



# AndProtect

## Selbstdatenschutz durch statische und dynamische Analyse zur Validierung von Android-Apps

[www.andprotect.de](http://www.andprotect.de)

### Motivation

Die Mehrheit der in Deutschland genutzten Smartphones arbeiten mit dem Android-Betriebssystem. Die Anzahl der Android-Apps wächst ständig weiter. Doch Apps sind nicht nur unterstützende Helfer im Alltag, sie lesen häufig auch personenbezogene Daten aus. Hat eine App einmal Zugriff auf private Daten, sind alle weiteren Verarbeitungsschritte (etwa die Speicherung, die Zusammenführung und die Weiterleitung) für den Nutzer nicht nachvollziehbar. Welche App verwendet meine persönliche Daten? Und wie werden diese weiterverwendet? Mit Fragen wie die Nachvollziehbarkeit und Risikobewertung für den Anwender im Alltag verbessert werden kann, befasst sich das Verbundprojekt **AndProtect**.

### Projektziele

Nutzerinnen und Nutzer sollen mithilfe des AndProtect-Werkzeuges in der Lage sein, eine qualifizierte Aussage über datenschutzrelevante Informationsflüsse in Apps zu treffen. Dies wird durch orchestrierten Einsatz von gebrauchstauglich aufbereiteten Ergebnissen statischer und dynamischer Analyseverfahren erreicht. Zusätzlich wird eine halbautomatisierte Prüfmethodologie entwickelt, die nachvollziehbare und transparente App-Validierung als Dienstleistung durch Prüfstellen möglich macht.

Information, wie eine App auf private Daten zugreift, welche Daten dies betrifft und insbesondere ob und in welche Richtung die Daten das Gerät verlassen	Nachvollziehbarkeit von Datenverarbeitungsvorgängen
Fundierte Aussagen über Datenschutzrisiken, konkrete Datenflüsse und deren Auswirkungen.	Risikobewertung

### Privatsphärenbedenken

Vertrauen und Akzeptanz auf Nutzerseite sind relevante Ziele bei der Gestaltung von Technologie, um eine erfolgreiche Nutzung zu erreichen. Privatsphärenbedenken und Misstrauen können dagegen zu Ablehnung führen. Daher ist die Entwicklung eines nutzerzentriert-gestalteten Werkzeuges zum Selbstdatenschutz zentrales Ziel der **Professur Allgemeine- und Arbeitspsychologie der TU Chemnitz**. Innerhalb von AndProtect wurden hierfür zunächst Datenarten identifiziert, die im mobilen Nutzungskontext entstehen können und bewertet, wie zweckmäßig deren Erfassung für unterschiedliche App-Services sind. Diese Datenarten wurden von Nutzerseite hinsichtlich ihrer Bedenklichkeit für die Wahrung der eigenen Privatsphäre innerhalb einer 10-wöchigen Fragebogenstudie bewertet. Insgesamt nahmen 227 Personen teil. Die Ergebnisse werden auf [andprotect.de](http://andprotect.de) zur Verfügung gestellt.

### Statische Analyse

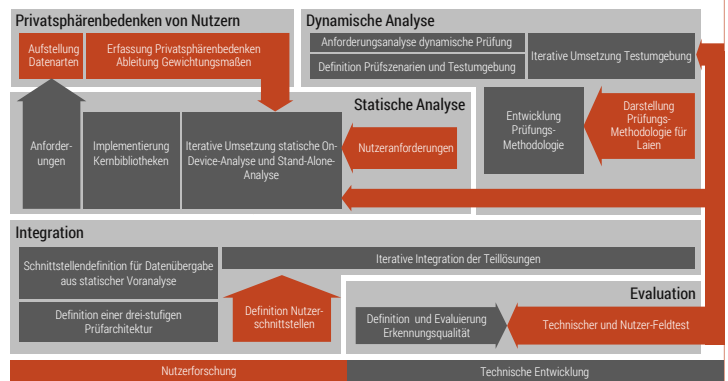
= Eine Methodologie zur Untersuchung von Software, die in Quellcode/Binärdatei vorliegen. Primäres Ziel der Analyse ist die Aufdeckung des App-Verhaltens durch die Untersuchung von Informationsflüssen. Dabei werden interprozedurale feld- und vererbungssensitive Datenflussanalysen auf handelsüblichen Android-Geräten durchgeführt. Ein mehrstufiges Analyse-Verfahren ermöglicht eine schonende Ressourcennutzung im mobilen Kontext, ohne bei der Funktionalität einbüßen zu müssen. Aufbauend auf den Erkenntnissen und Erfahrungen des **DAI-Labors** bei der Entwicklung von **Androlyzer\***, ein clientseitiges Tool zur statischen Analyse von Android-Apps, werden die Kernkomponenten weiter- bzw. neu entwickelt. Die statische Analyse kann zudem wertvolle Anhaltspunkte als Einstieg zur dynamischen Analyse liefern.



### Dynamische Analyse

Zur dynamischen Analyse wird die App zur Ausführung gebracht und dabei einer Analyse unterzogen. Hierdurch kann das tatsächliche Ablaufverhalten eines Programms bewertet werden. **secuvera** besitzt bereits Erfahrung im Aufbau technischer Prüfumgebungen für Android-Systeme. Diese Testumgebungen, die Integration verschiedener Smartphone-Modelle und die Testdurchführung wird in AndProtect weiter verfeinert. Ergebnisse anderer Forschungsprojekte (z. B. TaintDroid) werden analysiert und falls möglich wiederverwendet und integriert. Im Unterschied zum klassischen Testen von Software kann keine fest definierte Erwartungshaltung aufgestellt werden. Zentral ist die Frage nach der Vertrauenswürdigkeit und ob diese durch die App erfüllt wird. Hierzu muss eine Erwartungshaltung definiert werden, welche dynamisch beachtet werden muss.

### Interdisziplinäre Vernetzung



### Aktueller Projektstatus

- Auswertung der Fragebogenstudie
- Implementierung der Kernbibliothek für statische Analyse
- Definition Prüfbegriffe und prototypische Umsetzung der dynamischen Analyse

AndProtect: Selbstdatenschutz durch statische und dynamische Analyse zur Validierung von Android-Apps	1. Projektjahr	2. Projektjahr
<b>Privatsphärenbedenken von Nutzern im mobilen Kontext</b>		
Datenarten im mobilen Kontext		
Fragebogenstudie zur Erfassung von Privatsphärenbedenken		
Auswertung und Veröffentlichung		
<b>Statische Analyse</b>		
Implementierung der Ressourcen-Analyse-Kernbibliothek		
Statische On-Device-Analyse als App (AndProtect-Androlyzer)		
Statische Standalone-Analyse als Service		
<b>Dynamische Analyse</b>		
Anforderungsanalyse zur dynamischen Prüfung, grundlegende Prüfbegriffe, prototypische Umsetzung		
Dynamische Prüfumgebung		
Ableitung und Veröffentlichung einer Prüfungs-Methodologie für mobile Apps (Privacy und Security)		
Integration mit statischer Analyse		
Schnittstellen für verschiedene Nutzergruppen (z. B. MDM, public AP)		
<b>Evaluation und Verwertung</b>		
Definition der Bewertungsfaktoren und Evaluation der Erkennungsqualität (Methodologie, Datenbasis, Ergebnisse)		
Technischer und Nutzer-Feldtest zur Untersuchung der Alltagsstauglichkeit		
Ableitung von Geschäftsmodellen im Bereich mobiler App-Prüfung		

### Projektpartner

secuvera GmbH  
Ansprechpartner: Sebastian Fritsch, [sfritsch@secuvera.de](mailto:sfritsch@secuvera.de)

Allgemeine- und Arbeitspsychologie, TU Chemnitz  
Ansprechpartner: Susen Döbel, [susen.doebel@psychologie.tu-chemnitz.de](mailto:susen.doebel@psychologie.tu-chemnitz.de)

DAI-Labor, TU Berlin  
Ansprechpartner: Hoang Nguyen, [minh-hoang.nguyen@dai-labor.de](mailto:minh-hoang.nguyen@dai-labor.de)



ALLGEMEINE UND ARBEITSPSYCHOLOGIE  
TU CHEMNITZ



GEFÖRDERT VOM

