RUHR-UNIVERSITÄT BOCHUM

RUB

RUBIN

SCIENCEMAGAZINE

SPECIAL ISSUE

IT SECURITY

Three tough nuts for quantum computers to crack

This is how artificially generated images reveal their true colours

Start-up: Ready for the new generation of mobile communications

33
Volume

Special Issue
2023

Secret services want to know as much as possible. For example, they try to circumvent data encryption. This can cause collateral damage, warn Bochum researchers.

Intentional vulnerabilities in encryption algorithms seem tempting to secret services and law enforcement agencies alike – after all, they allow supposedly secure information to be read. Professor Gregor Leander and Dr. Christof Beierle from the Chair of Symmetric Cryptography and Dr. David Rupprecht from the Chair of System Security discuss the sense and nonsense of such backdoors and describe a very long-lasting example of such a gap. Together with international colleagues, they showed that current smartphones still have the insecure mobile phone encryption GEA-1 installed. It has been around since the 1990s, and according to mobile phone standards, it should have disappeared in 2013.

Professor Leander, Dr. Rupprecht, Dr. Beierle, you are looking for secret backdoors. What exactly is that?

David Rupprecht: A backdoor is a kind of in-built weak link in the encryption process. You can think of it like a master key that shouldn't exist in the first place. In the case we are investigating, it is physically located in a chipset installed in mobile phones, i.e. on the hardware.

Gregor Leander: In our case, it's symmetric cryptography. This means that all those legitimately involved in the communication – in this case mobile phones and cell towers – have the same key. The underlying algorithm is, so to speak, the recipe for producing these keys.

Rupprecht: In order to generate the key, which, by the way, is regenerated with every new contact between the mobile phone and the mast, an additional secret code stored on the SIM card of the mobile phone is needed. Based on this, the GEA key is calculated by an algorithm, both from the mobile phone and the mobile mast. The result means for both of them: we are friends, we can communicate.

Which data is affected by the security vulnerability in GEA-1?

Leander: Basically, all of them. But this is not relevant for all data. Because when I use online banking, for example, the data is additionally encrypted by the bank, end-to-end, so it is not decrypted at all in between.

Christof Beierle: In the 1990s, when GEA encryption was first introduced, this was not yet the case.

Leander: However, such backdoors are less about the actual contents of the information that is sent back and forth, but rather about metadata, which is often underestimated. It's about the information: who communicates with whom and when? This metadata is of tremendous value. This is evident from the fact that Meta Platforms introduced end-to-end encryption for WhatsApp without much pressure from users. This seems like a contradiction, because Facebook lives off data. The reason is simple: Facebook still sees the metadata. And this is enough.

Who instigates the installation of backdoors in the systems?

Leander: Such backdoors are of course in the interest of the secret services and law enforcement agencies. Invariably, backdoors for these purposes are always being discussed, even if they don't make much sense. In the case of GEA-1, you have to remember that it was developed in the 1990s. At that time, cryptography was considered a weapon. Powerful cryptography was not allowed to be exported abroad, there were strict export restrictions. But of course people wanted to sell mobile phones to other countries, too. So they had to get around these export restrictions.

Beierle: We have a document from 1998 on the requirements for the cipher. One of them was: the encryption had to be exportable according to certain restrictions. That means: it had to be just weak enough to get through, but not too weak either.

Who sets such standards as those governing encryption?

Rupprecht: In the case of GEA, it was the European Standard Organisation ETSI, a kind of DIN institute at European level. The organisation includes, for example, large manufacturers, companies such as Deutsche Telekom, as well as governmental organisations.

Leander: We can't rule out the possibility that members of the secret services were also employed there at the time.

▸

Interview

SECURITY WITH AN **IN-BUILT VULNERABILITY**

Gregor Leander, David Rupprecht and Christof Beierle (from left) deal with backdoors in computer systems.

The former weaknesses of cryptography are now known, and the procedures have become more public.

Has the backdoor in GEA-1 been exploited?

Leander: As far as GEA is concerned, we don't know whether it was used or not. But in other cases, it has been proven that backdoors were exploited.

Rupprecht: The revelations published by Edward Snowden, for example, brought to light that Angela Merkel's mobile phone was bugged. If you wonder how that could have been accomplished, you quickly come up with encryption methods that work not unlike GEA and are used for voice telephony. Here, too, a relatively weak algorithm was integrated.

Dr. Leander, you've just indicated that you don't consider deliberately built-in backdoors to be useful as far as the authorities are concerned.

Leander: There are 1,000 legitimate reasons for law enforcement and intelligence agencies to want such backdoors to exist. But they are the wrong way to go. A master key like that can also be found by someone who may have criminal intentions. And once the loophole is there, it is always there – after all, we can see that it hasn't been possible to eliminate GEA-1 to this day, even though it should have been done years ago.

Rupprecht: There is another aspect: if everyone knows that only weak algorithms are allowed, criminals will hide from the authorities by using secure encryption. Criminals don't care that cryptography is forbidden. They simply switch to their own system. In addition, of course, there are fundamental principles of democracy such as the protection of privacy. Mass surveillance is not compatible with democratic values.

How come GEA is still integrated in the latest devices, even though we know that the encryption has a backdoor?

Rupprecht: Well, the manufacturing industry is huge, so maybe it just slips under the radar because it's not a priority at the moment.

Should we assume that encryption algorithms with backdoors are active in all our devices?

Leander: No. We are now keeping a close eye on things.

Rupprecht: Not in end devices. This is currently an issue in the network products, for example routers, on which the internet is based. There are examples of more recent encryptions with backdoors. A recent case is the manipulation of random number generators by the US secret service NSA. Randomness is often necessary in encryption algorithms, and if you ensure that zeros instead of ones are generated super randomly, you can simplify the encryption keys. In the case of NSA, the manipulated algorithm was so slow that no one wanted it, so companies were paid to put it in.

Leander: On the other hand, cryptographic algorithms without a backdoor do exist.

Rupprecht: There's been a shift since the 1990s: the weaknesses of cryptography at that time are now known, and the algorithms have become more public.

Beierle: It's always suspicious when algorithms are not public. The GEA1 standard, for example, was secret.

Leander: Today, the selection of encryption methods is pub-

The problem of backdoors remains abstract for many. However, the industry community really wants to do something.

> „CRIMINALS DON'T CARE THAT CRYPTOGRAPHY IS FORBIDDEN.“
>
> David Rupprecht

lic and transparent. Researchers submit proposals, which are evaluated in a multi-stage process. If there's even a hint of ambiguity, the proposal is immediately rejected. So there are no more deliberate weaknesses in public encryption protocols. This is also one of the reasons why we at the Cluster of Excellence CASA believe that protection against secret services like the NSA is possible: mathematical algorithms do exist that no-one in the world can break. Therefore, we can be hopeful.

What are your plans for your future activities?

Leander: We will continue to look for backdoors. There are indications that they exist, the only problem is finding them. We are looking for them in a structured way. We look at large programmes, sift out the cryptography and analyse them – especially the ones that are new to us. Some of them are secret. In the case of GEA-1, a whistleblower tipped us off, and the same applies to another case we are currently investigating.

How come there is no public outcry when such discoveries come to light?

Leander: There's no outcry from users, but there is a great echo in the press. The interest is there.

Beierle: Maybe there wasn't such a big outcry at GEA, because the method is so old and no longer poses a danger.

Rupprecht: We have to make end users understand what is at stake. But the problem remains very abstract for many. The situation is different in the industry. Manufacturers are really willing to do something about it.

Leander: You really have to distinguish between users and decision-makers. End users don't care about their data. Quite the contrary, considering how they use social media. The same applies to using amazing services on the internet for free – how does that work? Simply by having your data harvested. But people don't care about that. The decision-makers have to care. It's like driving a car: if seat belts weren't compulsory, no-one would wear them.

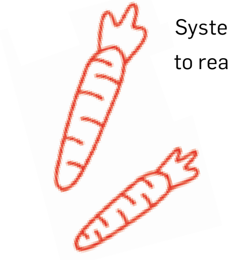
text: md, photos: ms

EDITOR'S DEADLINE

CASA UNIVERSE
WHAT'S THE FUZZ ABOUT HUB C AND THE MISSING CARROTS?
A JOURNEY THROUGH THE SECRETS OF SECURE SYSTEMS AND THE EXCITING RESEARCH WORLD OF CASA

The rabbits in the CASA Universe are startled: the seemingly well-secured access to Rabbit Mark's carrot stash has been hacked and all winter supplies have been stolen. The brave bunny Betty then starts looking for support at the nearby CASA Hub C – a mysterious place that is supposed to hold solutions for digital security. Thus begins the adventure of Betty the bunny, the protagonist of the first science comic from the Cluster of Excellence CASA. Along with Betty, the readers explore the Research Hub and learn about the research priorities and challenges that the scientists in the Research Hub C "Secure Systems" deal with on a daily basis. Find out how to read this and more CASA comics at no cost at:

↗ *casa.rub.de/en/outreach/science-comics*



Answers
DEEP FAKE-QUIZ
The following faces are real:
1a, 2a, 3b, 4a, 5b, 6a

??

LEGAL NOTICE

PUBLISHER: Cluster of Excellence CASA at the Horst Görtz Institute for IT Security at Ruhr University Bochum in collaboration with the Corporate Communications Department at Ruhr University Bochum (Hubert Hundt, v.i.S.d.P.)

EDITORIAL ADDRESS: Corporate Communications Department, Editorial Office Rubin, Ruhr-Universität Bochum, 44780 Bochum, Germany, phone: +49 234 32 25228, rubin@rub.de, news.rub.de/rubin

EDITORIAL BOARD: Dr. Julia Weiler (jwe, editor-in-chief); Meike Drießen (md); Lisa Bischoff (lb)

PHOTOGRAPHER: Michael Schwettmann (ms), Dammstr. 6, 44892 Bochum, Tel.: +49 177 3443543, info@michaelschwettmann.de, www.michaelschwettmann.de

COVER: Sashkin – stock.adobe.com

PHOTOGRAPHS FOR TABLE OF CONTENTS: Michael Schwettmann

GRAPHIC DESIGN, ILLUSTRATION, LAYOUT:
Agentur für Markenkommunikation, Ruhr-Universität Bochum,
www.einrichtungen.rub.de/de/agentur-fuer-markenkommunikation

PRINTED BY: LD Medienhaus GmbH & Co. KG, Van-Delden-Str. 6-8, 48683 Ahaus, Germany, Tel.: +49 231 90592000, info@ld-medienhaus.de, www.ld-medienhaus.de

EDITION: 800

DISTRIBUTION: Rubin is published twice a year in German language; the regular issues are available from the Corporate Communications Department at Ruhr-Universität Bochum. The magazine can be subscribed to free of charge at news.rub.de/rubin/abo. The subscription can be cancelled by email to rubin@rub.de. The special issue 2021 is available from the Horst Görtz Institute for IT Security. In case of interest, please contact hgi-presse@rub.de.

ISSN: 0942-6639

Reprinting with reference to source and submission of proof copies