Eingrenzung des Secure Platform Problems bei Internetwahlsystemen mit Hilfe von Code Voting

Kurzfassung

Jörg Helbach
Lehrstuhl für Netz- und Datensicherheit

In den vergangenen Jahren ist das Interesse an elektronischen Wahlsystemen immer weiter angestiegen. Neben den heute bei politischen Wahlen bereits weit verbreiteten Wahlmaschinen, werden dabei auch Internetwahlsysteme immer intensiver diskutiert, obwohl teilweise noch erheblicher Diskussionsbedarf - auch über die technischen Grenzen hinaus - besteht. Die beiden größten technischen Probleme bei der Verwendung von Internetwahlsystemen sind dabei zum einen, dass die Stimmen über ein unsicheres Netzwerk übertragen werden, zum anderen, dass zur Stimmabgabe der Computer oder allgemein ein elektronisches Gerät des Wählers verwendet wird, welches nicht a priori vertrauenswürdig ist. Da heutzutage Schadsoftware weit verbreitet ist, sind kryptografische Maßnahmen, z.B. die Verschlüsselung der Stimmen vor Versendung über das Internet, wirkungslos, da entsprechend eingerichtete Schadsoftware die Stimme bereits vor der Verschlüsselung auslesen und verändern kann. Zusätzlich können sämtliche Ausgaben der Wahlsoftware durch diese Software manipuliert und der Wähler somit in seiner Wahlentscheidung beeinflusst oder beeinträchtigt werden, indem beispielsweise die Reihenfolge der Kandidaten auf der Webseite in einer anderen Reihenfolge dargestellt wird, als sie an den Wahlserver übermittelt wird. Für diese Problematik wurde 2002 von Ronald Rivest der Begriff Secure Platform Problem geprägt [Riv02]. In 2002 wurden bereits einige Maßnahmen zur Bekämpfung des Secure Platform Problems beschrieben [Opp02], jedoch zeigt sich, dass die einzige für Wahlen in einem großen Umfang sinnvolle Möglichkeit, die Verwendung eines Code Voting Verfahrens ist, für das David Chaum bereits in 2001 die Grundlagen entwickelte. Dieses Verfahren basiert auf einer Trennung der Kommunikationskanäle, indem die Wähler in einer ersten Phase ein Code Sheet erhalten, auf dem für jede Wahloption ein Code aufgedruckt ist. Statt einer Wahloption im Klartext übermittelt der Wähler nur diesen Code an den Wahlserver. Dadurch kann Schadsoftware, die ggf. auf dem Wahlclient installiert ist, zwar diesen Code unter Umständen auslesen, die Anonymität der Wahl aber nicht brechen.

In dieser Arbeit werden, nach der Erarbeitung einiger Grundlagen, zunächst einige Schwächen des Code Voting Verfahrens, wie es von Chaum entwickelt wurde, aufgezeigt. Anschließend werden diese Lücken geschlossen, indem das Verfahren in mehreren Schritten erweitert wird. Dazu wird eine weitere Code Nummer eingeführt, die zur Finalisierung einer Wahloption verwendet wird. Desweiteren wird die Problematik des Stimmenkaufs bzw. der Erpressung eines Wählers in Bezug auf Code Voting betrachtet. Da das Verfahren anfällig gegen diese Attacke ist, indem der Wähler lediglich das erhaltene Code Sheet weitergeben muss, wird Code Voting in einem nächsten Entwicklungsschritt mit Gruppensignaturen verknüpft.

Abschließend wird das neu entwickelte Verfahren analysiert, die noch bestehenden Mängel des Ansatzes gezeigt sowie zwei Anwendungsbeispiele präsentiert.