RUHR-UNIVERSITÄT BOCHUM

RUB

RUBIN

WISSENSCHAFTSMAGAZIN

Schwerpunkt Metropolen

WIE HACKER GANZE STÄDTE LAHMLEGEN

METROPOLE RUHR: WAS SCHILDER ÜBER DIE MENSCHEN VERRATEN

MYTHOS NEW YORK: WIE TRAUM UND WIRKLICHKEIT ENTSTEHEN

UA RUHR

27
Jahrgang

Nr. 2 | 2017

IT-Sicherheit

WIE HACKER GANZE STÄDTE LAHMLEGEN

Gemeinsam mit Kollegen der Technischen Universität Dortmund und weiteren Projektpartnern wollen Wissenschaftler der RUB Windkraftanlagen und andere kritische Infrastrukturen vor Angriffen schützen.

Auf einmal ging nichts mehr. Kein Licht, kein Fernsehen, nichts, was mit Strom betrieben werden muss. Es war das Jahr 2015, kurz vor Weihnachten. Mehrere Stunden waren damals 700.000 Haushalte in der Ukraine von der Energieversorgung abgeschnitten. Und nicht nur sie, sondern auch industrielle Einrichtungen bekamen große Probleme. Beispielsweise konnte ein Hochofen nicht geregelt heruntergefahren werden; die dadurch entstandenen Schäden waren schwerwiegend. Das Perfide an der Situation: Sie war bewusst und von Menschenhand herbeigeführt worden. Ein Hackerangriff auf die Computersysteme der Energieversorger steckte dahinter.

Stromnetze gehören, ebenso wie die Wasserversorgung oder Transportsysteme, zu den sogenannten kritischen Infrastrukturen. Sie vor Angriffen zu schützen ist das Ziel des deutsch-französischen Forschungsprojektes Bercom, das seit September 2015 läuft und vom Bundesministerium für Bildung und Forschung unterstützt wird. Der Name steht für „Blaupause für eine pan-europäische Systemplattform für widerstandsfähige kritische Infrastrukturen“. Zwölf Projektpartner, darunter Wissenschaftler der Ruhr-Universität Bochum und der Technischen Universität Dortmund, arbeiten dafür zusammen. Gemeinsam wollen sie bis August 2018 zum Beispiel ein sicheres Mobilfunknetz entwickeln, das für Betreiber von kritischen Infrastrukturen reserviert sein soll und das in die bereits bestehende Kommunikationsinfrastruktur integriert werden kann.

Zum Bochumer Team gehört David Rupprecht, Doktorand am Horst-Görtz-Institut für IT-Sicherheit. Er erklärt, warum Mobilfunk für Netzbetreiber überhaupt eine so große Rolle spielt: „In Deutschland gibt es beispielsweise aufgrund der Energiewende immer mehr Windkraftparks. Die Windräder, die die Energie erzeugen, sind über große Flächen verstreut. Damit die Mitarbeiter sie von der Schaltzentrale aus steuern können, nutzen sie zumindest auf der letzten Strecke Mobilfunk.“

Eine zuverlässige Steuerung solcher Anlagen ist wichtig, beispielsweise um eine Kontrolle über die erzeugte Energiemenge zu haben. Ist sie viel höher als die abgenommene Energiemenge, wird das Stromnetz überlastet, und es kann zu Ausfällen kommen, was wiederum auch die Kommunikationssysteme lahmlegt. Angreifer können das System stören, indem sie eine überschüssige Stromproduktion zulassen und Sicherheitsmaßnahmen des Systems außer Kraft setzen. Ein Netzausfall wie in der Ukraine wäre die Folge. Beunruhigend sei, so David Rupprecht, dass momentan viele Betreiber von ▸

kritischen Infrastrukturen veraltete und damit unsichere Kommunikationstechnologien einsetzen wie etwa Modems oder auch den veralteten Mobilfunkstandard GSM, kurz für Global System for Mobile Communications. Er ist im Privatbereich längst abgelöst worden von LTE – die Abkürzung steht für Long Term Evolution –, der übernächsten Generation von Mobilfunkstandards. Im Vergleich zu seinen Vorgängern ist er zwar gegen eine große Zahl bekannter Angriffe geschützt, doch auch LTE hat Sicherheitslücken.

Die Projektpartner von Bercom sind zuversichtlich, dass sie diese beheben können und LTE so zu einem sichereren Mobilfunkstandard für den Energiesektor machen können. Hat er sich dort etabliert, kann er für weitere kritische Infrastrukturen, auch in anderen Ländern als Deutschland und Frankreich, nützlich werden.

David Rupprecht hat in diesem Zusammenhang Tests entwickelt, mit denen er die Chipsätze, die in den Steuereinheiten von Windrädern zur Kommunikation verbaut sind, auf sicherheitsrelevante Punkte wie Verschlüsselung und Authentifizierung hin überprüfen kann. Verschlüsselung bedeutet, dass ein Angreifer Nachrichten nicht mitlesen kann und somit keine Information über das System erhält. Mit Authentifizierung ist gemeint, dass ein Angreifer sich nicht als ein echtes Mobilfunknetz ausgeben und somit keine gefälschten Befehle an die Steuereinheit senden kann. Ein entsprechender Schutz ist im LTE-Standard zwar bereits grundsätzlich enthalten, eine vollständig korrekte Umsetzung in den einzelnen Chipsätzen ist dadurch aber noch nicht garantiert. So können herstellungsbedingte Unterschiede in den Geräten einem Angreifer Zugriff gewähren, beispielsweise zum Versenden gefälschter Nachrichten.

Da solche Experimente nicht in realen kritischen Infrastrukturen durchgeführt werden sollten, hat David Rupprecht seine Tests stattdessen mithilfe von verschiedenen Mobiltelefonen gemacht, in denen die gleichen Chipsätze verbaut sind wie in den großen Anlagen. Für die Tests nutzte der Bochumer Doktorand sogenannte Software Defined Radios. Sie ermöglichen das Senden und Empfangen von LTE-Signalen. Der Vorteil von diesen Geräten ist, dass die Verarbeitung der Signale nicht, wie üblich, in der Hardware stattfindet, sondern Systeme gezielt durch Software definiert werden. Genau diese Eigenschaft erleichtert die flexible Entwicklung von Sicherheitstests. So konnte Rupprecht eine LTE-Basisstation nachbilden, mit der er auch nicht-standardkonforme Nachrichten an den getesteten Chipsatz schicken konnte. Auf diese Weise konnte er Angriffe auf den Chipsatz simulieren und Sicherheitslücken identifizieren.

Das Ergebnis der Tests: Von den zehn getesteten Mobiltelefonen warnte keines seinen Nutzer vor einem unverschlüsselten Datenaustausch. Bei der Authentifizierung fiel hingegen nur eins durch, die anderen neun erkannten gefälschte Nachrichten und ließen deren Empfang nicht zu. „In erster Linie war es jedoch mein Ziel zu zeigen, wie entsprechende Tests aussehen und wie sie entwickelt werden können“, erklärt Rupprecht, der seine Ergebnisse bereits veröffentlicht hat. So lassen sich nicht nur Sicherheitslücken aktueller Chipsätze ▸

David Rupprecht arbeitet am Bochumer Horst-Görtz-Institut für IT-Sicherheit in der Arbeitsgruppe Informationssicherheit.

Windräder stehen zwar oft abseits auf dem freien Feld. Aber unsere Städte hängen an ihnen – in Zeiten der Energiewende immer mehr.

socionext™
for better quality of experience

We are ...

Socionext is a leading provider of next generation System-on-Chip (SoC) solutions. Born from the system LSI businesses of Fujitsu and Panasonic, Socionext was launched globally in March 2015.

Socionext Europe GmbH provides SoCs with focus on optical networking applications, image processing and custom SoC solutions for a variety of high-tech applications such as in the areas of communications, automotive and industrial.

We are a dynamic high-tech enterprise, with 300 employees, which focuses on product development through the cooperation of several locations in Europe.

We are looking for ...

Field Application Engineer ISP (m/f)

Our "Milbeaut" image signal processors (ISP) are used in world leading still and video image solutions. We are currently looking for an experienced FAE to join our Socionext team in Germany (Langen or Munich). In this role, you will be the technical expert for our ISP products and you will work directly with our European customers and our development teams in Japan and Germany.

Detailed Tasks:

- Provide pre- & post-sales customer support, including product demonstrations, assistance on SW design, on-site optimization, troubleshooting and Q&A.
- Develop excellent understanding of customer's imaging products.
- Lead technical communication between customers & internal teams.
- Monitor and report on customer status.
- Provide technical inputs for future ISP products.
- May develop applications notes, articles, and technical presentations for customer trainings.

Skills:

- Qualified to at least degree level or equivalent in Electronics or related disciplines with knowledge of semiconductor industry.
- C/C++ programming on embedded systems.
- Good SW experience in Linux including kernel API.
- Knowledge of image sensors and the image signal processing (ISP) pipeline.
- Passion for imaging/photography preferred.
- Good people skills & an ability to work directly with customers.
- Ability to travel domestically and internationally.
- Ability to think strategically and act operationally without direction.
- Flexible attitude working in a leading edge environment with many unknowns.
- Good verbal and written communication skills (German and English required).

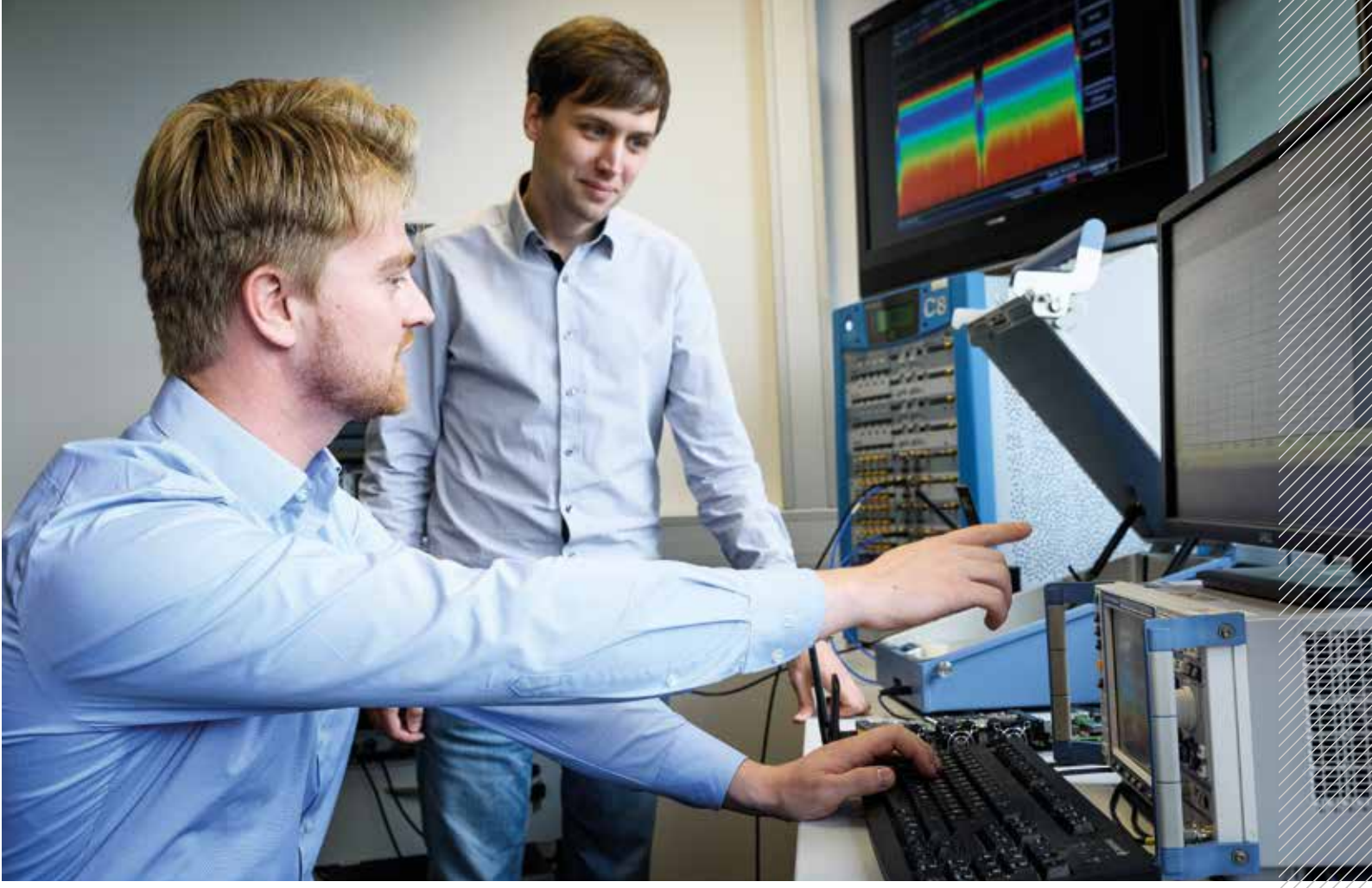
"We're working on the fastest communications systems with the latest Semiconductor processes – so if you like 'cutting edge' technology it doesn't get much better than this"

We offer ...

- Total compensation packages with attractive extended benefits
- The advantages of working at a midsize company with regards to flexibility and knowing your co-workers
- Opportunities, programmes and benefits similar to those offered by much larger corporate groups
- Freedom to develop your own creativity
- Training opportunities and structured development paths
- An employee friendly corporate culture

If you are interested in this new professional challenge, we are looking forward to receiving your application. Please send your complete application documents in English or German to hr_sneu@eu.socionext.com

socionext™



Der Dortmunder Doktorand Stefan Monhof (rechts) und David Rupprecht (links) nutzen ein Software Defined Radio, um verschiedene Mobiltelefone und ihre Chipsätze auf Schwachstellen zu testen.

Das Spektrum eines Signals gibt Aufschluss über die Frequenzen, die ein Mobiletelefon zur Kommunikation mit der Basisstation verwendet. Die Forscher ermitteln es mit einem sogenannten Spectrum-Analyzer.

identifizieren, sondern auch die Entwicklung zukünftiger Geräte kann sicherer gestaltet werden. Für seine Tests nutzte Rupprecht unter anderem eine Basisstation, die die Dortmunder Forscher vom Lehrstuhl für Kommunikationsnetze unter der Leitung von Prof. Dr. Christian Wietfeld abgeschirmt im Labor betreiben, sodass durch die Experimente keine Störungen entstehen. „Wir stehen in engem Kontakt, telefonieren regelmäßig und tauschen uns bei Treffen aus“, beschreibt er die Zusammenarbeit. Inhaltlich beschäftigen sich die Dortmunder allerdings mit einer etwas anderen Frage als die Bochumer Wissenschaftler. Bei ihnen geht es darum, wie Daten zuverlässig, auch zeitkritisch, sprich in wenigen Millisekunden, zugestellt werden können. So kann jederzeit ein sicherer Betrieb der auf stabile Kommunikation angewiesenen Infrastrukturen gewährleistet werden. Neben herausfordernden Situationen wie Naturkatastrophen werden durch die Zusammenarbeit beider Universitäten insbesondere Angriffe auf beispielsweise eine Windkraftanlage durch rechtzeitige Gegenmaßnahmen handhabbar gemacht.

Für David Rupprecht bietet das Bercom-Projekt auch in den kommenden Monaten genug Arbeit. So wird er weiter die Sicherheit von Komponenten im Mobilfunknetz analysieren und ermöglichen, dass aktuelle und zukünftige Mobilfunkstandards sicher in kritischen Infrastrukturen eingesetzt werden können.

Text: rr, Fotos: rs

REDAKTIONSSCHLUSS

Die Rubin-Redaktion kümmert sich nicht nur um das Wissenschaftsmagazin, sondern hat in den vergangenen Monaten gemeinsam mit verschiedenen Forschern der RUB auch einen Kalender für das Jahr 2018 auf die Beine gestellt – mit Fotos von Exkursionen in entlegene Ecken der Welt. Metropolen stehen dabei zwar nicht im Vordergrund. Aber diese Nachtaufnahme von André Baumeister aus Kapstadt hat es in die Auswahl geschafft. Der Kalender ist erhältlich im Unishop der RUB, im Blue Square Store in der Bochumer Innenstadt sowie in verschiedenen Bochumer Buchhandlungen.

↗ *www.news.rub.de/mitgereist*

IMPRESSUM

HERAUSGEBER: Rektorat der Ruhr-Universität Bochum in Verbindung mit dem Dezernat Hochschulkommunikation (Abteilung Wissenschaftskommunikation) der Ruhr-Universität Bochum

WISSENSCHAFTLICHER BEIRAT: Prof. Dr. Gabriele Bellenberg (Philosophie und Erziehungswissenschaften), Prof. Dr. Astrid Deuber-Mankowsky (Philologie), Prof. Dr. Reinhold Glei (Philologie), Prof. Dr. Achim von Keudell (Physik und Astronomie), Prof. Dr. Michael Hübner (Elektrotechnik/Informationstechnik), Prof. Dr. Wolfgang Linke (Medizin), Prof. Dr. Denise Manahan-Vaughan (Medizin), Prof. Dr. Martin Muhler (Chemie), Prof. Dr. Franz Narberhaus (Biologie), Prof. Dr. Andreas Ostendorf (Prorektor für Forschung, Transfer und wissenschaftlichen Nachwuchs), Prof. Dr. Michael Roos (Wirtschaftswissenschaft), Prof. Dr. Tom Schanz (Bau- und Umweltingenieurwissenschaften), Prof. Dr. Michael Wala (Geschichtswissenschaft)

REDAKTIONSANSCHRIFT: Dezernat Hochschulkommunikation, Abteilung Wissenschaftskommunikation, Ruhr-Universität Bochum, 44780 Bochum, Tel.: 0234/32-25228, Fax: 0234/32-14136, rubin@rub.de, news.rub.de/rubin

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

FOTOGRAFIE: Damian Gorczany (dg), Hofsteder Str. 66, 44809 Bochum, Tel.: 0176/29706008, damiangorczany@yahoo.de, www.damiangorczany.de; Roberto Schirdewahn (rs), Offerkämpe 5, 48163 Münster, Tel.: 0172/4206216, post@people-fotograf.de, www.wasaufdieaugen.de

COVERFOTO: Roberto Schirdewahn

BILDNACHWEISE INHALTSVERZEICHNIS: Teaserfotos für die Seiten 16, 54, 58: Damian Gorczany; Teaserfoto für die Seite 20: NASA JPL-Caltech; Teaserfotos für die Seiten 38 und 44: Roberto Schirdewahn

GRAFIK, ILLUSTRATION, LAYOUT UND SATZ: Agentur der RUB, www.rub.de/agentur

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

AUFLAGE: 7.000

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

BEZUG: RUBIN erscheint zweimal jährlich und ist erhältlich im Dezernat Hochschulkommunikation (Abteilung Wissenschaftskommunikation) der Ruhr-Universität Bochum. Das Heft kann kostenlos abonniert werden unter rubin.rub.de/abonnement.

ISSN: 0942-6639