

Towards Secure Cellular User Equipment

Daniel Klischies

Summary

Smartphones process highly sensitive information, from private messages to military communications, which makes their security critically important. This dissertation examines smartphone security with particular attention to chipsets, the processors, firmware, and drivers that enable communication and accelerate tasks such as graphics rendering and machine learning.

To assess the status quo, we first investigate the security posture of chipsets used in commercial off-the-shelf smartphones via a longitudinal, retrospective study covering 3,676 vulnerabilities and 6,866 smartphone models. We find that chipset security is in a generally dire state, with many vulnerabilities never being mitigated via an update made available to end-users. Moreover, we find that the most vulnerability-prone chipset component is the cellular modem, also called baseband or Cellular Processor (CP).

Second, we examine whether ambiguous cellular specifications have a security impact on CPs and devise a technique, grounded on formal methods, to identify undefined behavior in cellular specifications. Using this approach, we discover five undefined behaviors across three LTE functionalities that have become exploitable vulnerabilities in CP implementations.

Last, we approach CP security from the implementation side, complementing the previous specification-focused method. In this realm, two competing approaches to assess CP implementation security exist. Over-The-Air (OTA) testing enables realistic evaluations across a diverse range of protocol features, while emulation-based testing provides introspection and scalability. Emulation, however, is limited by missing cellular state that is regularly initialized based on OTA information. To bridge the gap between both approaches, we present BaseBridge, enabling state restoration for CP firmware in emulators. This approach supports deep protocol interaction for crash analysis and facilitates vulnerability discovery via fuzzing, uncovering five previously unknown flaws, including an unauthenticated remote code execution.

This dissertation thus shines a light on the state of the art of chipset security, discovers several vulnerabilities affecting millions of devices, and provides ways to improve cellular specifications and CP implementations.

Zusammenfassung

Smartphones verarbeiten hochsensible Informationen, von privaten Chatnachrichten bis hin zu militärischer Kommunikation, weshalb ihre Sicherheit von entscheidender Bedeutung ist. Diese Dissertation untersucht die Sicherheit von Smartphones und insbesondere von deren Chipsätzen; jenen Prozessoren, Firmware und Treibern, die sowohl Kommunikationsfunktionalitäten als auch unter anderem Grafikbeschleunigung und Hardwareunterstützung für maschinelles Lernen bereitstellen.

Um den Status quo zu ermitteln, evaluieren wir zunächst das Sicherheitsprofil von Chipsätzen in 6.866 handelsüblichen Smartphone-Modellen mittels einer retrospektiven Längsschnittstudie über 3.676 Schwachstellen. Dabei stellen wir fest, dass Chipsätze vielfältige Angriffsvektoren bieten, wobei viele Schwachstellen nie durch ein für den Endbenutzer verfügbares Update behoben werden. Insbesondere auf das Mobilfunkmodem, auch als Baseband oder Communication Processor (CP) bezeichnet, entfallen dabei bemerkenswert viele Schwachstellen.

Im zweiten Schritt untersuchen wir daher, ob undefiniertes Verhalten in Mobilfunkspezifikationen zu Schwachstellen in Mobilfunkmodems führt. Hierzu entwickeln wir ein Verfahren, um undefiniertes Verhalten in Spezifikationen mittels einer formalen Methodik aufzuzeigen. Unter Anwendung dieses Verfahrens auf die LTE-Spezifikationen finden wir fünf undefinierte Verhaltensweisen in drei LTE-Funktionen, deren praktische Implementierung zu ausnutzbaren Schwachstellen in kommerziell verfügbaren Mobilfunkmodems geführt hat.

Abschließend und komplementär zum vorherigen, spezifikationsbasierten Verfahren, richten wir unseren Fokus auf die Sicherheit von Mobilfunkmodems auf Implementierungsebene. Es existieren zwei diametrale Verfahren, um Schwachstellen in Mobilfunkmodems zu finden und zu triagieren. Während die Nutzung von physischer Hardware über die Luftschnittstelle realistische Evaluationen über vielfältige Protokollfunktionalitäten erlaubt, ermöglicht Emulation tiefergehende Beobachtungen des Verhaltens der Modemfirmware und erhöht die Skalierbarkeit. Limitiert wird Emulation jedoch durch unbekannte und uninitialisierte Zustandsvariablen, die bei der Nutzung physischer Hardware über die Luftschnittstelle initialisiert würden. Um diesen Nachteil von Emulation zu beseitigen und so die Lücke zwischen beiden Ansätzen zu füllen, präsentieren wir BaseBridge, ein Verfahren, um Zustandsvariablen aus physischen Modems in Emulatoren zu übertragen. BaseBridge ermöglicht damit sowohl umfangreiche Protokollinteraktionen mit emulierten Modems, als auch das Auffinden von Schwachstellen mittels Fuzzing. Unter den fünf weiteren so gefundenen Schwachstellen befindet sich insbesondere auch eine Möglichkeit für Angreifer, das Modem mittels Remote Code Execution und ohne Authentifizierung vollständig zu übernehmen.

Diese Dissertation gibt damit einen Überblick über den aktuellen Zustand der Chipsetsicherheit, offenbart mehrere Schwachstellen, die Millionen von Geräten betreffen, und zeigt auf, wie sowohl die Spezifikationen als auch Implementierungen diesbezüglich verbessert werden können.