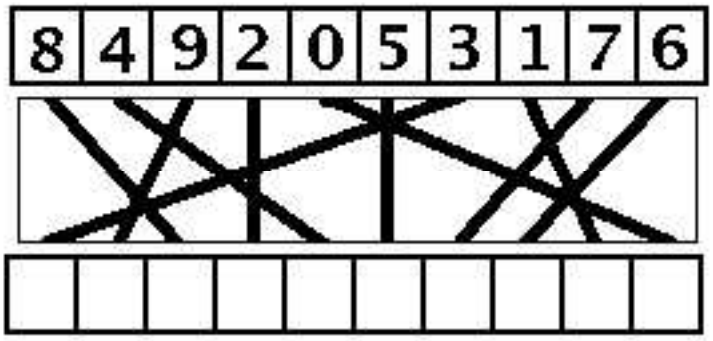
Eberhard Karls Universität Tübingen
Wilhelm-Schickard-Institut für Informatik (WSI)
Arbeitsbereich für Theoretische Informatik/Formale Sprachen

Themenvorschlag für eine Studienarbeit 11. Oktober 2007

Kryptologische Analyse eines Verfahrens zur abhörsicheren Eingabe der PIN

Bei Online Accounts besteht das Problem, dass das Passwort bzw. die PIN durch einen sogenannten *Keylogger*, der als Virus heimlich auf den PC des Benutzers gebracht wurde, beim Eingeben abgehört werden kann. Das folgende Verfahren wurde vorgeschlagen, um dieses Problem zu lösen: Der Benutzer bekommt vom Account-Betreiber eine Karte, auf der eine 10-stellige Permutation graphisch dargestellt ist, siehe unten. Beim Einloggen werden dem Benutzer nach der Angabe seines Account-Namens zwei Leisten mit jeweils zehn Feldern angezeigt: auf der einen sind die 10 Ziffern vertauscht dargestellt, auf der anderen sind die Felder leer. Der Benutzer legt seine Karte auf den Bildschirm, und zwar zwischen die zwei Leisten, siehe unten. Dann kann er auf der unbeschrifteten Leiste mit der Maus seine PIN einklicken, und zwar, indem er auf die Felder klickt, die den Ziffern auf der anderen Leiste gemäß der Permutation entsprechen.



Es soll untersucht werden, wie oft der Benutzer mit der Karte seine PIN eingeben kann, ohne dass der Keylogger-Virus so viel von der PIN und von der Permutation auf der Karte weiss, dass er sich selbständig mit einer relativ hohen Erfolgs-Wahrscheinlichkeit in den Account einloggen kann (weder die PIN noch die Karte ändern sich). Nach der ersten Eingabe der PIN kann der Virus offenbar noch keine Rückschlüsse ziehen, nach der zweiten kann er schon ein paar Schlüsse ziehen, und nach sagen wir 30 PIN-Eingaben sollte er auf jeden Fall genug Informationen haben, die PIN Eingabe heimlich selber simulieren zu können. Wievielmal kann die Karte sicher benutzt werden? Es geht also um eine Wahrscheinlichkeits-Analyse, wie schnell der Keylogger-Virus die PIN und die auf der Karte dargestellte Permutation lernen kann. Die Analyse kann rein mathematisch vorgehen, oder aber auch eine Computer-Analyse sein. Ganz konkret soll z.B. die Frage beantwortet werden: wievielmal kann die Karte bei einer 5-stelligen PIN benutzt werden, ohne dass der Virus sich mit einer Erfolgs-Wahrscheinlickeit von 1/100 in den Account einloggen kann?

Die Patentschrift von 2002: http://www.wipo.int/pctdb/en/wo.jsp?WO=2002/017556

Betreuer: Dr. Bernd Borchert, Dr. Klaus Reinhardt
http://www-fs.informatik.uni-tuebingen.de/~borchert