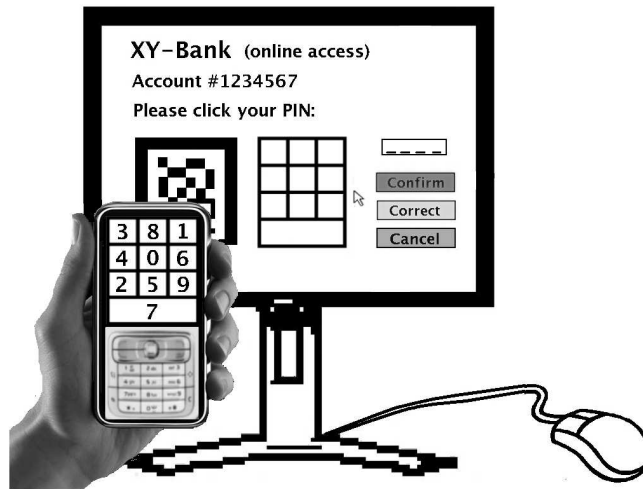


Online Schlüssel-Übergabe für das Fotohandy-PIN Verfahren

Online Accounts mit dem üblichen Passwort- bzw. PIN-Verfahren sind unsicher gegen das Ablauschen des Passworts: ein auf den Rechner des Benutzers eingeschleppter Trojaner-Virus (auch *Keylogger* genannt) kann die Tastatureingaben bzw. den Bildschirm und die Mausclicks abhören und so das Passwort ablauschen. Das Foto-PIN Verfahren mit einem Foto-Handy verhindert diesen Lauschangriff (unter der Annahme, dass das Handy virus-frei ist): Das Foto-Handy zeigt nach dem Abfotografieren eine Vertauschung der Ziffern an, gemäß der der Benutzer seine PIN durch Maus-Klicks eingibt. Ein Trojaner auf dem Rechner des Benutzers kann mit den Klick-Positionen nichts anfangen, denn er kennt die Bedeutung nicht.



Ein Prototyp für das Foto-PIN Verfahren ist schon implementiert worden:

<http://www-fs.informatik.uni-tuebingen.de/studdipl/Foto-PIN/>

Der Schlüssel kann z.B. bei einem Online Bankkonto auf das Handy übertragen werden, indem die Bank dem Kunden einen Brief mit einem aufgedruckten 2D-Code schickt, der vom Foto-PIN Programm auf dem Handy abfotografiert wird. Bei anderen Online Accounts (z.B. email, Foren, Spiele) möchte der neue Account-Besitzer nicht ein paar Tage warten, sondern sofort Zugang haben; ausserdem ist die postalische Adresse eventuell gar nicht bekannt. Deshalb sollte die Übertragung des Schlüssels online vonstatten gehen, und zwar trojaner-sicher.

Dazu stellt der Server einen öffentlichen Schlüssel zur Verfügung, den das Foto-PIN Programm mit einliest. Das Programm auf dem Handy erzeugt einen Schlüssel, wobei der dazu notwendige Zufall aus einer Foto-Aufnahme stammen könnte. Der erzeugte Schlüssel wird mit dem öffentlichen Schlüssel des Servers verschlüsselt. Die Übertragung an den Server erfolgt durch eine SMS an eine vom Server ebenfalls im 2D-Code mit angegebene Telefon-Nummer. Der Server kennt also nach der Übertragung den Schlüssel und kann – nach der Initialisierung der Wunsch-PIN des Kunden – mit dem Klienten via Foto-PIN Verfahren trojanersicher kommunizieren.

Die Studienarbeit soll dieses Online Verfahren zur Erzeugung und Weitergabe des Schlüssels implementieren, d.h. in den schon existierenden Proto-Typen einbauen: auf dem Handy in J2ME, beim Server in PHP und JavaScript.

Betreuer: Dr. Bernd Borchert, Dr. Klaus Reinhardt

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