Sicherheit von E-Banking auf Smart-Platforms

Fachgebiet: IT-Security
Betreuer: Prof. Reto Koenig
Experte: Walter Stucki (PostFinance)

Electronic Banking ist keinesfalls ein junges Produkt. Bereits in den 80er Jahren kamen erste, elektronische Zahlungsmöglichkeiten auf. Heute nimmt, das uns bekannte E-Banking, einen immer höheren Stellenwert im alltäglichen, digitalen Leben ein. Kein Wunder: Das digitale Bankgeschäft ist in der Regel benutzerfreundlich, praktisch, nahezu immer sowie von fast überall verfügbar und gilt grundsätzlich als sehr sicher. Diese Arbeit zeigt jedoch ein differenzierteres Bild dieser Technik und der dahinter steckenden, vermeintlichen Sicherheit auf.

Allgemeines

E-Banking an und für sich, kann als sicher angesehen werden, da die E-Banking Server nahezu uneinnehmbar sind. Die in der Thesis behandelte Thematik des Secure Platform Problem zeigt auf, dass sich das Problem hauptsächlich auf der Seite des Benutzers befindet: Sowohl die Gutgläubigkeit, teils auch die Unachtsamkeit der Anwender, aber auch das Sicherheitskonzept auf den Endgeräten lassen zu wünschen übrig.

Einführung

Kaum ein Markt wächst derzeit so rasant wie derjenige der Smart-Devices: Egal ob Tablets oder Smartphones – die mobilen Endgeräte vollziehen aktuell einen Siegeszug, der seinesgleichen sucht.

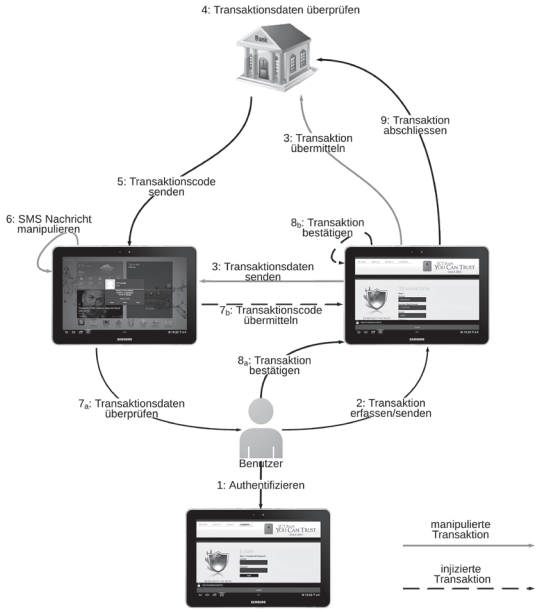
Das in dieser Arbeit ausgearbeitete Szenario zeigt einen komplett autonomen Angriff auf das E-Banking System auf der Basis von Smart-Devices. Dieser bleibt sowohl vor dem Benutzer, als auch vor der beteiligten Bank völlig verborgen. Das Szenario legt dabei den Fokus auf das häufig verwendete mTAN-Verfahren, ist aber grundsätzlich nicht auf dieses begrenzt.

Der Proof-of-Concept zeigt das Angriffspotential in seiner ganzen Tragweite auf. Das Szenario hinterfragt dabei die Sicherheit der für die Verifikation der Transaktionen eingesetzten Techniken, welche in zahlreichen aktuellen E-Banking Lösungen zum Einsatz kommen.

Angriff

Das Szenario basiert auf der Tatsache, dass das Erfassen einer Transaktion und die jeweilige Bestätigung mittels Transaktionscode (mTAN) nicht mehr über einen alternativen, dedizierten Kanal erfolgt, da die Kanäle durch den Einsatz eines Smart-Device nun zusammenfallen.

Konkret lassen sich Transaktionen manipulieren und vor dem E-Banking Benutzer verschleiern. Nebst den, vom Benutzer explizit ausgelösten und bestätigten Transaktionen, können beliebige Überweisungen autonom injiziert und zu Gunsten des Angreifers verarbeitet werden.



Ablauf im Überblick

Der betroffene Benutzer wird den Angriff erst beim Verwenden eines alternativen, nicht kompromittierten Geräts oder mit dem nächsten, per Post zugestellten Bankauszug bemerken.

Fazit

Wie im Angriff gezeigt, ist die Sicherheit etablierter E-Banking Lösungen beim Einsatz von Smart-Devices nicht gewährleistet. Die in dieser Arbeit aufgezeigten Angriffe lassen sich grundsätzlich auf alle Formen von E-Banking anwenden, bei denen kein dediziertes, hardwarebasiertes Security-Token zum Einsatz kommt.

Die Umsetzung der konkreten Angriffe ist mit der Einführung von Smart-Devices um Grössenordnungen einfacher geworden und birgt somit ein sehr hohes, kriminelles Potential.

Danijel Brei

Simon Klaus
sklaus@sevenbit.ch