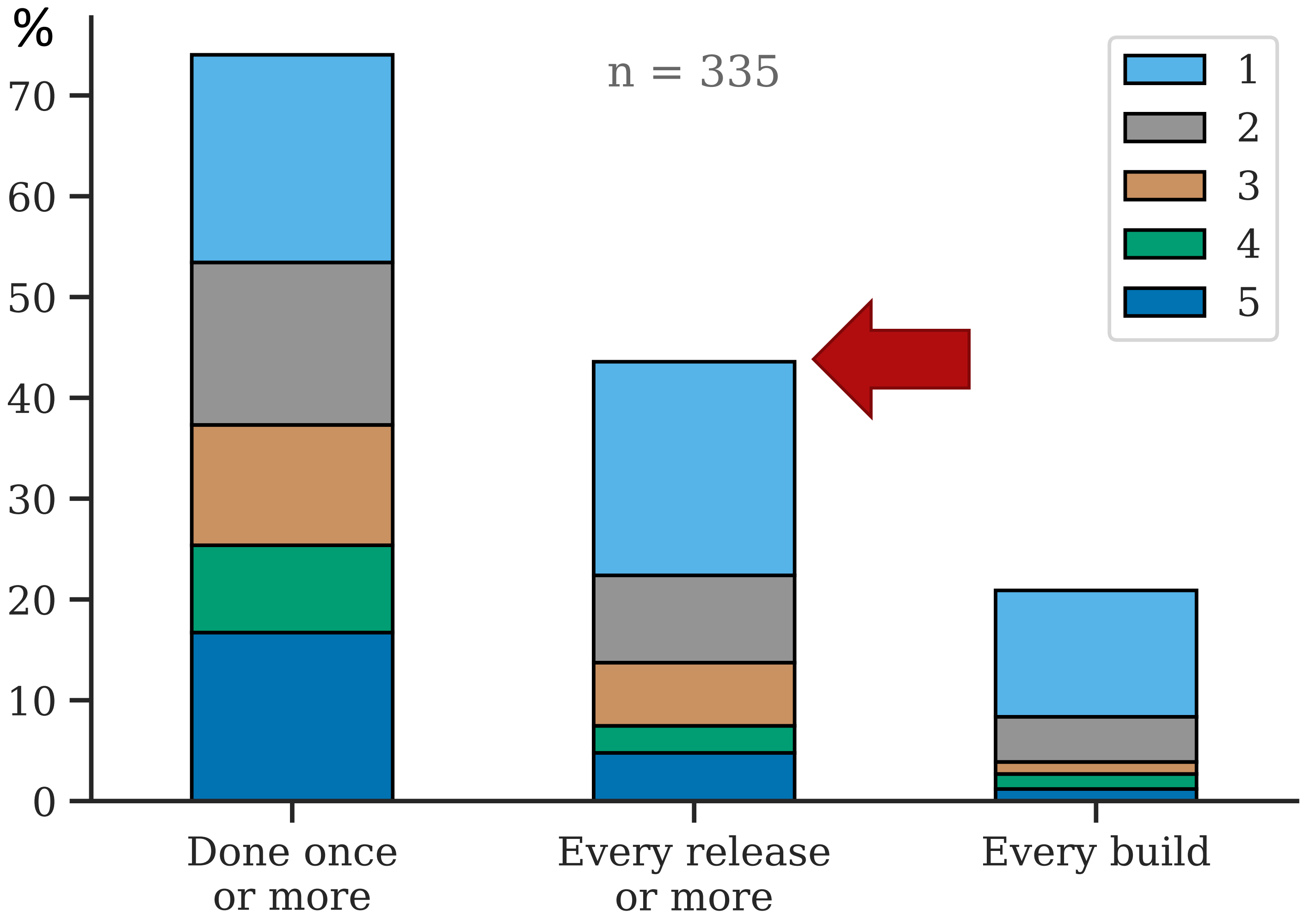
Adding the Binary App Analysis



Importance of Different Requirements



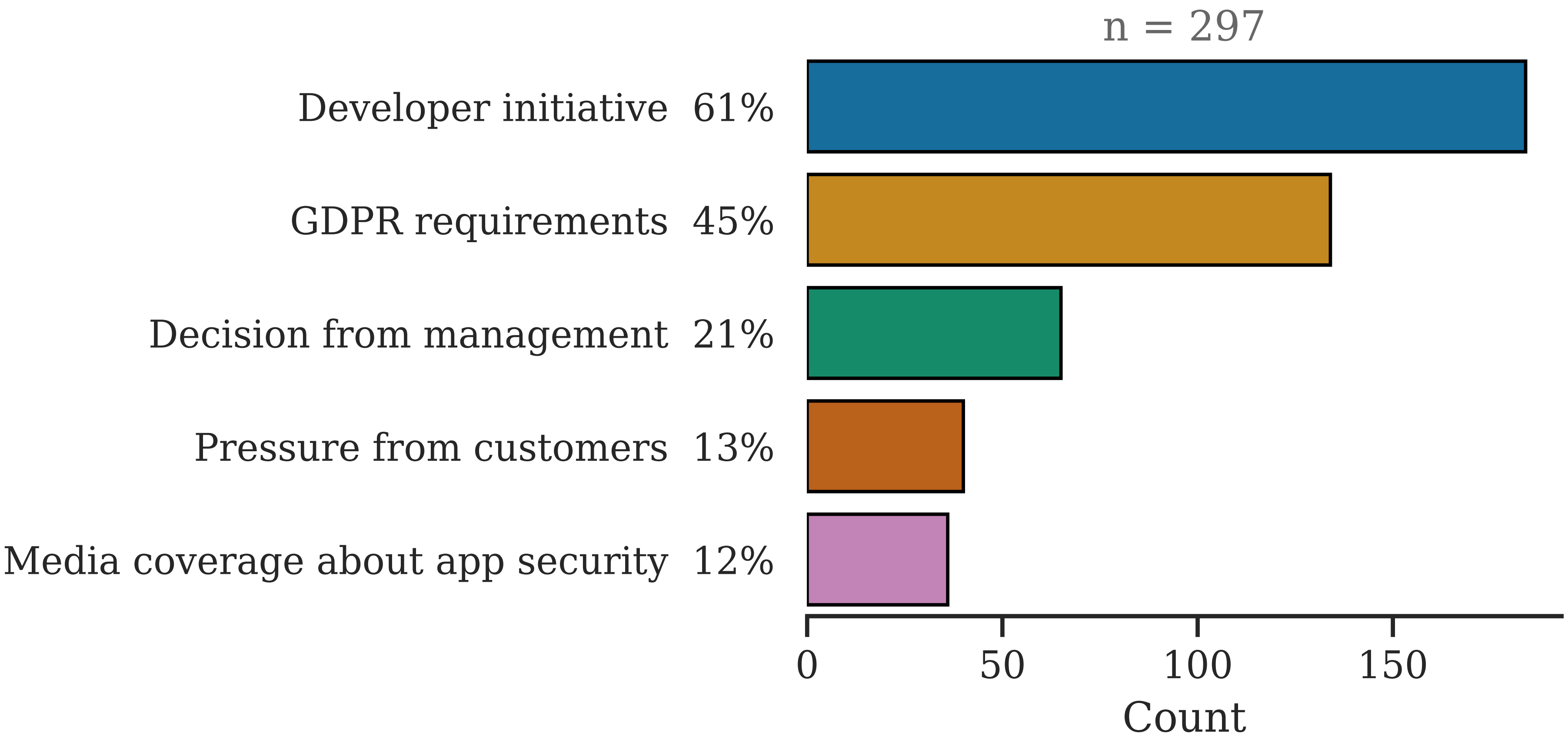
Use of Assurance Techniques



# Assurance Techniques Used

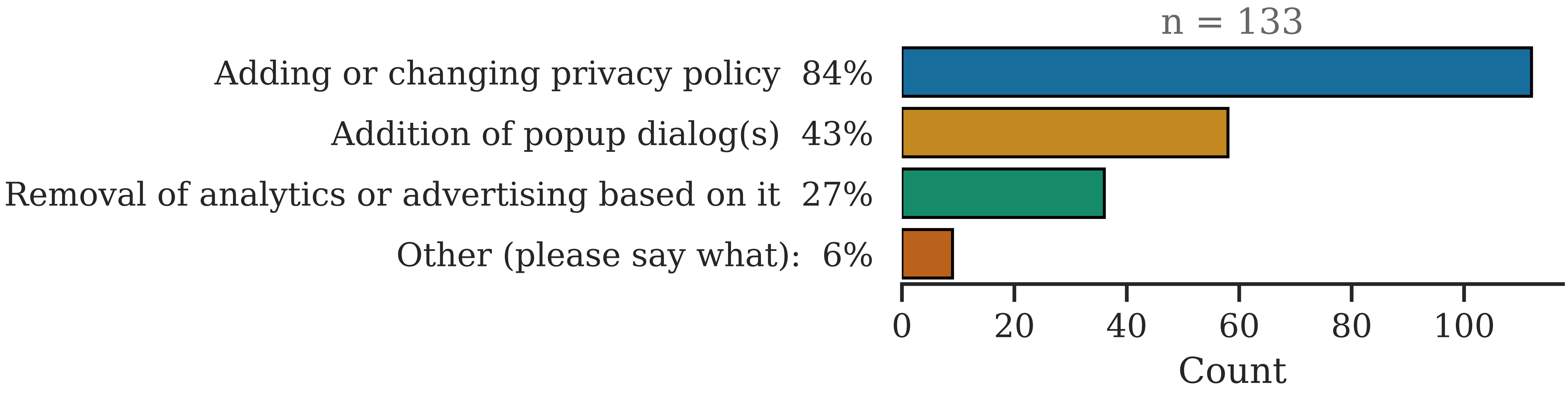
Adoption of Assurance Techniques

First Technique	Second Technique	Proportion
Automatic Code Review	Automatic Library Vulnerabilities	38%
Automatic Code Review	Code Review	32%
Code Review	Automatic Library Vulnerabilities	22%
Threat Assessment	Code Review	16%

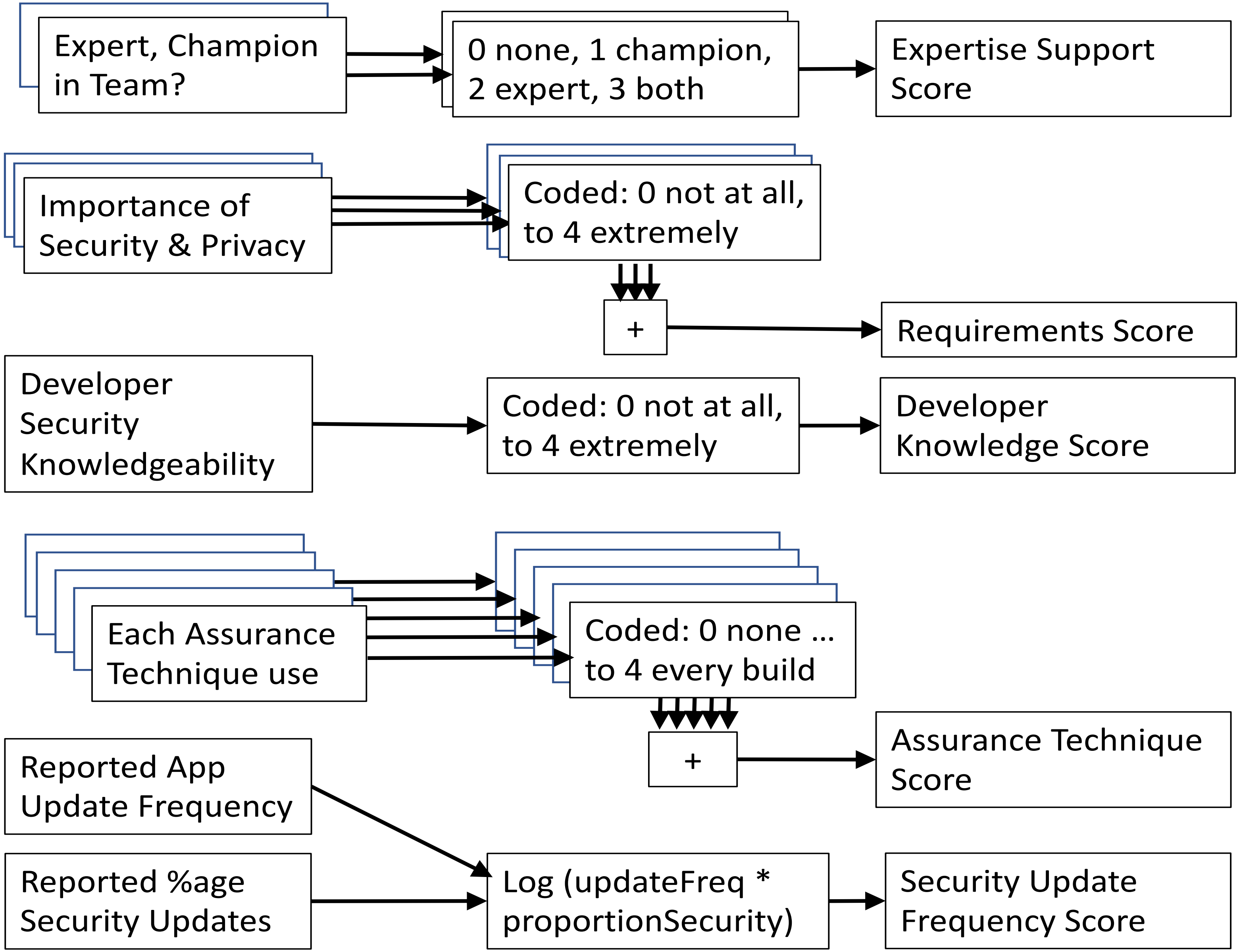


Reasons for Security Changes

GDPR Changes



Relationships in the Survey Data



Expert, Champion in Team?

0 none, 1 champion, 2 expert, 3 both

Expertise Support Score

Importance of Security & Privacy

Coded: 0 not at all, to 4 extremely

+

Requirements Score

Developer Security Knowledgeability

Coded: 0 not at all, to 4 extremely

Developer Knowledge Score

Each Assurance Technique use

Coded: 0 none … to 4 every build

+

Assurance Technique Score

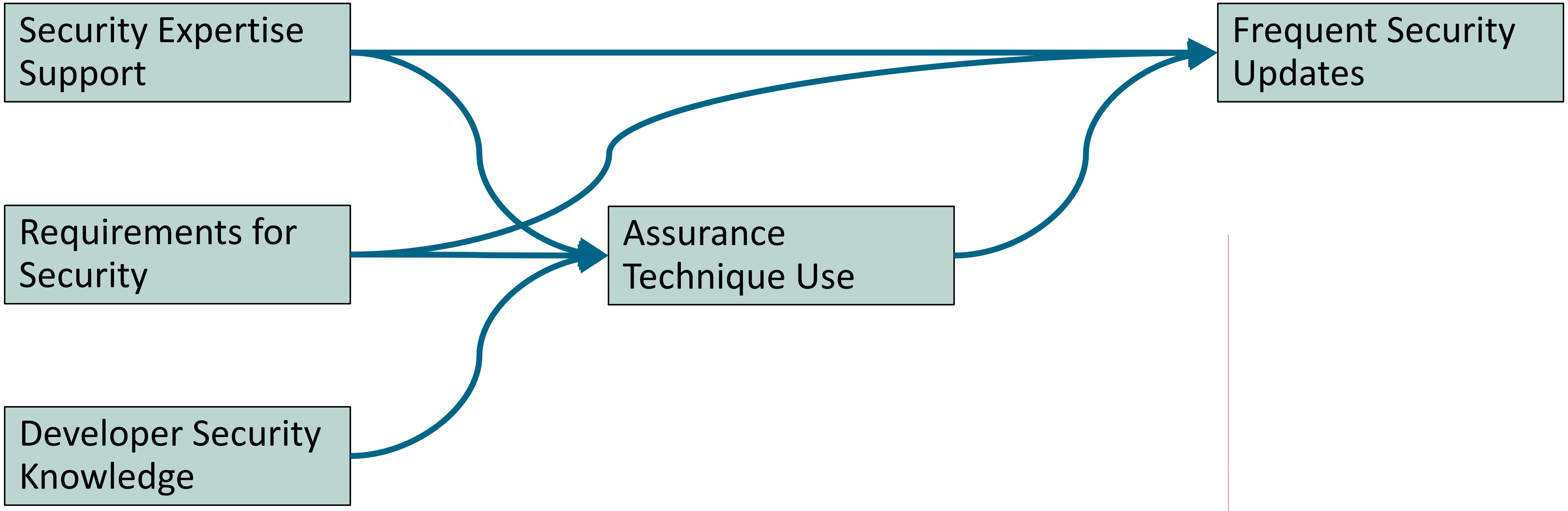
Reported App Update Frequency

Reported %age Security Updates

Log (updateFreq * proportionSecurity)

Security Update Frequency Score

Correlations Found



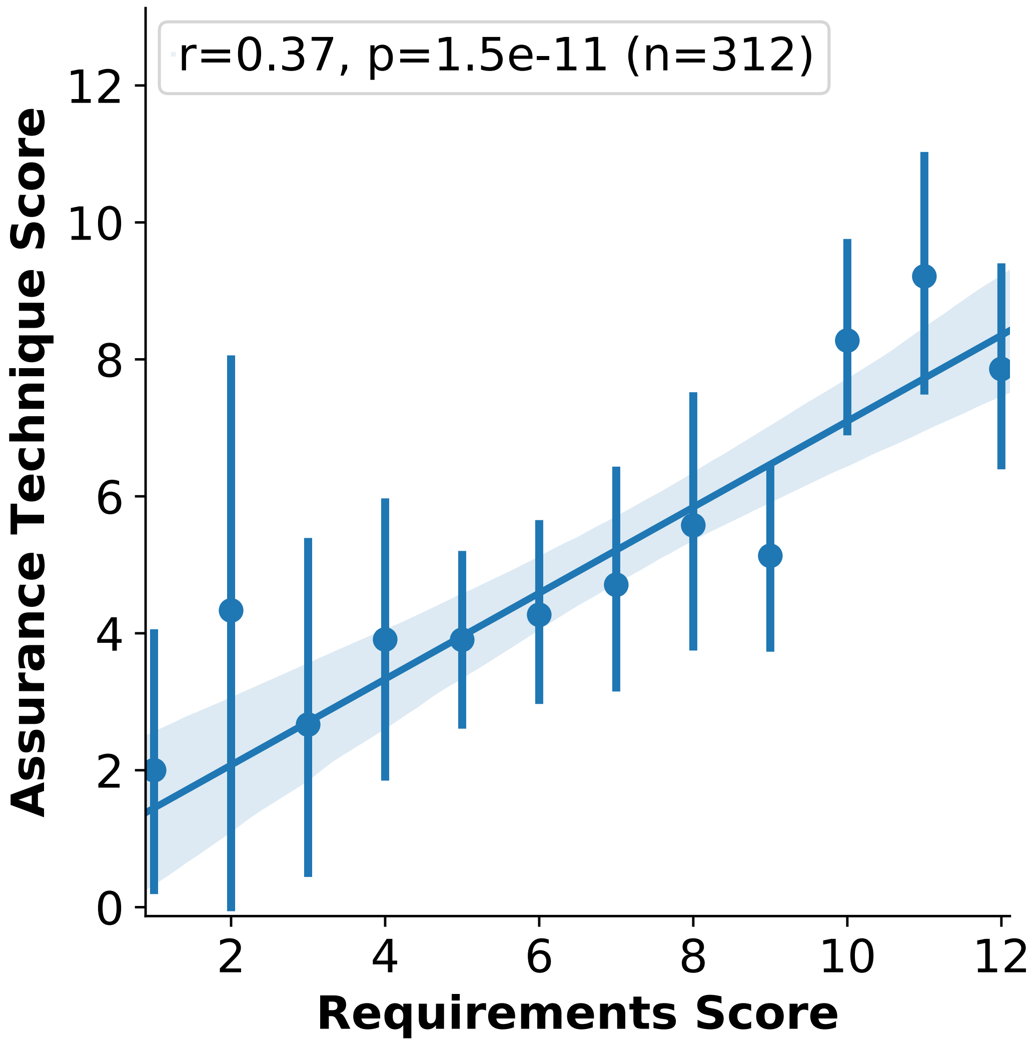
Security Expertise Support

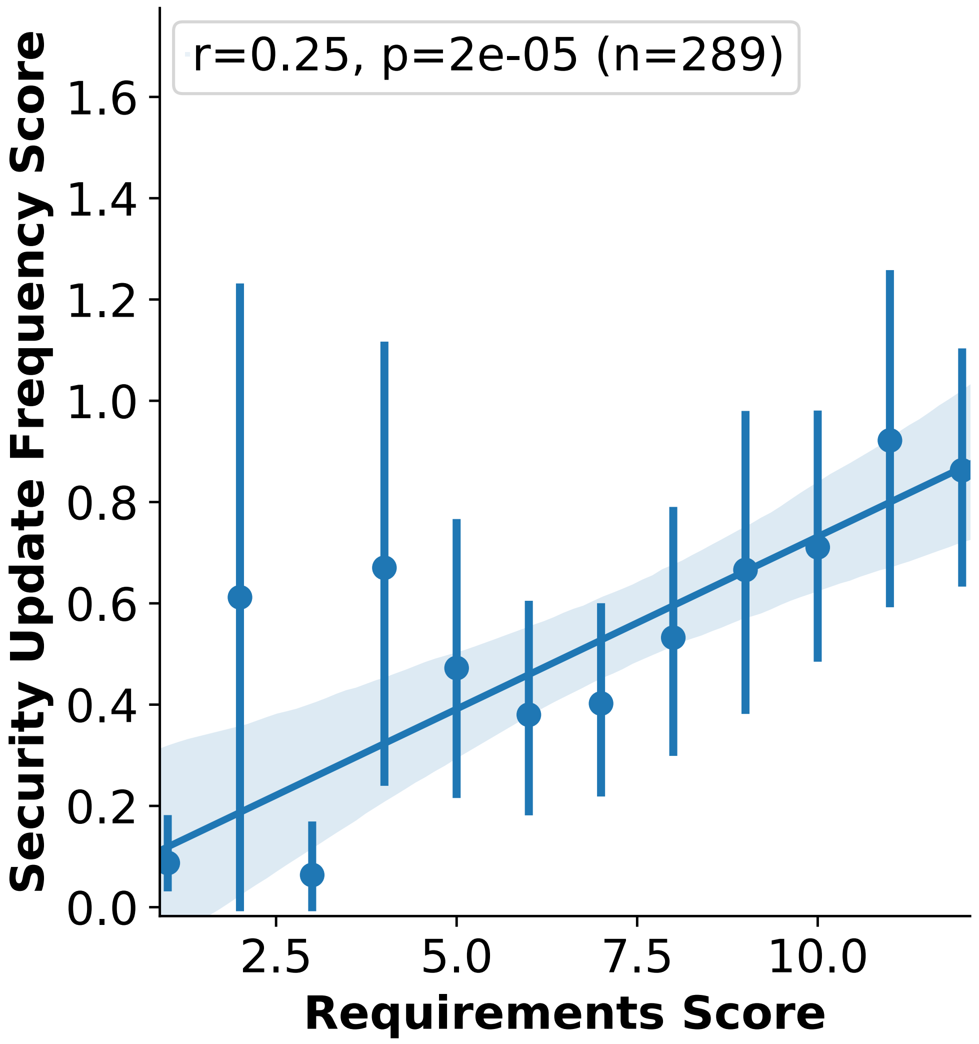
Requirements for Security

Developer Security Knowledge

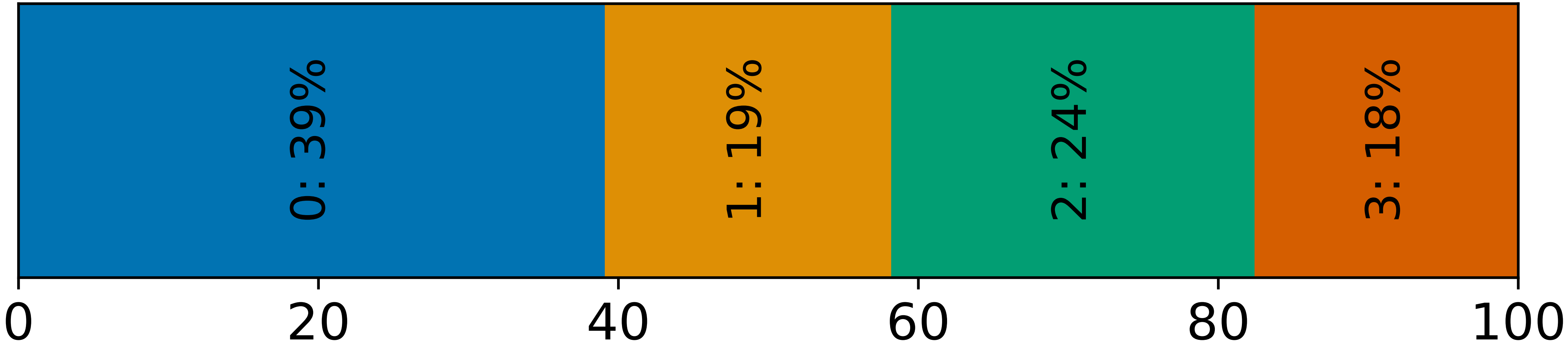
Assurance Technique Use

Frequent Security Updates


r=0.37, p=1.5e-11 (n=312)
Assurance Technique Score
0
2
4
6
8
10
12
2
4
6
8
10
12
Requirements Score


r=0.25, p=2e-05 (n=289)
Security Update Frequency Score
0.0
0.2
0.4
0.6
0.8
1.0
1.2
1.4
1.6
2.5
5.0
7.5
10.0
Requirements Score

Adding the App Analysis Data

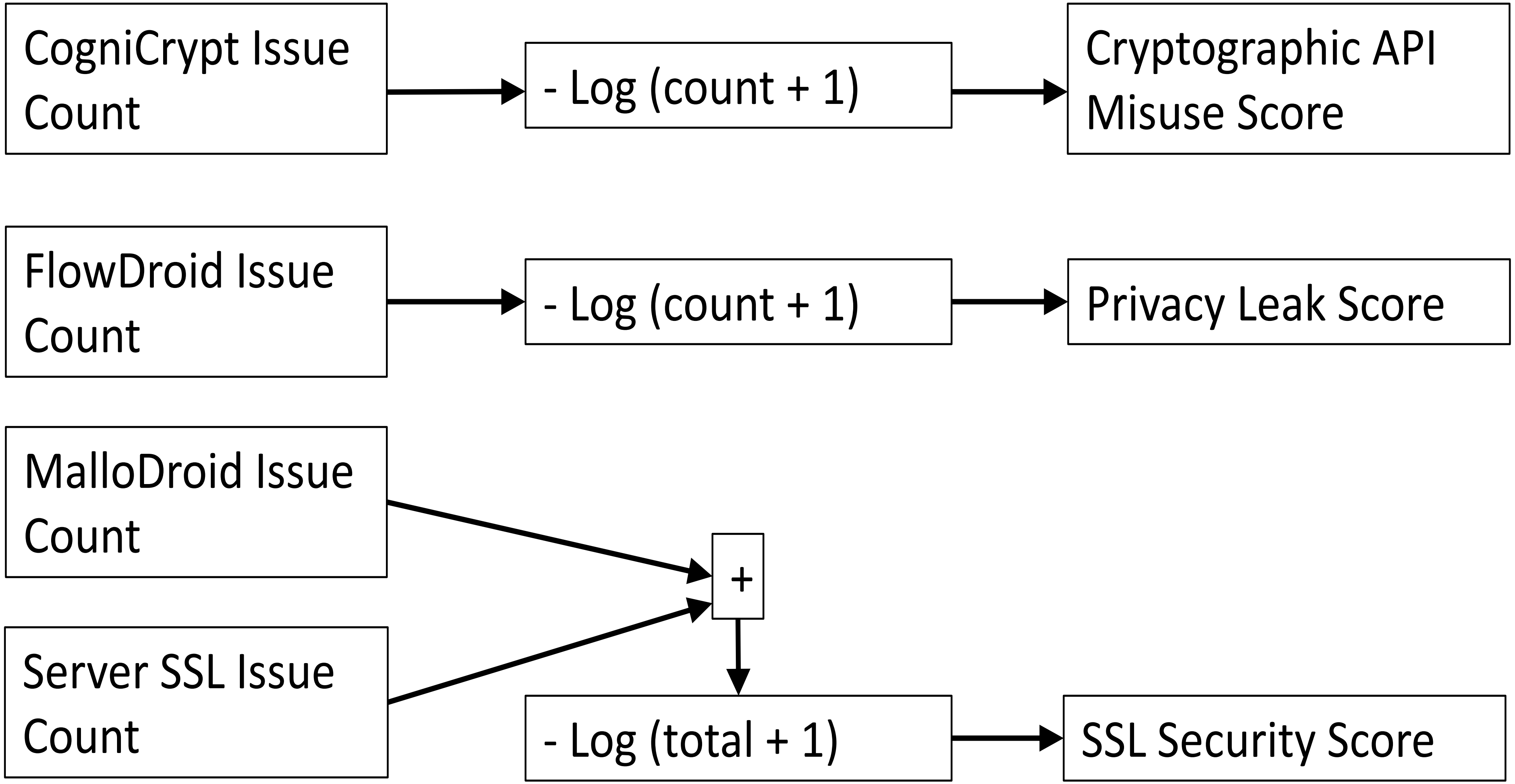


Binary Analysis ‘Failures’

FlowDroid

CogniCrypt

MalloDroid, plus OPAL framework, curl & openSSL



CogniCrypt Issue Count

- Log (count + 1)

Cryptographic API Misuse Score

FlowDroid Issue Count

- Log (count + 1)

Privacy Leak Score

MalloDroid Issue Count

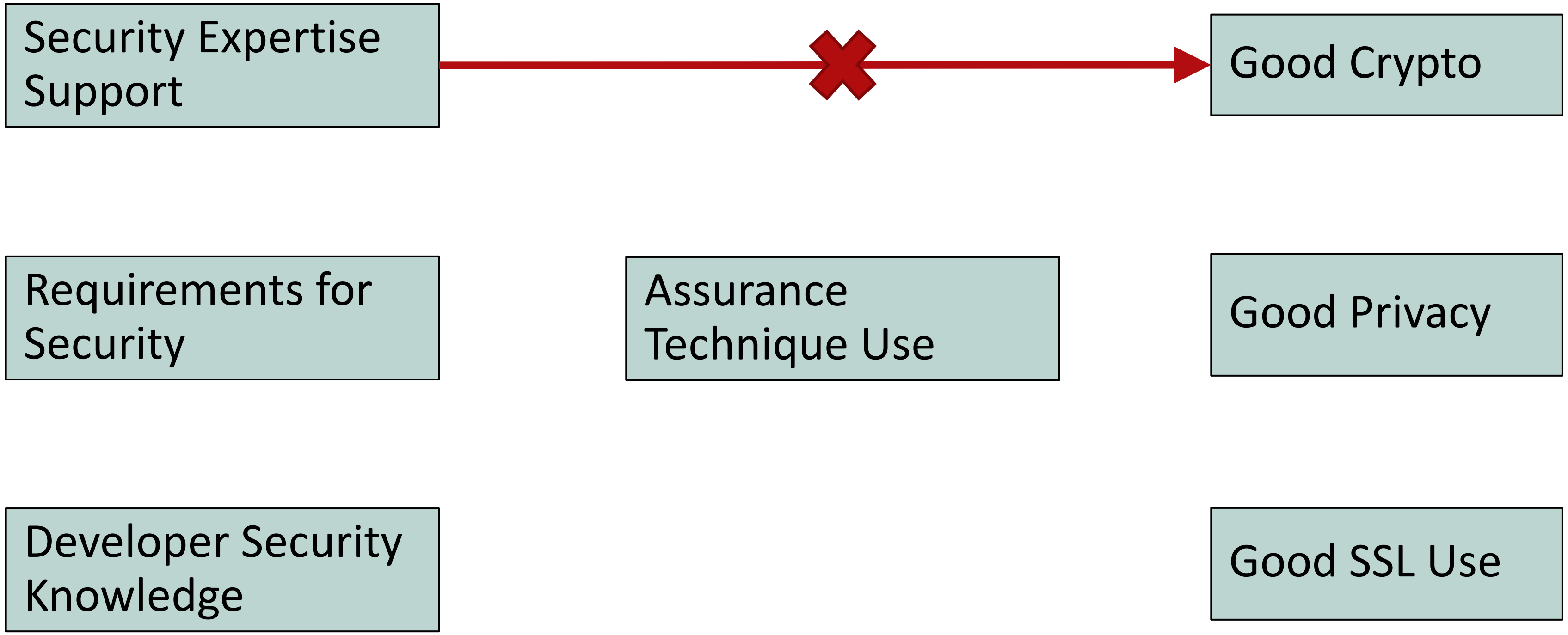
Server SSL Issue Count

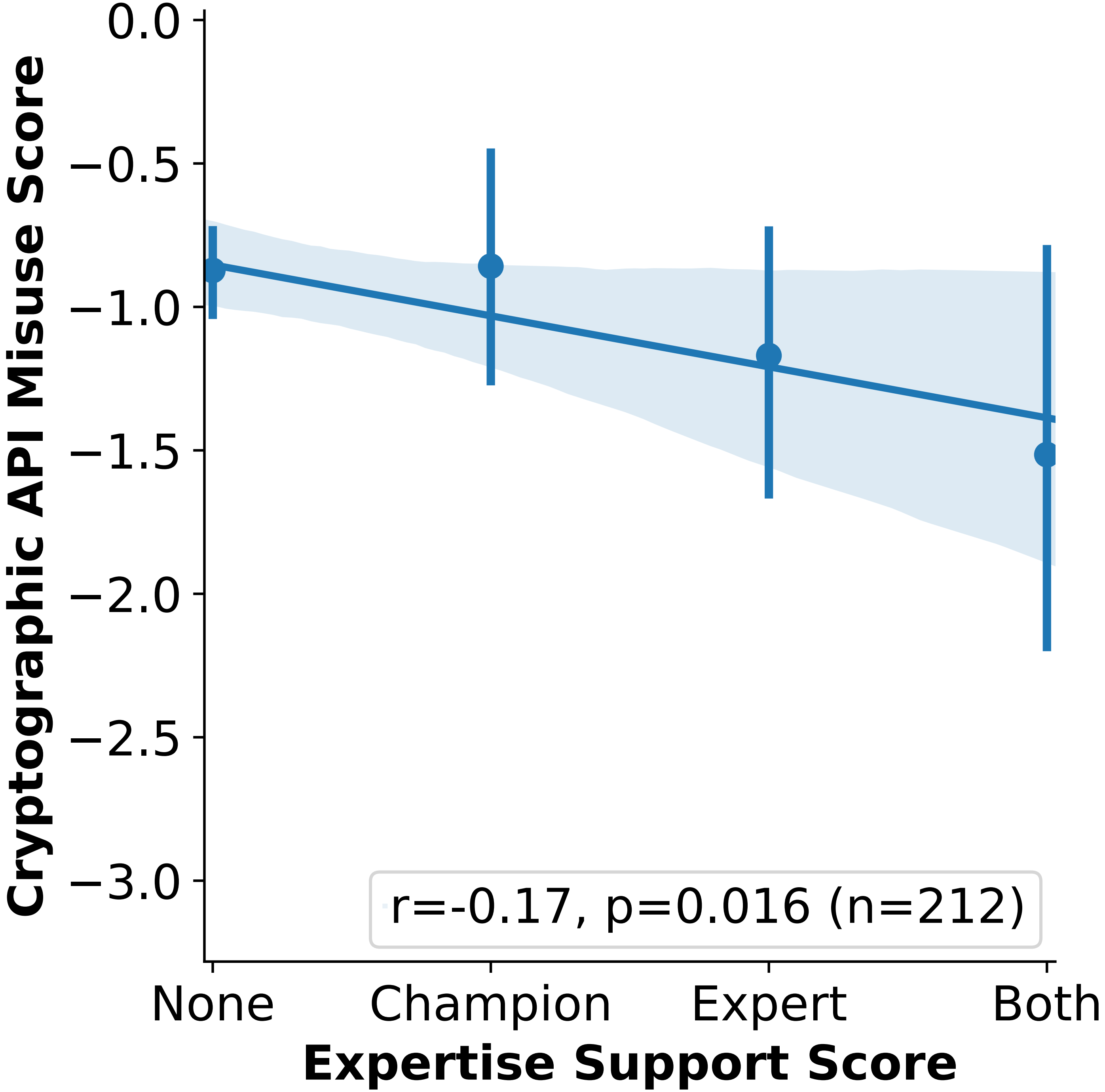
+

- Log (total + 1)

SSL Security Score

Correlations Found


Security Expertise Support
Good Crypto
Requirements for Security
Assurance Technique Use
Good Privacy
Developer Security Knowledge
Good SSL Use


Cryptographic API Misuse Score
0.0
−0.5
−1.0
−1.5
−2.0
−2.5
−3.0
r=-0.17, p=0.016 (n=212)
None
Champion
Expert
Both
Expertise Support Score

Summary: Android Developers and their Apps

- Less than a quarter of developers have access to security experts
- Less than half use assurance techniques regularly
- GDPR has had little impact
- Assurance technique use, and app security updates, both relate to security need
- Security expert involvement is linked to more crypto issues
- Binary analysis tools are not yet adequate for measurement