RUHR-UNIVERSITÄT BOCHUM

50 Jahre

RUB

RUBIN

WISSENSCHAFTSMAGAZIN

SONDERAUSGABE

50 JAHRE FAKULTÄT FÜR ELEKTROTECHNIK UND INFORMATIONSTECHNIK

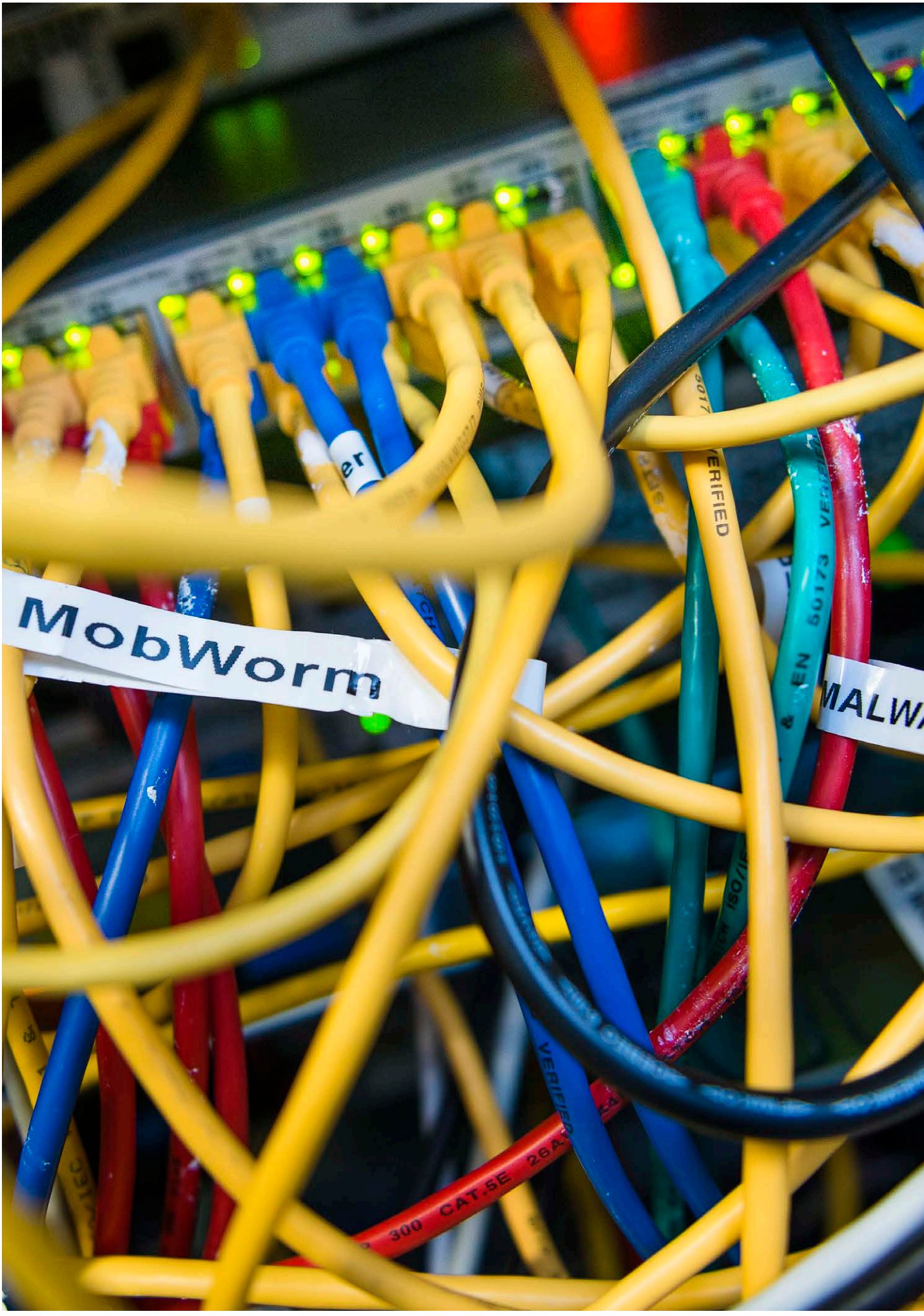
IT-SICHERHEIT

Smartphones, Browser, Ladesäulen schützen

PLASMAFORSCHUNG

Kunststoffe dichter machen und Keime töten

#25 Jahrgang
Sonderheft | 2015
4,00 Euro


MobWorm
VERIFIED
CAT.5E
300

MOBIL UND SICHER

Die meisten Smartphone-Apps erfüllen einfach nur den Zweck, für den ein Nutzer sie installiert hat. Doch in manchen Anwendungen versteckt sich Schadsoftware, die unbemerkt auf dem Telefon ihr Unwesen treibt.

Das Auto auf dem Parkplatz wiederfinden, den aktuellen Planetenstand anzeigen lassen und das iPhone in ein Kaleidoskop oder Babyfone verwandeln – Smartphone-Apps können so ziemlich alles. Manchmal können sie aber auch Dinge, die für ihre Funktion gar nicht notwendig erscheinen. Warum möchte die Taschenlampen-App auf das Adressbuch zugreifen? Wieso muss das Kaleidoskop den Standort kennen? Wozu benötigt die Fußball-App das Recht, kostenpflichtige SMS zu senden? Wenn ein Nutzer eine Anwendung auf dem Handy installiert, muss er ihr bestimmte Rechte einräumen. Nicht selten erlaubt er dem Programm dabei mehr, als es für seine eigentliche Funktion benötigt. Das ermöglicht es Angreifern, Kontaktdaten zu stehlen oder kostenpflichtige Dienste zu missbrauchen. Nicht jede App, die unnötige Rechte einfordert, hat automatisch einen kriminellen Hintergrund. Vielleicht ist sie auch einfach ungeschickt programmiert. Für den Nutzer ist das jedoch nicht zu unterscheiden.

„Wenn man eine App installiert, hat man nur die Wahl, die geforderten Berechtigungen zu akzeptieren oder nicht. Lehnt man sie ab, bekommt man die App nicht“, sagt IT-Sicherheitsforscher Prof. Dr. Thorsten Holz. „Das ist aber nicht, was man möchte. Man möchte bei jeder einzelnen Berechtigung entscheiden können, ob eine App sie bekommen soll.“ Im Projekt „MobWorm“, gefördert vom Bundesministerium für Bildung und Forschung, hat Holz mit seinem Team eine Lösung entwickelt, die dem Nutzer genau das ermöglicht. Bevor jemand eine neue App auf seinem Handy installiert, kann er wählen, welche Rechte die Anwendung bekommen soll, etwa Internetzugriff, aber keinen Einblick in Adressbuch und Standort. Das Tool der Bochumer Forscher schreibt den Code der App nach den Wünschen des Nutzers um. Will sie etwa auf das Adressbuch zugreifen, sorgt das RUB-Programm dafür, dass die Anwendung nur eine leere Kontaktliste erhält. Statt der aktuellen GPS-Koordinaten wird ein zufällig gewählter Standort ausgegeben.

Für Android-Geräte hatten andere Forschergruppen bereits entsprechende Tools zur Verfügung gestellt. Thorsten Holz' Team zeigte erstmals, wie sich das Problem für das Apple-Betriebssystem iOS lösen lässt. „Das ist deutlich anspruchsvoller“, erklärt er. Denn anders als für das Open Source-Betriebssystem Android von Google ist der Quellcode für iOS nicht öffentlich. „Wir arbeiten also nicht mit menschenlesbarem Code, sondern wesentlich maschinennäher.“ Um die Rechte von iPhone-Apps anzupassen, hantieren die RUB-Ingenieure mit Assembler-Instruktionen. Das sind kurze Befehle in der Sprache des Prozessors wie „Lade vier Byte aus dem Speicher und schreibe sie in einen bestimmten Zwischenspeicher“.

Eine schicke Nutzeroberfläche haben die IT-Sicherheitsexperten an der RUB für ihr Tool noch nicht gebastelt. Sie erstellen in der Regel Konzepte für die Lösung eines Problems, die Firmen dann anwenderfreundlich umsetzen. Im Projekt „MobWorm“ arbeitete das Team von Thorsten Holz unter anderem mit dem Hersteller „G DATA“ für Antivirensoftware zusammen. Die Firma wendet Analysetechniken der Bochumer Forscher an, um Schadprogramme in Apps aufzuspüren. Problematisch sind vor allem Anwendungen von Drittanbietern, die nicht aus den offiziellen App Stores von Google und Apple stammen. Denn die großen Konzerne checken die Programme sorgfältig, bevor sie sie zum Download anbieten.

Es gibt zwei Möglichkeiten herauszufinden, was eine unbekannte App tut: die statische und die dynamische Analyse. Mit beiden arbeiten die Bochumer. Bei der dynamischen Analyse untersuchen sie eine App, während sie diese ausführen. Bei der statischen Analyse betrachten sie den Code, ohne die App laufen zu lassen. Jede Anwendung hat einen Startpunkt, eine erste Instruktion, die sie ausführt, wenn sie aufgerufen wird. Anschließend können verschiedene andere Instruktionen folgen, die jeweils eine Vielzahl weiterer Prozesse anstoßen können.

Die Forscher stellen die Programmarchitektur in Form eines verzweigten Grafen dar. Ihre Analysealgorithmen untersuchen einzelne Blöcke und schauen, wie diese zusammenhängen. Das erlaubt Rückschlüsse auf die Funktion. Die Wissenschaftler sehen etwa, dass die App zuerst Kalendereinträge liest, diese verarbeitet und ein paar davon zum Server eines Angreifers schickt. Mit den Verfahren des Lehrstuhls für Systemsicherheit können Computer die Analyse automatisch bewerkstelligen – und so für mehr Sicherheit auf mobilen Geräten sorgen. „Wir sind auf einem guten Weg, die Dinge, die man bei der Sicherheit von Desktoprechnern nicht gut gemacht hat, auf den mobilen Geräten besser zu machen“, resümiert Thorsten Holz.

Text: jwe, Foto: dg

RUBIN IM NETZ

Zugangsdaten vor Onlinedieben schützen
rubin.rub.de/de/zugangsdaten-schuetzen

REDAKTIONSSCHLUSS

99,9 %

DES UNIVERSUMS BESTEHEN AUS PLASMA.

Die Erde ist hingegen beinahe plasmafrei – bis auf Blitze, Feuer und Polarlichter. Da Plasmen aber den energiereichsten Zustand der Materie darstellen, sorgt der Mensch dafür, dass sie ein klein wenig häufiger auf der Erde werden. In Forschung und Industrie werden Plasmen technisch hergestellt und für eine Vielzahl von Anwendungen genutzt. Wofür? Ein paar Beispiele finden sich in diesem Heft auf den Seiten 12 bis 27.

Bild: NASA, ESA, and M. Livio and the Hubble 20th Anniversary Team (STScI)

IMPRESSUM

HERAUSGEBER: Fakultät für Elektrotechnik und Informationstechnik der Ruhr-Universität Bochum in Verbindung mit dem Dezernat Hochschulkommunikation (Abteilung Wissenschaftskommunikation) der Ruhr-Universität Bochum

REDAKTIONSANSCHRIFT: Dezernat Hochschulkommunikation, Abteilung Wissenschaftskommunikation, Ruhr-Universität Bochum, 44780 Bochum, Tel.: 0234/32-25528, Fax: 0234/32-14136, rubin@rub.de, rubin.rub.de

REDAKTION: Dr. Julia Weiler (jwe, Redaktionsleitung); Meike Drießen (md); Raffaela Römer (rr)

Die Redaktion hat sich um die Einholung der nötigen Bildrechte mit allen Mitteln bemüht; wo das nicht möglich war, bitten wir eventuelle Rechteinhaber, sich mit der Redaktion in Verbindung zu setzen.

FOTOGRAFIE: Damian Gorczany (dg), Hofsteder Str. 45a, 44791 Bochum, Tel.: 0176/29706008, www.damiangorczany.de; Roberto Schirdewahn (rs), RUB Agentur

COVERFOTO: Damian Gorczany

WEBAUFTRITT: Andreas Rohden, Abteilung Markenbildung, RUB

GRAFIK, LAYOUT UND SATZ: VISUELL MARKETING GMBH, Springorumallee 2, 44795 Bochum, Tel.: 0234/459803, www.visuell-marketing.com

DRUCK: VMK Druckerei GmbH, Faberstrasse 17, 67590 Monsheim, Tel.: 06243/909-110, www.vmk-druckerei.de

AUFLAGE: 4.000

ANZEIGENVERWALTUNG UND -HERSTELLUNG: VMK GmbH & Co. KG, Faberstraße 17, 67590 Monsheim, Tel.: 06243/909-0, www.vmk-verlag.de

BEZUG: Die Sonderausgabe 2015 des Wissenschaftsmagazins RUBIN ist erhältlich in der Fakultät für Elektrotechnik und Informationstechnik der Ruhr-Universität, Gebäude ID, Etage 1, Raum 643. Das Wissenschaftsmagazin RUBIN erscheint zweimal im Jahr. ISSN 0942-6639