Karsten Nohl

From Wikipedia, the free encyclopedia

[Jump to navigation](https://en.wikipedia.org/wiki/Karsten_Nohl#mw-head)[Jump to search](https://en.wikipedia.org/wiki/Karsten_Nohl#searchInput)

**Karsten Nohl** (born August 11, 1981)[[1]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-stern-1) is a German [cryptography](https://en.wikipedia.org/wiki/Cryptography) expert[[2]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-heise-2) and hacker. His areas of research include GSM security, RFID security, and privacy protection.[[3]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-cv-3)



**Contents**

* [1Life](https://en.wikipedia.org/wiki/Karsten_Nohl#Life)
* [2Areas of Research](https://en.wikipedia.org/wiki/Karsten_Nohl#Areas_of_Research)
  + [2.1RFID Security](https://en.wikipedia.org/wiki/Karsten_Nohl#RFID_Security)
    - [2.1.1Mifare Security](https://en.wikipedia.org/wiki/Karsten_Nohl#Mifare_Security)
    - [2.1.2Legic Security](https://en.wikipedia.org/wiki/Karsten_Nohl#Legic_Security)
    - [2.1.3Car Immobilizer](https://en.wikipedia.org/wiki/Karsten_Nohl#Car_Immobilizer)
  + [2.2Mobile Network Security](https://en.wikipedia.org/wiki/Karsten_Nohl#Mobile_Network_Security)
    - [2.2.1deDECTed.org](https://en.wikipedia.org/wiki/Karsten_Nohl#deDECTed.org)
    - [2.2.2A5/1 Security Project](https://en.wikipedia.org/wiki/Karsten_Nohl#A5/1_Security_Project)
    - [2.2.3GSM Sniffing](https://en.wikipedia.org/wiki/Karsten_Nohl#GSM_Sniffing)
    - [2.2.4GPRS Security](https://en.wikipedia.org/wiki/Karsten_Nohl#GPRS_Security)
    - [2.2.5SIM Card DES-Hack](https://en.wikipedia.org/wiki/Karsten_Nohl#SIM_Card_DES-Hack)
    - [2.2.6GSM Security Map und SnoopSnitch](https://en.wikipedia.org/wiki/Karsten_Nohl#GSM_Security_Map_und_SnoopSnitch)
    - [2.2.7SS7 Hacking](https://en.wikipedia.org/wiki/Karsten_Nohl#SS7_Hacking)
    - [2.2.8Android Patching](https://en.wikipedia.org/wiki/Karsten_Nohl#Android_Patching)
  + [2.3Security of payment and booking systems](https://en.wikipedia.org/wiki/Karsten_Nohl#Security_of_payment_and_booking_systems)
    - [2.3.1Attacks on the Electronic Cash protocol](https://en.wikipedia.org/wiki/Karsten_Nohl#Attacks_on_the_Electronic_Cash_protocol)
    - [2.3.2Security gaps in travel booking systems](https://en.wikipedia.org/wiki/Karsten_Nohl#Security_gaps_in_travel_booking_systems)
  + [2.4IT Security research](https://en.wikipedia.org/wiki/Karsten_Nohl#IT_Security_research)
    - [2.4.1BadUSB](https://en.wikipedia.org/wiki/Karsten_Nohl#BadUSB)
* [3External links](https://en.wikipedia.org/wiki/Karsten_Nohl#External_links)
* [4References](https://en.wikipedia.org/wiki/Karsten_Nohl#References)

Life[[edit](https://en.wikipedia.org/w/index.php?title=Karsten_Nohl&action=edit&section=1&editintro=Template:BLP_editintro)]

Nohl grew up in the [Rhineland](https://en.wikipedia.org/wiki/Rhineland) area of Germany and studied electrical engineering at the [Heidelberg University](https://en.wikipedia.org/wiki/Heidelberg_University) of applied sciences from 2001 to 2004.[[1]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-stern-1)[[3]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-cv-3) From 2005 to 2008, he earned his PhD at the [University of Virginia](https://en.wikipedia.org/wiki/University_of_Virginia) on Implementable Privacy for RFID Systems.[[3]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-cv-3) Since 2010 Nohl has served as the Managing Director and Chief Scientist of the Berlin-based consultancy and think tank, Security Research Labs.[[3]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-cv-3)[[4]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-linkedin-4)[[5]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-impressum-5) Karsten has also served as interim CISO for the Indian corporation [Jio](https://en.wikipedia.org/wiki/Jio) from 2014 to 2017, as well as, for the Indonesian corporation [Axiata](https://en.wikipedia.org/wiki/Axiata) in 2017.[[4]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-linkedin-4)

Areas of Research[[edit](https://en.wikipedia.org/w/index.php?title=Karsten_Nohl&action=edit&section=2&editintro=Template:BLP_editintro)]

**RFID Security**[[edit](https://en.wikipedia.org/w/index.php?title=Karsten_Nohl&action=edit&section=3&editintro=Template:BLP_editintro)]

**Mifare Security**[[edit](https://en.wikipedia.org/w/index.php?title=Karsten_Nohl&action=edit&section=4&editintro=Template:BLP_editintro)]

Together with Henryk Plötz and [CCC](https://en.wikipedia.org/wiki/Chaos_Computer_Club) Berlin's, [Starbug](https://en.wikipedia.org/wiki/Jan_Krissler), Nohl gave a presentation in December 2007 on how the encryption algorithm used in [Mifare Classic](https://en.wikipedia.org/wiki/MIFARE) RFID smart cards was cracked. The Mifare Classic Card has been used in many micropayment applications, such as the Oyster card, CharlieCard, or the OV Chipkaart for payment.[[6]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-press-6)[[7]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-cccplan-7)[[8]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-cccvid-8)

**Legic Security**[[edit](https://en.wikipedia.org/w/index.php?title=Karsten_Nohl&action=edit&section=5&editintro=Template:BLP_editintro)]

Together with Henryk Plötz, Nohl gave a presentation in December 2009 documenting the flawed security of Legic Prime RFID security. The talk demonstrated how the system employed multiple layers of strange and obscure techniques in lieu of standard encryption and cryptographic protocols. This allowed cards to be read, emulated, and even for arbitrary master tokens to be created.[[9]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-legic-9)

**Car Immobilizer**[[edit](https://en.wikipedia.org/w/index.php?title=Karsten_Nohl&action=edit&section=6&editintro=Template:BLP_editintro)]

At SIGINT-2013, Nohl gave a presentation on the insecurity of electronic car immobilizers used to prevent vehicle theft, documenting vulnerabilities in the three most widely used systems: DST40 ([Texas Instruments](https://en.wikipedia.org/wiki/Texas_Instruments)), Hitag 2 ([NXP Semiconductors](https://en.wikipedia.org/wiki/NXP_Semiconductors)) and Megamos ([EM Micro](https://en.wikipedia.org/wiki/EM_Micro)).[[10]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-car-10)

**Mobile Network Security**[[edit](https://en.wikipedia.org/w/index.php?title=Karsten_Nohl&action=edit&section=7&editintro=Template:BLP_editintro)]

**deDECTed.org**[[edit](https://en.wikipedia.org/w/index.php?title=Karsten_Nohl&action=edit&section=8&editintro=Template:BLP_editintro)]

Nohl was part of the project group deDECTed.org[[11]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-dedected-11) [11], which in 2008 at [25C3](https://en.wikipedia.org/wiki/Chaos_Communication_Congress) pointed out serious deficiencies in the DECT protocol.[[12]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-12)

In April 2010, Nohl, together with Erik Tews and Ralf-Philipp Weinmann, published details on the cryptographic analysis of DECT proprietary and secret encryption algorithm used ([DECT standard cipher](https://en.wikipedia.org/wiki/Digital_Enhanced_Cordless_Telecommunications)), which is based on [reverse engineering](https://en.wikipedia.org/wiki/Reverse_engineering) of DECT hardware and descriptions from a patent specification.[[13]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-dectcrypto-13)

**A5/1 Security Project**[[edit](https://en.wikipedia.org/w/index.php?title=Karsten_Nohl&action=edit&section=9&editintro=Template:BLP_editintro)]

In the summer of 2009 Nohl introduced the A5 / 1 Security Project.[[14]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-a51-14) The project demonstrated an attack on the GSM encryption standard [A5/1](https://en.wikipedia.org/wiki/A5/1) using [Rainbow Tables](https://en.wikipedia.org/wiki/Rainbow_table). With the help of volunteers, the key tables were calculated in a few months and published on the 26C3 in December 2009.[[15]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-15)

The [GSM Association](https://en.wikipedia.org/wiki/GSM_Association) described Nohl's plans as illegal and denied that wiretapping was actually possible. He replied that his research was purely academic.[[16]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-16)

As early as 2008, the hacker group THC had begun with the pre-calculation of key tables for A5 / 1, but probably never published the tables because of legal problems.[[14]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-a51-14)

**GSM Sniffing**[[edit](https://en.wikipedia.org/w/index.php?title=Karsten_Nohl&action=edit&section=10&editintro=Template:BLP_editintro)]

At the [27C3](https://en.wikipedia.org/wiki/Chaos_Communication_Congress) in December 2010, Nohl, together with Sylvain Munaut, demonstrated how mobile calls can be cut and decrypted with the help of converted cheap mobile phones and the open-source software OsmocomBB.[[17]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-17) The pair showed that the GSM encryption can be cracked "in about 20 seconds" and that calls can be recorded and played back.[[18]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-18)[[19]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-19)

**GPRS Security**[[edit](https://en.wikipedia.org/w/index.php?title=Karsten_Nohl&action=edit&section=11&editintro=Template:BLP_editintro)]

At [Chaos Communication Camp](https://en.wikipedia.org/wiki/Chaos_Communication_Camp) 2011, Nohl and Luca Melette gave a presentation showing how [GPRS](https://en.wikipedia.org/wiki/GPRS) networks do not securely encrypt their mobile traffic.[[20]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-20) The pair stated that they had recorded data transmissions in the networks of several German mobile providers, including [Deutsche Telekom](https://en.wikipedia.org/wiki/Deutsche_Telekom), [O2 Germany](https://en.wikipedia.org/wiki/Telef%C3%B3nica_Germany), [Vodafone](https://en.wikipedia.org/wiki/Vodafone_Germany) and [E-Plus](https://en.wikipedia.org/wiki/E-Plus).[[2]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-heise-2) Several mobile service providers used either no or only insufficient encryption. With a modified mobile phone, mobile traffic could be read from within a radius of five kilometers.[[2]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-heise-2)

**SIM Card DES-Hack**[[edit](https://en.wikipedia.org/w/index.php?title=Karsten_Nohl&action=edit&section=12&editintro=Template:BLP_editintro)]

At both [Black Hat](https://en.wikipedia.org/wiki/Black_Hat_Briefings) 2013 and [OHM](https://en.wikipedia.org/wiki/Observe._Hack._Make.) 2013, Nohl demonstrated that many SIM cards use the outdated and insecure [DES](https://en.wikipedia.org/wiki/Data_Encryption_Standard) encryption, undermining the privacy and security of mobile phone users.[[21]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-itu-21)[[22]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-des-22)[[23]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-sim-23) Through "Over The Air (OTA)" communication, such as SMS messages, it is possible to provide a SIM card with updates, applications, or new encryption keys. Such messages are digitally signed with DES, 3DES or AES.[[22]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-des-22)[[23]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-sim-23) Nohl generated a [Rainbow Table](https://en.wikipedia.org/wiki/Rainbow_Table) for 56-bit DES within a year based a on specially signed error message with known plain text.[[22]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-des-22)[[23]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-sim-23) The resulting attack scenario: an attacker sends the victim a signed text message.[[22]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-des-22)[[23]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-sim-23) With the help of the Rainbow Table it is then possible to crack the DES key of a SIM card in minutes and crack the internal key. (Known Plaintext Attack).[[21]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-itu-21)[[22]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-des-22) This allows an attacker to send a signed SMS, which in turn loads a Java app onto the SIM card. These apps are capable of multiple actions, including sending SMS or sharing the location of the device. An attacker could, for example, command a device to send SMS messages to foreign premium services at the cost of the device owner.[[22]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-des-22)[[23]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-sim-23) In principle, the [Java Virtual Machine](https://en.wikipedia.org/wiki/Java_Virtual_Machine) should make sure that every Java app can only access predefined interfaces.[[23]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-sim-23) Nohl found that the Java sandbox implementations of at least two major SIM card manufacturers, including market leader [Gemalto](https://en.wikipedia.org/wiki/Gemalto), are insecure and it is possible for a Java app to escape the sandbox environment and thus gain access to the entire SIM card.[[23]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-sim-23) This makes it possible to duplicate SIM cards including the IMSI, authentication key (Ki) and payment information stored on the card.[[23]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-sim-23)

**GSM Security Map und SnoopSnitch**[[edit](https://en.wikipedia.org/w/index.php?title=Karsten_Nohl&action=edit&section=13&editintro=Template:BLP_editintro)]

At the [30C3](https://en.wikipedia.org/wiki/Chaos_Communication_Congress) in December 2013, Nohl introduced the Android app "GSMmap". Initially designed for use on a Galaxy S2 or S3 (including root access), the app collects information on the level a mobile network secures its traffic. The collected data can be uploaded, with the app user’s consent, to a database that evaluates the security of mobile networks worldwide, based on selected protection capability criteria. The results of this analysis are displayed on the "GSM Security Map" website, where the security level of mobile providers are visualized on an interactive world map and made available for download as "country reports".

At the [31C3](https://en.wikipedia.org/wiki/31C3) in December 2014, Nohl presented the Android app "SnoopSnitch" as a possible countermeasure against various mobile network security attacks. On various smartphones models with Qualcomm chipset and root access, mobile network traffic can be collected and analyzed locally with "SnoopSnitch,” where the app gives the user information about the encryption and authentication algorithm being used by the network, the possibility for SMS and SS7 attacks, as well as the potential presence of [IMSI-catchers](https://en.wikipedia.org/wiki/IMSI-catcher).

The data collected via “SnoopSnitch” can also be uploaded, with the user’s consent, to a database to support additional security analysis, which is shared on the "GSM Security Map" website.

**SS7 Hacking**[[edit](https://en.wikipedia.org/w/index.php?title=Karsten_Nohl&action=edit&section=14&editintro=Template:BLP_editintro)]

Also at the [31C3](https://en.wikipedia.org/wiki/31C3), Nohl presented a [side channel attack](https://en.wikipedia.org/wiki/Side_channel_attack) using [Signaling System 7](https://en.wikipedia.org/wiki/Signaling_System_7) (SS7) on [UMTS](https://en.wikipedia.org/wiki/UMTS) communication and described other SS7-based attacks that can allow the reading of text messages, the determination of location coordinates, and various scenarios for fraud.

**Android Patching**[[edit](https://en.wikipedia.org/w/index.php?title=Karsten_Nohl&action=edit&section=15&editintro=Template:BLP_editintro)]

In April 2018, Nohl presented on security in the mobile Android environment.[[24]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-24) Nohl and his colleagues analyzed Android firmware images from various smartphone vendors. In some cases, a so-called "patch gap" was found, where vendors had not applied all security patches that otherwise should have been present based on the monthly patch level date specified in the firmware. Nohl released an updated version of the open source “Snoopsnitch” app with new features to allow users to run tests on their Android phones to check for a "patch gap" on their device.[[25]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-25)

**Security of payment and booking systems**[[edit](https://en.wikipedia.org/w/index.php?title=Karsten_Nohl&action=edit&section=16&editintro=Template:BLP_editintro)]

**Attacks on the Electronic Cash protocol**[[edit](https://en.wikipedia.org/w/index.php?title=Karsten_Nohl&action=edit&section=17&editintro=Template:BLP_editintro)]

At the [32C3](https://en.wikipedia.org/wiki/32C3), Nohl and colleagues presented an attack on the EC card protocols ZVT and Poseidon, which are a dialect of [ISO 8583](https://en.wikipedia.org/wiki/ISO_8583).[[26]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-26)[[27]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-27) Both protocols are the most common payment protocols in German-speaking countries.

**Security gaps in travel booking systems**[[edit](https://en.wikipedia.org/w/index.php?title=Karsten_Nohl&action=edit&section=18&editintro=Template:BLP_editintro)]

At the [33C3](https://en.wikipedia.org/wiki/33C3), Nohl and colleagues highlighted security holes in [Amadeus](https://en.wikipedia.org/wiki/Amadeus_IT_Group), [Sabre](https://en.wikipedia.org/wiki/Sabre_(computer_system)), and [Travelport](https://en.wikipedia.org/wiki/Travelport), three of the largest [Global Distribution Systems](https://en.wikipedia.org/wiki/Global_distribution_system) (GDS) which combined, handle approximately 90% of worldwide flight reservations and a large proportion of hotel, car rental, and other travel bookings.[[28]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-28)

**IT Security research**[[edit](https://en.wikipedia.org/w/index.php?title=Karsten_Nohl&action=edit&section=19&editintro=Template:BLP_editintro)]

**BadUSB**[[edit](https://en.wikipedia.org/w/index.php?title=Karsten_Nohl&action=edit&section=20&editintro=Template:BLP_editintro)]

At [Black Hat](https://en.wikipedia.org/wiki/Black_Hat_Briefings) 2014, Nohl and Jacob Lell presented on security risks associated with USB devices.[[29]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-blackhatusb-29)[[30]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-blackhat2014-30)[[31]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-srlusb-31)[[32]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-zeitusb-32) The USB standard is versatile and includes many different classes of devices.[[31]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-srlusb-31) Their research is based on the reprogramming of USB controller chips, which are widely used and found in USB sticks.[[31]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-srlusb-31) There is no effective protection against reprogramming, so a harmless USB device can be converted and used as a malicious device in many ways.[[31]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-srlusb-31)

Possible scenarios for abuse include:

* A USB device can emulate a keyboard and issue commands on behalf of the logged-in user to install malware on their computer, malware which would also infect other USB devices connected.[[31]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-srlusb-31)
* A USB device can pretend to be a network card, change the computer's DNS setting, and redirect traffic.[[31]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-srlusb-31)
* A modified USB stick or a USB hard drive can load a small virus during the boot process, which infects the operating system before booting.[[31]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-srlusb-31)

Preventing such attacks is not yet possible because malware scanners have no access to the firmware version of USB devices and behavior detection is difficult.[[31]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-srlusb-31) USB firewalls that can block only certain device classes do not (yet) exist.[[31]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-srlusb-31) The usual process to remove malware - reinstalling the operating system - fails here because the USB stick that installs the operating systems may itself already be infected, as well as a built-in webcam or other USB devices.[[31]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-srlusb-31)

In addition, a proof of concept for Android devices was released to test the security.[[31]](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_note-srlusb-31)

External links[[edit](https://en.wikipedia.org/w/index.php?title=Karsten_Nohl&action=edit&section=21&editintro=Template:BLP_editintro)]

* [Security Research Labs: GSM Security Map](https://gsmmap.org/)
* [Snoopsnitch](https://opensource.srlabs.de/projects/snoopsnitch/): An Android app for analyzing mobile traffic data. Gives the user information about the encryption and authentication algorithm, SMS and SS7 attacks and IMSI catcher.

References[[edit](https://en.wikipedia.org/w/index.php?title=Karsten_Nohl&action=edit&section=22&editintro=Template:BLP_editintro)]

* 1. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-stern_1-0) [***b***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-stern_1-1) *Goebbels, Teresa (August 11, 2011).*[*"GPRS-Hacker Karsten Nohl: Der perfekte Verbrecher"*](https://www.stern.de/digital/smartphones/gprs-hacker-karsten-nohl-der-auftragshacker-3781206.html)*. stern.de (in German).*
  2. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-heise_2-0) [***b***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-heise_2-1) [***c***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-heise_2-2) *Bachfeld, Daniel (August 10, 2011).*[*"GPRS-Verbindungen leicht abhörbar"*](https://www.heise.de/security/meldung/GPRS-Verbindungen-leicht-abhoerbar-1320879.html)*. heise online (in German).*
  3. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-cv_3-0) [***b***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-cv_3-1) [***c***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-cv_3-2) [***d***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-cv_3-3) [*"Karsten Nohl CV"*](http://www.cs.virginia.edu/~kn5f/pdf/CV.Karsten_Nohl.pdf)*(PDF).*
  4. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-linkedin_4-0) [***b***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-linkedin_4-1) [*"Karsten Nohl Linkedin"*](https://www.linkedin.com/in/karsten-nohl/)*. Retrieved May 9, 2019.*
  5. [**^**](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-impressum_5-0) [*"Impressum der Security Research Labs GmbH (SRLABS)"*](https://web.archive.org/web/20160304124510/https:/srlabs.de/impressum)*. Archived from*[*the original*](https://srlabs.de/impressum)*on March 4, 2016.*
  6. [**^**](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-press_6-0) [*"Press Release: Lost Mifare obscurity raises concerns over security of OV-Chipkaart"*](http://www.cs.virginia.edu/~kn5f/OV-card_security.html)*. January 8, 2008. Retrieved August 11,2011.*
  7. [**^**](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-cccplan_7-0) [*"24C3:Mifare"*](https://fahrplan.events.ccc.de/congress/2007/Fahrplan/events/2378.en.html)*. Retrieved August 11, 2011.*
  8. [**^**](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-cccvid_8-0) [*"24C3:Mifare"*](http://dewy.fem.tu-ilmenau.de/CCC/24C3/mpeg4/24c3-2378-en-mifare_security.mp4)*. Retrieved August 11, 2011.*
  9. [**^**](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-legic_9-0) [*"Legic Prime: Obscurity in Depth"*](https://media.ccc.de/v/26c3-3709-en-legic_prime_obscurity_in_depth)*. media.ccc.de. December 28, 2009. Retrieved May 9, 2019.*
  10. [**^**](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-car_10-0) [*"Schedule SIGINT 2013"*](https://web.archive.org/web/20141231100748/http:/sigint.ccc.de/schedule/events/5034.html)*. July 5, 2013. Archived from*[*the original*](http://sigint.ccc.de/schedule/events/5034.html)*on December 31, 2014.*
  11. [**^**](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-dedected_11-0) [*"deDECTed.org"*](https://web.archive.org/web/20101027172605/https:/dedected.org/trac)*. Archived from*[*the original*](https://tools.wmflabs.org/giftbot/deref.fcgi?url=https%3A%2F%2Fdedected.org%2Ftrac)*on October 27, 2010. Retrieved May 9, 2019.*
  12. [**^**](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-12) *Krempl, Stefan (December 30, 2008).*[*"25C3: Schwere Sicherheitslücken beim Schnurlos-Telefonieren mit DECT(update)"*](https://www.heise.de/security/meldung/25C3-Schwere-Sicherheitsluecken-beim-Schnurlos-Telefonieren-mit-DECT-update-192782.html)*. heise online (in German). Retrieved May 9, 2019.*
  13. [**^**](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-dectcrypto_13-0) *Bachfeld, Daniel (April 26, 2010).*[*"Kryptanalyse der DECT-Verschlüsselung"*](https://www.heise.de/security/artikel/Kryptanalyse-der-DECT-Verschluesselung-986714.html)*. Heise Online (in German). Retrieved May 9,2019.*
  14. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-a51_14-0) [***b***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-a51_14-1) *Bachfeld, Daniel (August 26, 2009).*[*"Open-Source-Projekt geht GSM an den Kragen"*](https://www.heise.de/security/meldung/Open-Source-Projekt-geht-GSM-an-den-Kragen-753193.html)*. Heise Online (in German). Retrieved May 9, 2019.*
  15. [**^**](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-15) [*"26C3: GSM: SRSLY?"*](http://dewy.fem.tu-ilmenau.de/CCC/26C3/mp4/26c3-3654-en-gsm_srsly.mp4)*. Retrieved August 11, 2011.*
  16. [**^**](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-16) *Hochstätter, Christoph H.; Nusca, Andrew (December 29, 2009).*[*"26C3: Deutscher Hacker knackt GSM-Verschlüsselung"*](http://www.zdnet.de/news/41525048/26c3-deutscher-hacker-knackt-gsm-verschluesselung.htm)*. ZDNet(in German). Retrieved August 11, 2011.*
  17. [**^**](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-17) [*"27C3:Wideband GSM Sniffing"*](https://media.ccc.de/v/27c3-4208-en-wideband_gsm_sniffing)*. media.ccc.de. Chaos Computer Club. December 28, 2010. Retrieved August 11, 2011.*
  18. [**^**](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-18) *Krempl, Stefan (December 28, 2010).*[*"27C3: Abhören von GSM-Handys weiter erleichtert"*](https://www.heise.de/newsticker/meldung/27C3-Abhoeren-von-GSM-Handys-weiter-erleichtert-1159542.html)*. heise online (in German). Retrieved August 11, 2011.*
  19. [**^**](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-19) [*"27C3 Wideband GSM Sniffing"*](http://dewy.fem.tu-ilmenau.de/CCC/27C3/mp4-h264-HQ/27c3-4208-en-wideband_gsm_sniffing.mp4)*. December 28, 2010. Retrieved August 11, 2011.*
  20. [**^**](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-20) [*"Camp 2011:GPRS Intercept"*](https://fahrplan.events.ccc.de/camp/2011/Fahrplan/events/4504.en.html)*. August 10, 2011. Retrieved May 9, 2019.*
  21. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-itu_21-0) [***b***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-itu_21-1) *Kirsch, Christian (July 21, 2013).*[*"ITU warnt vor Gefahr durch SIM-Karten-Hack"*](https://www.heise.de/security/meldung/ITU-warnt-vor-Gefahr-durch-SIM-Karten-Hack-1920896.html)*. heise Security (in German). Retrieved May 9,2019.*
  22. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-des_22-0) [***b***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-des_22-1) [***c***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-des_22-2) [***d***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-des_22-3) [***e***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-des_22-4) [***f***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-des_22-5) *Schmidt, Jürgen (July 21, 2013).*[*"DES-Hack exponiert Millionen SIM-Karten"*](https://www.heise.de/security/artikel/DES-Hack-exponiert-Millionen-SIM-Karten-1920898.html)*. heise Security (in German). Retrieved May 9, 2019.*
  23. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-sim_23-0) [***b***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-sim_23-1) [***c***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-sim_23-2) [***d***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-sim_23-3) [***e***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-sim_23-4) [***f***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-sim_23-5) [***g***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-sim_23-6) [***h***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-sim_23-7) [*"Rooting SIM cards"*](https://srlabs.de/bites/rooting-sim-cards/)*. Security Research Labs. Retrieved July 9, 2014.*
  24. [**^**](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-24) [*"Uncovering the Android Patch Gap"*](https://www.youtube.com/watch?v=413cminL7c4)*. Hack in the Box 2018. April 28, 2018. Retrieved April 16, 2019.*
  25. [**^**](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-25) [*"SnoopSnitch"*](https://opensource.srlabs.de/projects/snoopsnitch)*. Retrieved May 9, 2019.*
  26. [**^**](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-26) [*"Outdated payment protocols expose customers and merchants"*](https://srlabs.de/bites/pos-vulns/)*. Security Research Labs. Retrieved December 29,2015.*
  27. [**^**](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-27) *Beuth, Patrick (December 22, 2015).*[*"EC Karten: Sicherheitsforscher hacken das EC-Bezahlsystem"*](https://www.zeit.de/digital/datenschutz/2015-12/electronic-cash-bezahlsystem-terminals-gehackt)*. Zeit Online (in German). Retrieved December 29, 2015.*
  28. [**^**](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-28) [*"Legacy booking systems disclose travelers' private information"*](https://srlabs.de/bites/travel-hacking/)*. Security Research Labs. Retrieved March 29, 2018.*
  29. [**^**](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-blackhatusb_29-0) [*"BadUSB – On Accessories that Turn Evil by Karsten Nohl + Jakob Lell"*](https://www.youtube.com/watch?v=nuruzFqMgIw)*. Black Hat. August 11, 2014. Retrieved September 15,2014.*
  30. [**^**](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-blackhat2014_30-0) [*"Black Hat USA 2014"*](https://www.blackhat.com/us-14/briefings.html#Nohl)*. Retrieved September 15, 2014.*
  31. ^ [Jump up to:***a***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-srlusb_31-0) [***b***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-srlusb_31-1) [***c***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-srlusb_31-2) [***d***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-srlusb_31-3) [***e***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-srlusb_31-4) [***f***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-srlusb_31-5) [***g***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-srlusb_31-6) [***h***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-srlusb_31-7) [***i***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-srlusb_31-8) [***j***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-srlusb_31-9) [***k***](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-srlusb_31-10) [*"Turning USB peripherals into BadUSB"*](https://web.archive.org/web/20160418134155/https:/srlabs.de/badusb/)*. Security Research Labs. Archived from*[*the original*](https://opensource.srlabs.de/projects/badusb)*on April 18, 2016. Retrieved July 14, 2015.*
  32. [**^**](https://en.wikipedia.org/wiki/Karsten_Nohl#cite_ref-zeitusb_32-0) *Beuth, Patrick (July 31, 2014).*[*"Jedes USB-Gerät kann zur Waffe werden"*](https://www.zeit.de/digital/datenschutz/2014-07/usb-controller-chip-angriff-srlabs)*. Die Zeit (in German). Retrieved September 15, 2014.*