



ZIM-Erfolgsbeispiel

Manipulationen an Bankterminals sicher erkannt

Mit unklonbaren radiometrischen Fingerabdrücken, die durch elektromagnetische Funksignale und Messung ihrer Ausbreitung generiert werden, wird die physische Integrität sicherheitskritischer Gehäuse verifiziert. Auch kleinste mechanische Manipulationen an Bank- und Fahrkartenautomaten, Schließsystemen und anderen sicherheitsrelevanten Geräten können dadurch zuverlässig detektiert werden.

Um an das Geld von Bankkunden zu kommen, manipulieren Betrüger Geldautomaten auf vielfältige Weise. So werden z. B. mittels verdeckt angebrachter Lesegeräte und Kameras die Daten von Zahlungskarten ausgelesen und zusammen mit der PIN aufgezeichnet („Skimming“). Eine andere Betrugsmethode beruht darauf, dass durch Anbringen von Klebefolie am Ausgabeschacht das abgehobene Geld hängen bleibt und der Betrüger in den Besitz des abgehobenen Bargeldes gelangt, während der Bankkunde von einem technischen Defekt des Automaten ausgeht („Cash Trapping“). Allen diesen Methoden ist gemeinsam, dass sie mechanische Manipulationen am oder im Gehäuse der Geräte voraussetzen.

Bisher eingesetzte sensor- oder kameragestützte Sicherheitstechnologien, mit denen Geldautomaten und andere sicherheitsrelevante Geräten vor Manipulationen geschützt werden sollen, sind sehr kostenaufwändig und unzureichend zuverlässig.

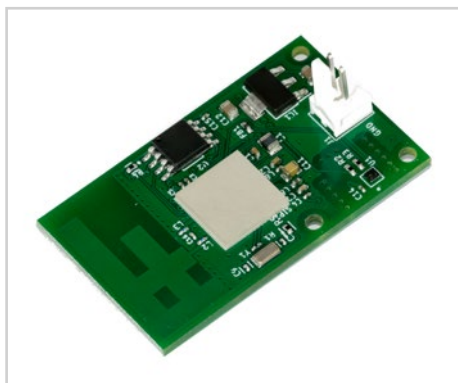
Das Produkt und seine Innovation

In einer FuE-Kooperation mit dem Lehrstuhl Digitale Kommunikationssysteme der Ruhr-Universität Bochum (RUB) verfolgte die PHYSEC GmbH einen völlig neuartigen Ansatz, um auch kleinste mechanische Manipulationen an sicherheitsrelevanten Geräten zu erkennen: Mit Hilfe von elektromagnetischen Funksignalen und der Messung ihrer Ausbreitung im

Gehäuse werden radiometrische Fingerabdrücke generiert und zur Verifizierung der physischen Integrität der Gehäuse herangezogen.

Hierzu wurden an der RUB Modelle für die Mehrwegeausbreitung der Funksignale speziell in Gerätegehäusen unter Einbeziehung auch von beweglichen Teilen und der unmittelbaren Gehäuseumgebung entwickelt und Simulationen sowie Messungen für reale Testumgebungen analysiert. Der PHYSEC GmbH oblag der Aufbau der Testumgebungen und die experimentelle Validierung.

Ergebnis der Entwicklung sind in das Gehäuse integrierbare Anti-Tamper-Radio-(ATR-)Module,



Das eingesetzte Anti Tamper Radio (ATR) von PHYSEC ist briefmarkengroß und erlernt auch komplexe Umgebungen.

Infos zum Projekt

Laufzeit: 04/2018 bis 12/2020

Projektform: Kooperationsprojekte

Technologiefeld: IuK-Technologien

Kontakt



Dr. Christian Zenger
PHYSEC GmbH
Universitätsstr. 142, 44799 Bochum
www.physec.de



Prof. Dr.-Ing. Aydin Sezgin
Ruhr-Universität Bochum
Lehrstuhl Digitale Kommunikationssysteme
Fakultät für Elektrotechnik u. Informationstechnik
Universitätsstraße 150, 44801 Bochum
www.ruhr-uni-bochum.de



Geldautomaten sind hochkomplexe Systeme mit vielen mechanischen Komponenten.

die elektromagnetische Wellen aussenden, die im Innern des Gerätes in charakteristischer Weise reflektiert, überlagert und an vorgegebenen Positionen vermessen werden. Aus den empfangenen Signalen, die sich aus der Gehäusegeometrie mit den installierten Baugruppen und verlegten Kabeln ergeben, wird ein einzigartiger radiometrischer Fingerabdruck erzeugt, ohne den ein Zugriff auf sensible Gerätedaten nicht möglich ist. Schon aller kleinste Veränderungen im und am Gehäuse ändern die empfangenen Signale, sodass der radiometrische Fingerabdruck zerstört wird. Sobald sich jemand am Gehäuse zu schaffen macht, es aufbohrt, öffnet oder daran zusätzliche Objekte anbringt, wird somit der missbräuchliche Datenzugriff verhindert.

Der Markt und die Kunden

Die entwickelte Sicherheitstechnologie ist nicht nur sehr zuverlässig, sondern aufgrund der Verwendung von Standard-Hardware und ihrer einfachen Implementierung auch kostengünstig. Neben dem erfolgreichen Einsatz in Bankautomaten soll die neue Technologie auch in anderen sicherheitsrelevanten Bereichen eingesetzt werden, wie z. B. Einrichtungen der kritischen Infrastrukturen. Das Marktpotenzial ist dementsprechend sehr groß.

Die Kooperationspartner

Das Cybersecurity-Unternehmen PHYSEC GmbH wurde 2016 als Spin-off des an der Ruhr-Universität Bochum angesiedelten Horst Görtz Instituts für IT-Sicherheit (HGI) gegründet. Es ist auf angewandte Kryptographie für das Internet der Dinge (IoT) spezialisiert.

Der Forschungsschwerpunkt des Lehrstuhls Digitale Kommunikationssysteme der Ruhr-Universität Bochum liegt in der Informationserfassung und -verarbeitung für verschiedenste Applikationen sowie in der zuverlässigen, effizienten und sicheren Kommunikation zwischen Informationssystemen.

Infos zum Programm

Das Zentrale Innovationsprogramm Mittelstand (ZIM) des Bundesministeriums für Wirtschaft und Klimaschutz fördert technologie- und branchenoffen:

- Einzelprojekte
 - Kooperationsprojekte
 - Innovationsnetzwerke
- sowie im Vorfeld Durchführbarkeitsstudien.

Infos und Beratung zu Kooperationsprojekten

AiF Projekt GmbH
Telefon 030 48163-451
www.zim.de

Impressum

Herausgeber

Bundesministerium für Wirtschaft und Klimaschutz, Öffentlichkeitsarbeit
11019 Berlin
www.bmwk.de

Stand

August 2022

Gestaltung

AiF Projekt GmbH, Berlin

Bildnachweis

Seite 1: Andrey Popov – stock.adobe.com
Seite 2: PHYSEC GmbH

