



Sicherheit der UdS-Card mit Mifare classic

Durch Veröffentlichungen in der einschlägigen Fachpresse ist bekannt geworden, dass der Verschlüsselungsalgorithmus, der auf den Mifare-Karten implementiert ist, durch ein Forscherteam der Universität Virginia gebrochen wurde und daher nicht mehr als vollständig sicher gelten kann.

Die Universität des Saarlandes setzt die UdS-Card, die auf dem Mifare-Standard beruht, als Studierendenausweis, Bibliotheksausweis, zur Bezahlung des Mensaessens und von Druckaufträgen sowie zur Zutritts-/Zufahrtskontrolle ein.

Nach bekannt werden der Sicherheitsdefizite der Mifare-Technologie hat sich die Universität des Saarlandes unverzüglich mit den Anbietern der eingesetzten Anwendungen und den Herstellern des Kartenmanagementsystems in Verbindung gesetzt. Die beteiligten Fachreferate und Institutionen haben die möglichen Gefährdungen, die aus der Unsicherheit des Mifare-Standards herrühren könnten, identifiziert, bewertet und die erforderlichen Schutzmaßnahmen in die Wege geleitet.

Nach Beurteilung der Risiken, geht die Universität des Saarlandes davon aus, dass die Gefährdungen für die Nutzer der UdS-Card beherrschbar sind. Die auf den Karten gespeicherten Daten sind wenig sensibel. Alle Studierendenverwaltungsfunktionen an den öffentlich zugänglichen Bedienstationen erfordern neben der UdS-Card die Eingabe der persönlichen PIN für die korrekte Authentifizierung.

Durch die regelmäßige Kontrolle und Überwachung der durch mit der UdS-Card verbundenen Verfahren, ist sichergestellt, dass missbräuchliche Nutzungen zeitnah erkannt und entsprechende Gegenmaßnahmen eingeleitet werden können. Die Universität des Saarlands schätzt die Sicherheit derzeit als angemessen in Hinblick auf die zu schützenden Daten und Verfahren ein. Eine Manipulation von Karten wurde bisher weder an der UdS noch bei anderen Nutzern der MIFARE-Technologie (nach Auskunft der Hersteller) beobachtet.

Die Universität des Saarlandes ist bestrebt, die Sicherheit auf hohem Niveau zu halten und wird sobald durch die Hersteller neue Sicherheitsmethoden angeboten werden, diese auf die Möglichkeit der Übernahme in das bestehende System hin überprüfen.

Saarbrücken, den 09.05.08
622 – Le

Ralf Lehmann