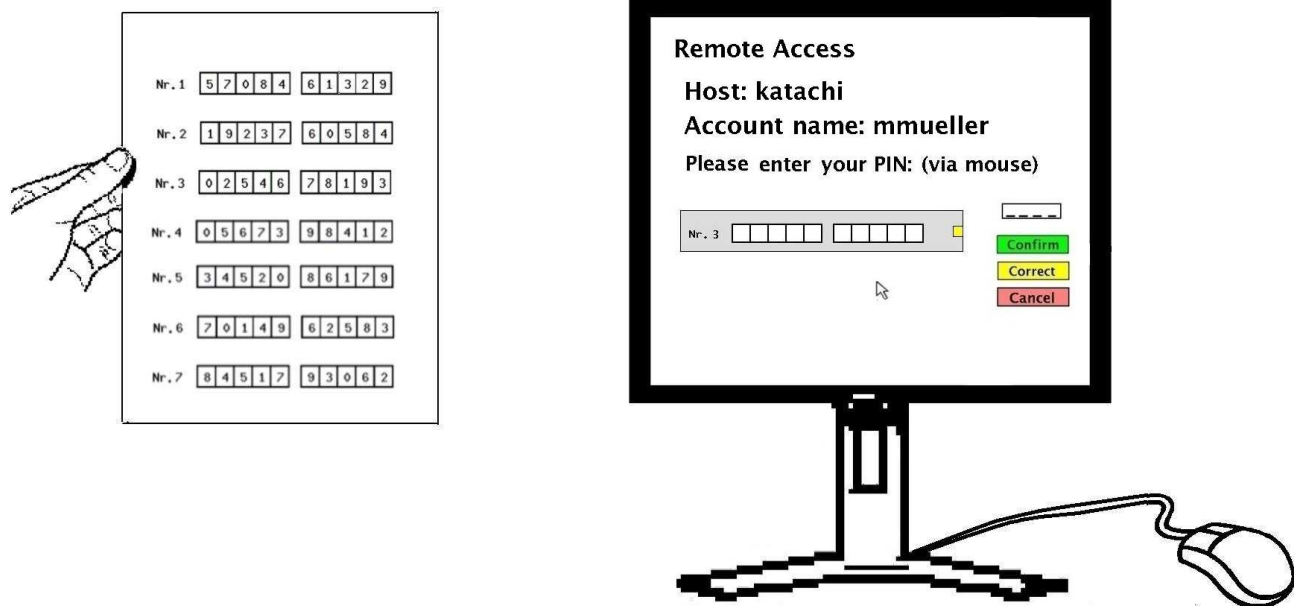




## Trojanersicherer Rechnerfernzugang (telnet, putty, ssh)

Der Fernzugang von Rechner A zu einem Rechner B in einem Rechnernetz ist unsicher: auch wenn die Fern-Verbindung verschlüsselt ist und Viren im Rechnernetz deshalb nicht abhören können, kann ein Trojaner auf dem Rechner A das Passwort beim Einloggen des Benutzers in Rechner B abhören (sog. *keylogger*).

Das Permutations-PIN Verfahren stellt einen Schutz gegen das Abhören des Passworts dar. Der Benutzer hat vom Administrator des Rechners B eine Liste von nummerierten Permutationen auf Papier bekommen. Anhand einer bestimmten Permutation wird die PIN eingegeben.



Das Verfahren garantiert, dass ein Trojaner auf dem Rechner A die PIN nicht abhören kann, denn der Trojaner sieht nur die Maus-Klicks, aber es weiss nicht, welche Ziffern damit gemeint sind. Es gibt diese online Demonstration für das Permutations-PIN Verfahren:

<http://www-fs.informatik.uni-tuebingen.de/~borchert/pPIN/>

Praktisch sähe der Einsatz dann so aus, daß ein Benutzer auf der Rechnerkonsole oder im lokalen Netz sich wie gehabt durch einfache PIN-Eingabe in seinen Account einloggen kann, aber beim Fernzugang sich nur per Permutations-PIN Verfahren anmelden kann – mit der gleichen PIN. Falls die Oberfläche für telnet in ASCII bleiben soll, kann alternativ kann statt der Eingabe via Maus-Klicks die PIN durch die Tasteneingabe – z.B. über die Reihe mit den Ziffern-Tasten – erfolgen.

Die Studienarbeit soll das Permutations-PIN Verfahren für telnet oder ssh als Demonstration auf einem der Rechner des Lehrstuhls implementieren.

Betreuer: Dr. Bernd Borchert, Dr. Klaus Reinhardt

<http://www-fs.informatik.uni-tuebingen.de/~borchert/Troja/>