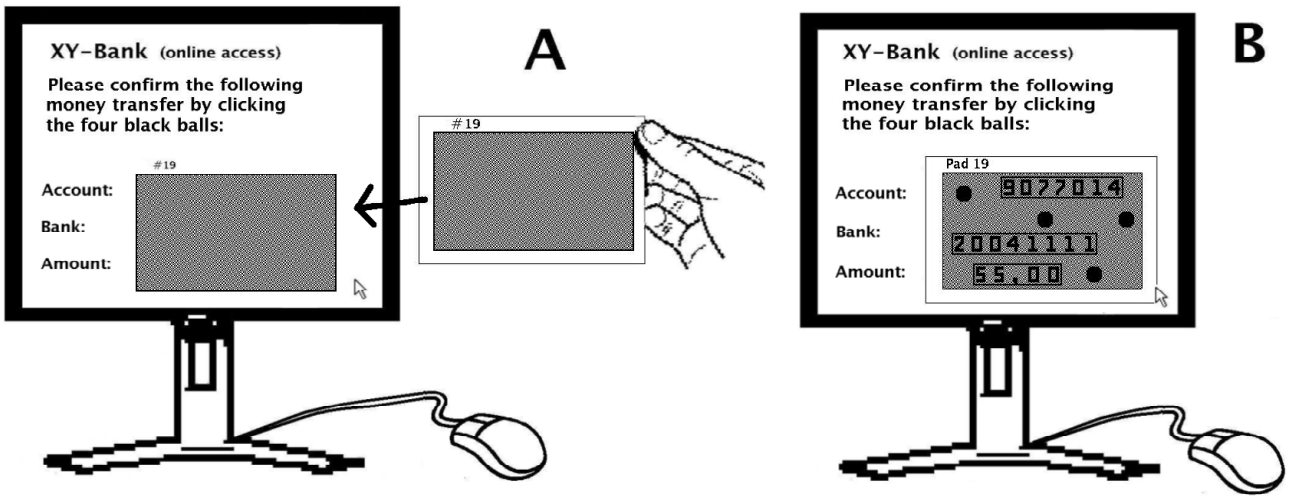
Eberhard Karls Universität Tübingen
Wilhelm-Schickard-Institut für Informatik (WSI)
Arbeitsbereich für Theoretische Informatik/Formale Sprachen

Themenvorschlag für eine Diplomarbeit 22. August 2008

Implementierung der visuellen TAN (vTAN)

Online Banking mit dem TAN- oder iTAN-Verfahren ist unsicher: ein auf den Rechner des Bankkunden als Trojaner einschleppter Virus kann durch einen sogenannten Man-in-the-Middle Angriff aus einer Überweisung von z.B. 50 Euro an X eine Überweisung von 5000 Euro an Y machen, und das, ohne dass der Bankkunde oder die Bank davon was merkt.

Als ein Schutz gegen diesen Angriff wurde die visuelle TAN (vTAN) vorgeschlagen. Sie basiert auf Visueller Kryptographie. Dem Bankkunden wird von der Bank statt iTANs ein Haftnotizblock mit nummerierten Folien zugeschickt. Bei einer Online-Überweisung füllt der Bankkunde wie gehabt ein Online-Formular mit den Überweisungsdaten aus und schickt es zur Bank. Danach wird er vom Bank-Server gebeten, eine bestimmte Folie auf das entsprechende Bild am Bildschirm legen. Das Bild am Bildschirm und die bedruckte Folie haben jeweils einzeln keine Information, aber nach dem Übereinanderlegen zeigen sie die Überweisungsdaten und die anzuklickenden Stellen. Wenn die angezeigten Daten ok sind, klickt der Bankkunde mit der Maus die Stellen an. Das wird von der Bank als Bestätigung der Überweisung angesehen, und die Überweisung wird ausgeführt.



Zuerst soll das vTAN Verschlüsselungssystem als Online Demonstration implementiert werden. Danach soll durch systematische Emperimente herausgefunden werden, bei welcher Pixel-Größe und Pixel-Form und bei welcher Überlappung der jeweiligen Pixelflächen die Daten einer Überweisung am deutlichsten lesbar sind, gleichzeitig soll die Adjustierung der zwei Bilder möglichst einfach sein. Ausserdem soll geprüft werden, ob bei einem Handy, an dessen Display Schienen angebracht worden sind, in die eine Folie geschoben werden kann, die Deutlichkeit der Darstellung der Informationen größer ist als bei einem Bildschirm. Gegebenenfalls soll der Webserver der Demonstration von einem dahinter liegenden Rechner ("Mainframe") effektiv getrennt werden, so dass dieser Rechner die Schlüssel und PINs verwaltet, verarbeitet und prüft, aber nicht an den – möglicherweise unsicheren – Webserver weitergibt.

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