Analysis of UI Redressing Attacks and Countermeasures

Kurzfassung von
Marcus Niemietz

UI-Redressing (UIR) beschreibt eine umfangreiche Menge an Angriffen, die benutzt werden können, um browserbasierte Sicherheitsmechanismen wie Sandboxing und die Same-Origin Policy zu umgehen. In der Regel möchte ein Angreifer das Opfer unter Verwendung von Social-Engineering Techniken in Kombination mit unsichtbaren Elementen und entführten Trustworthy-Events dazu bringen, Aktionen auszuführen, die außerhalb des Kontextes liegen. Die Menge der Angriffe beinhaltet dabei Techniken wie die Manipulation des Mauszeigers, das Stehlen von Touch-Gesten und das bösartige Wiederverwenden von Tastatureingaben. Im Jahr 2008 wurde Clickjacking als erster UIR-Angriff vorgestellt, der erlaubte nach einigen entführten Mausklicks innerhalb eines Flash-basierten Browserspiels einen automatischen Zugriff auf die Kamera und das Mikrofon des Opfers zu erhalten.

In dieser Arbeit werden auf UIR basierende Grundlagen, Angriffe und Gegenmaßnahmen detailliert analysiert. Darüber hinaus werden neben bekannten Angriffen mitunter neue Forschungsergebnisse aus bspw. Fallstudien über neue UIR-Angriffe erörtert.

Als ein wichtiger Beitrag zu den Grundlagen von UIR wird die erste umfangreiche Untersuchung über die Ziele von UIR-Angriffen vorgestellt. Diese Ziele werden in dieser Arbeit *Trustworthy-Events* genannt, so dass diese von dem Websicherheitskonzept der Trusted-Events abgegrenzt werden können. Aufgrund dieser Untersuchungen konnte das Konzept von Trusted-Events überlistet und drei neue Varianten von UIR-Angriffen, mit einer minimalisierten Sichtbarkeit, eingeführt werden. Darüber hinaus wird eine empirische Studie über die DOM basierte Same-Origin Policy, als der vermutlich wichtigste Sicherheitsmechanismus von Webapplikationen, beschrieben. Dessen Ziel Inhalte von verschiedenen Herkünften zu separieren kann mit der Hilfe von Trustworthy-Events umgangen werden. Aus diesem Grund wurde eine umfangreiche Untersuchung über dieses Ziel von UIR-Angriffen durchgeführt.

Im Hinblick auf die Beiträge zu UIR-Angriffen werden in dieser Arbeit neuartige Drag-and-Drop Angriffsvarianten, Maskierungen mit der Hilfe von SVGs, Tabnabbing und das Umadressieren von benannten Fenstern, skriptlose Angriffe zum Stehlen von Tastatureingaben, sowie unter anderem browserlose Angriffe auf Android-Systeme die auf Tapjacking basieren, beschrieben. Als Beiträge zu UIR-Gegenmaßnahmen werden Präventionsmaßnahmen gegen die Manipulation von Browserfenstern, JSAgents als praktische Alternative zur Content Security Policy und browserlose Abwehrmechanismen gegen Tapjacking präsentiert.