idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Pressemitteilung

Fraunhofer-Institut für Sichere Informationstechnologie (SIT)
Oliver Küch

25.09.2007
http://idw-online.de/de/news227131

Forschungs- / Wissenstransfer, Forschungsergebnisse
Gesellschaft, Informationstechnik, Medien- und Kommunikationswissenschaften, Wirtschaft
überregional

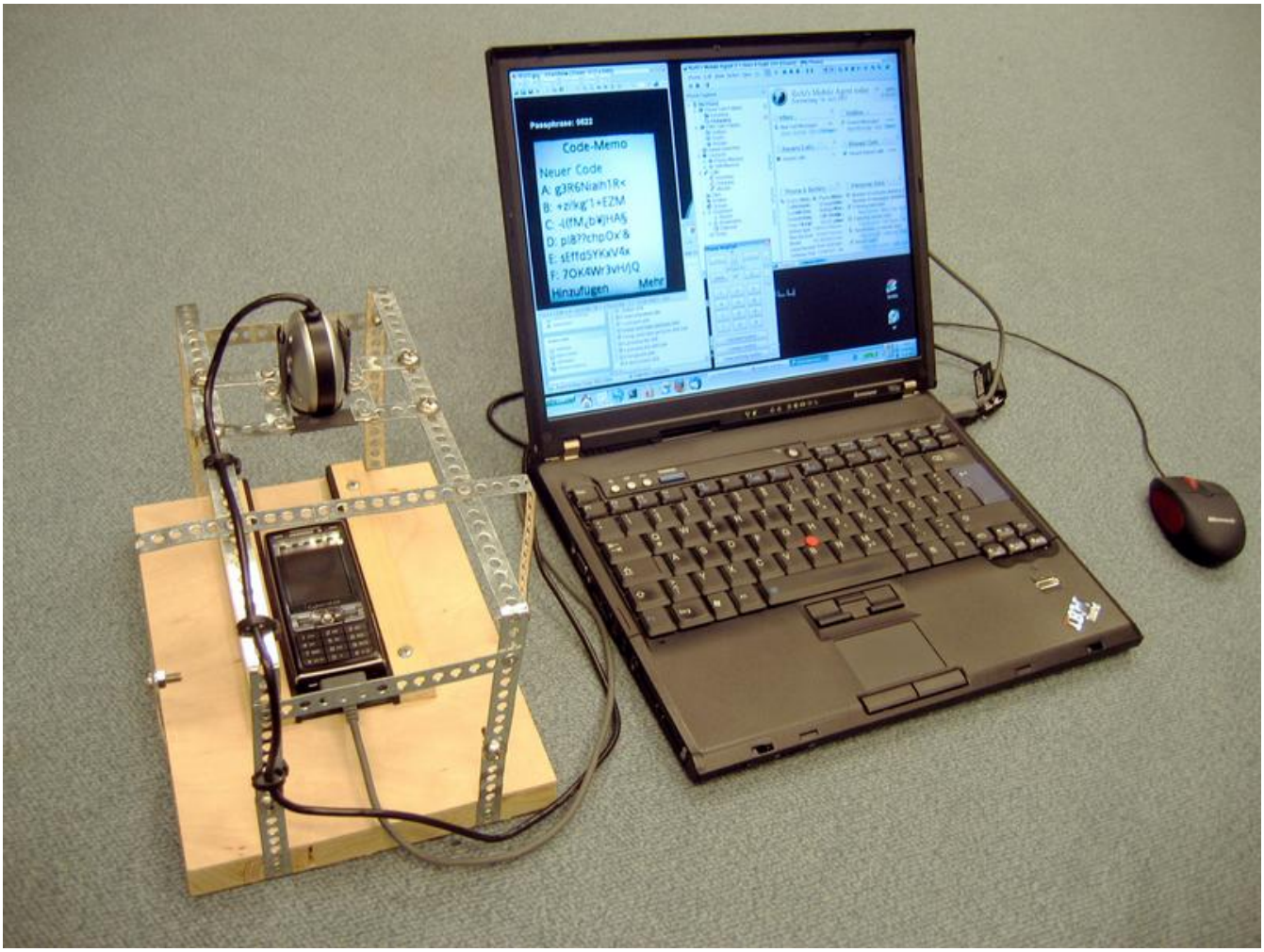
Passwort-Software von Sony-Ericsson-Handys unsicher

Fraunhofer-Institut SIT findet Sicherheitslücke im Passwort-Verwaltungsprogramm von Mobiltelefonen

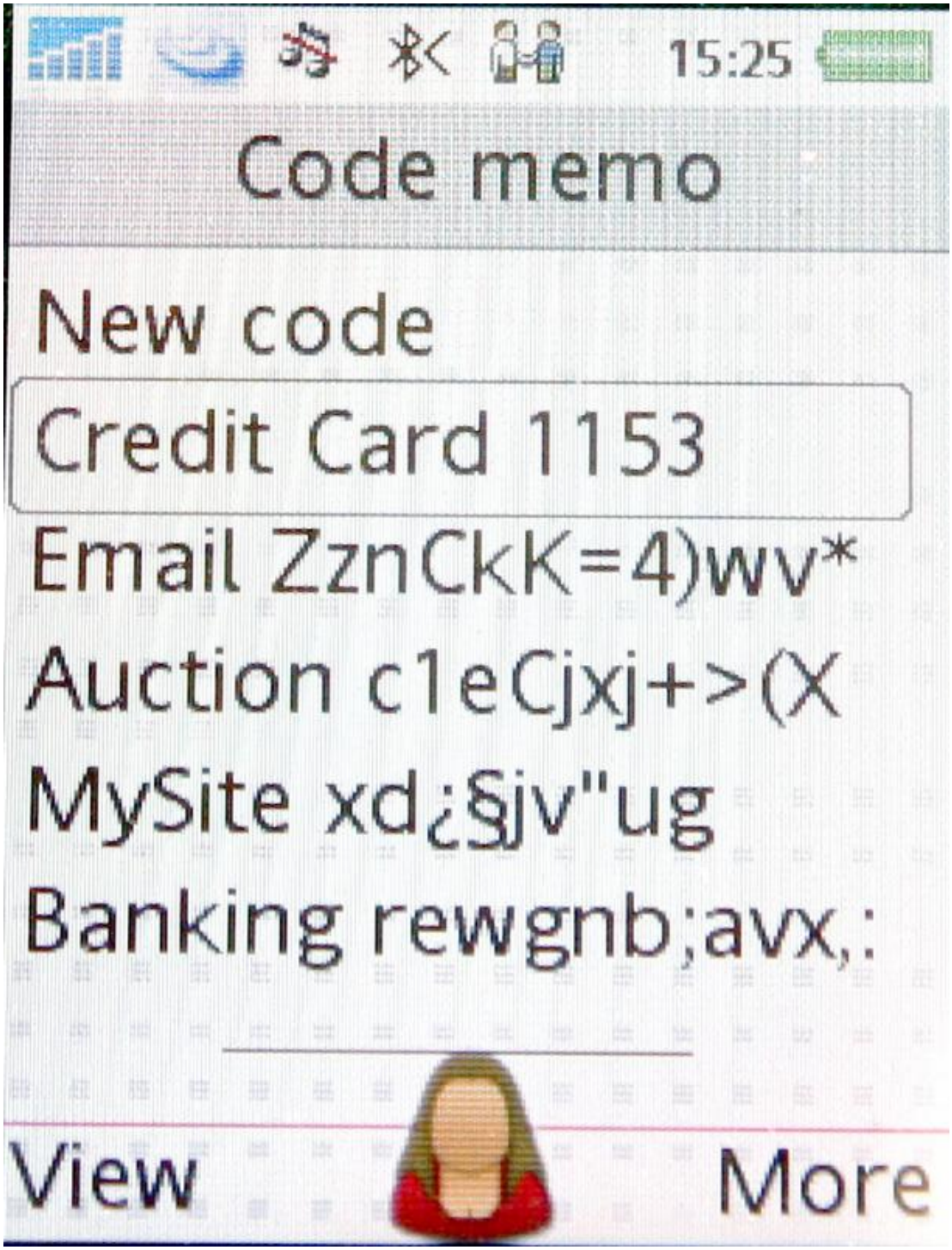
Mitarbeiter des Fraunhofer-Instituts für Sichere Informationstechnologie in Darmstadt haben eine Sicherheitslücke in der Passwort-Software Code-Memo gefunden. Die Software ist standardmäßig auf den meisten Sony-Ericsson-Handys installiert und ermöglicht es dem Nutzer, persönliche Geheimnisse wie Passwörter oder PINs verschlüsselt auf dem Mobiltelefon zu speichern. Die Wissenschaftler haben im Rahmen einer BlackBox-Analyse eine Schwachstelle gefunden, durch die Angreifer trotz Verschlüsselung mit einfachen Mitteln an alle mit Code-Memo gespeicherten Geheimnisse gelangen können. "Dazu sind keine speziellen Hackertools nötig, wir haben den Angriff mit einer handelsüblichen Webcam und kostenloser Standardsoftware durchgeführt", sagt Fraunhofer-Mitarbeiter Ruben Wolf, der die Sicherheitslücke Mitte September auf der Expertenkonferenz Mobility in Singapur vorstellte. Vorher hatte das Fraunhofer-Institut den Hersteller bereits über die Schwachstelle informiert.

Passwörter und PINs sind nach wie vor das am weitesten verbreitete Mittel, um den Zugang zu Internetdiensten, Unternehmensanwendungen und Bankkonten zu schützen. Viele Menschen haben jedoch zu viele dieser Geheimnisse, um sie sich zu merken, und nutzen deshalb spezielle Passwortprogramme wie Code-Memo. "Wie wir im Rahmen unserer Tests aber immer wieder feststellen, schützt Code-Memo die Nutzergeheimnisse deutlich cleverer als manch anderes Programm", sagt Wolf. Code-Memo zählt zu den Programmen, die versuchen, es Angreifern schwer zu machen, indem sie auch bei Eingabe eines falschen Masterpassworts keine Fehlermeldung zeigen, sondern mit Hilfe des falschen Masterpassworts falsche Geheimnisse generieren. "Bei dieser eigentlich sinnvollen Irreführung macht das Programm allerdings einen schweren Fehler", sagt Wolf, "denn es verwendet bei der vermeintlich irreführenden Entschlüsselung Sonderzeichen, die sich per Mobiltelefon gar nicht eingeben lassen - etwa das Paragraphen- oder das Prozentzeichen." Sobald das durch einen Entschlüsselungsversuch erhaltene Passwort ein Sonderzeichen aufweist, das der Nutzer gar nicht eingegeben haben kann, weiß der Angreifer deshalb sofort, dass das eingegebene Masterpasswort falsch sein muss. Um an die Geheimnisse zu gelangen, muss er also nur alle möglichen Masterpassworte eingeben und kontrollieren, ob verbotene Sonderzeichen in den Passwörtern erscheinen - dank Computer lässt sich dieser Prozess jedoch automatisieren und das richtige Masterpasswort dank der sehr überschaubaren Masterpasswortmenge von 10 000 verschiedenen Masterpasswortkombinationen in kurzer Zeit herausfinden. Genauere Informationen zur Sicherheitslücke finden sich im Internet unter http://141.12.72.35/%7erwolf/publications/security-codememo.pdf .

URL zur Pressemitteilung: http://www.sit.fraunhofer.de
URL zur Pressemitteilung: http://141.12.72.35/%7erwolf/publications/security-codememo.pdf



Mit einfachsten Hilfsmitteln ausgetrickst.
Fraunhofer-Institut SIT



Das Paragraphenzeichen verrät, dies ist ein falsches Masterpasswort.
Fraunhofer-Institut SIT