CASA UNIVERSE

IM SOG DER EINGEBETTETEN SICHERHEIT VON IHUB B

EINE REISE IN DIE TIEFEN DER
HARDWARE-SICHERHEIT UND DIE
AUFREGENDE FORSCHUNGSWELT VON CASA

IM SOG DER EINGEBETTETEN SICHERHEIT VON HUB B

EINE REISE IN DIE TIEFEN
DER HARDWARE-SICHERHEIT UND DIE
AUFREGENDE FORSCHUNGSWELT VON CASA

CASA
CYBER SECURITY IN THE AGE
OF LARGE-SCALE ADVERSARIES

CASA

Cyber Security in the Age of Large-Scale Adversaries

Herausragende Wissenschaftler*innen erforschen und entwickeln im Rahmen des Exzellenzclusters „CASA - Cyber Security in the Age of Large-Scale Adversaries“ (Cybersicherheit im Zeitalter großskaliger Angreifer*innen) starke und nachhaltige Gegenmaßnahmen gegen mächtige Cyber-Angreifer*innen, mit besonderem Fokus auf staatliche Angriffe. Die Forschung von CASA zeichnet sich durch einen starken interdisziplinären Ansatz aus, der nicht nur technische Fragen, sondern auch das Zusammenspiel von menschlichem Verhalten und IT-Sicherheit untersucht. Dieser einzigartige, ganzheitliche Ansatz bildet die Grundlage für exzellente IT-Sicherheitsforschung.

CASA umfasst vier Forschungsbereiche (Research Hubs):

HUB A „Kryptographie der Zukunft“: Forschung zur zukünftigen Kryptographie mit beweisbarer Sicherheit und Entwicklung von Ansätzen, die auch gegen Quantencomputer sicher sind.

HUB B „Eingebettete Sicherheit“: Untersuchung der Sicherheit eingebetteter Systeme auf der Hardware-Ebene sowie der Interaktion von Sicherheitssystemen mit ihrer physischen Umgebung.

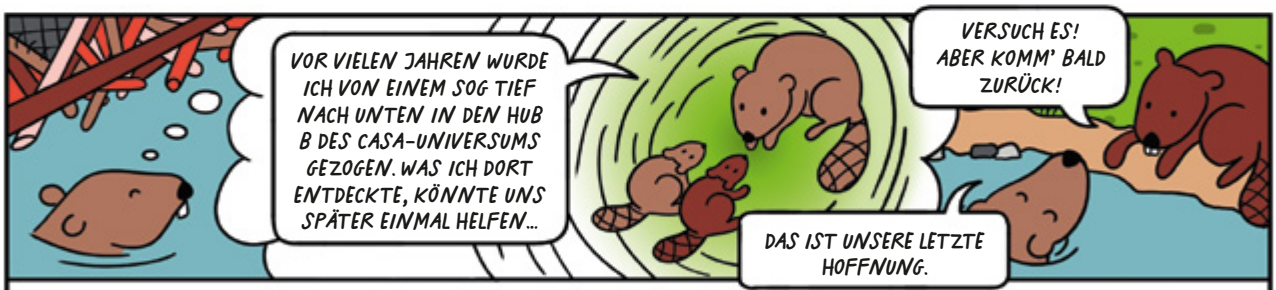
HUB C „Sichere Systeme“: Entwicklung von sicheren und effizienten Systemen auf der Software-Ebene, auch mit Hilfe von Methoden aus dem Bereich des maschinellen Lernens.

HUB D „Usability“: Konzentration auf benutzerfreundliche Sicherheit und Privatsphäre sowie die Erforschung der Schnittstelle zwischen Mensch und Technik.

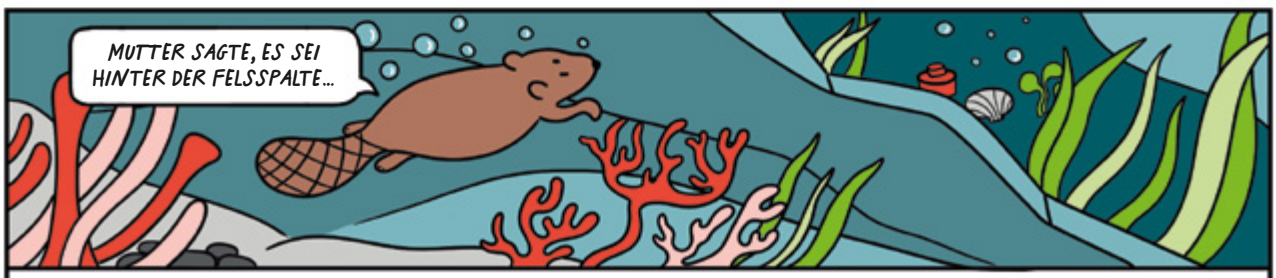
Jeder HUB befasst sich mit spezifischen Forschungsherausforderungen (Challenges), die sorgfältig ausgewählt wurden, um Sicherheitsfragen anzugehen, die für den Schutz vor komplexen Angriffen von entscheidender Bedeutung sind.

Die Challenges des HUB B sind:
Challenge 4: Plattform-Trojaner
Challenge 5: Physical-Layer Sicherheit
Challenge 6: Weiterentwicklung sicherer Implementierungen

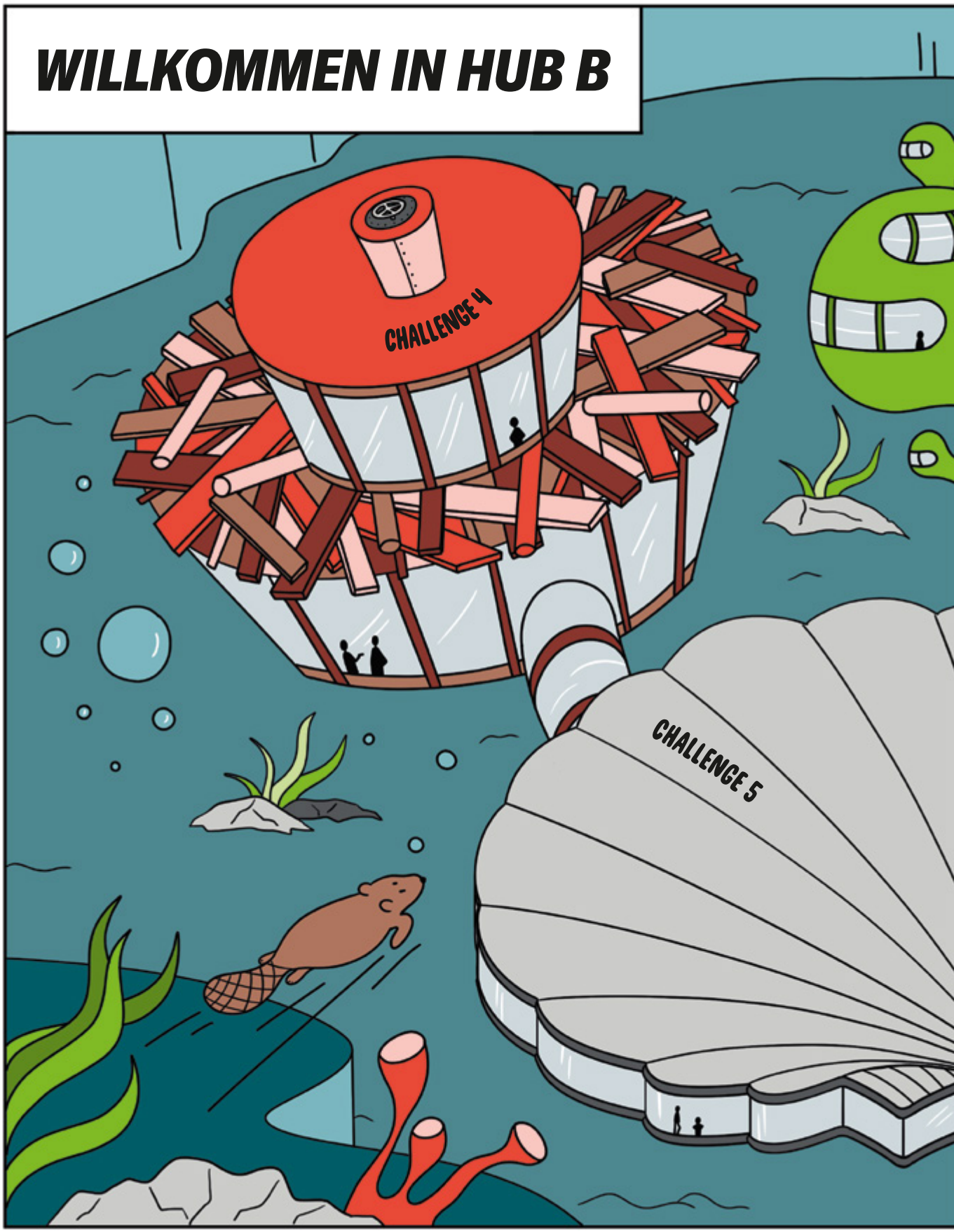
Tief unten im Flusstal des CASA-Universums kämpfen die Biberbrüder Paul und Carl um die Sicherung ihres Damms. Die hölzerne Struktur weist Risse auf und so langsam gehen ihnen die Ideen aus.

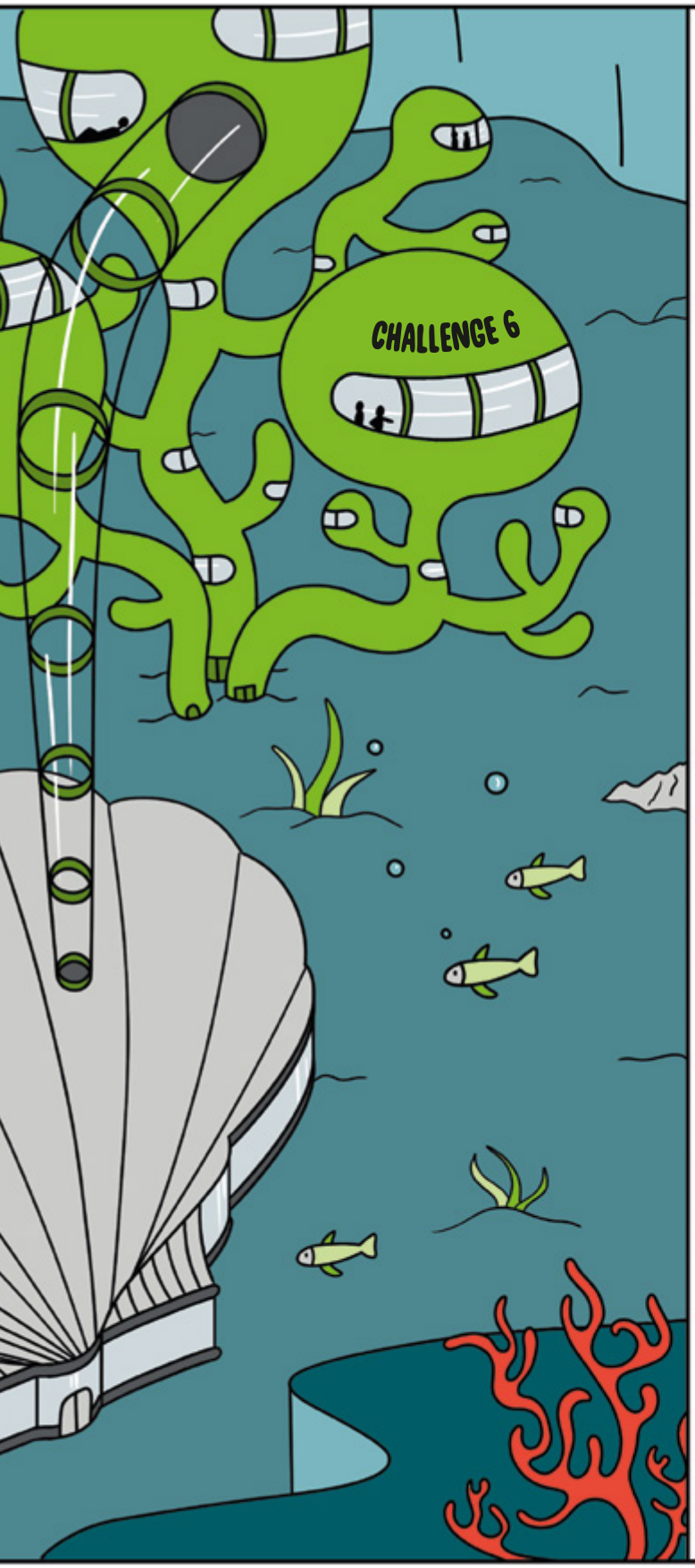


In diesem Moment erinnern sie sich an die Erzählung von einem verborgenen Ort in den Tiefen des Flusses, an dem die Lösung für das Problem der Geschwister zu finden sein könnte.



Paul holt tief Luft und taucht hinab: Nichts kann den verzweifelten Biber davon abhalten, seinen Staudamm zu retten.


WILLKOMMEN IN HUB B
CHALLENGE 4
CHALLENGE 5



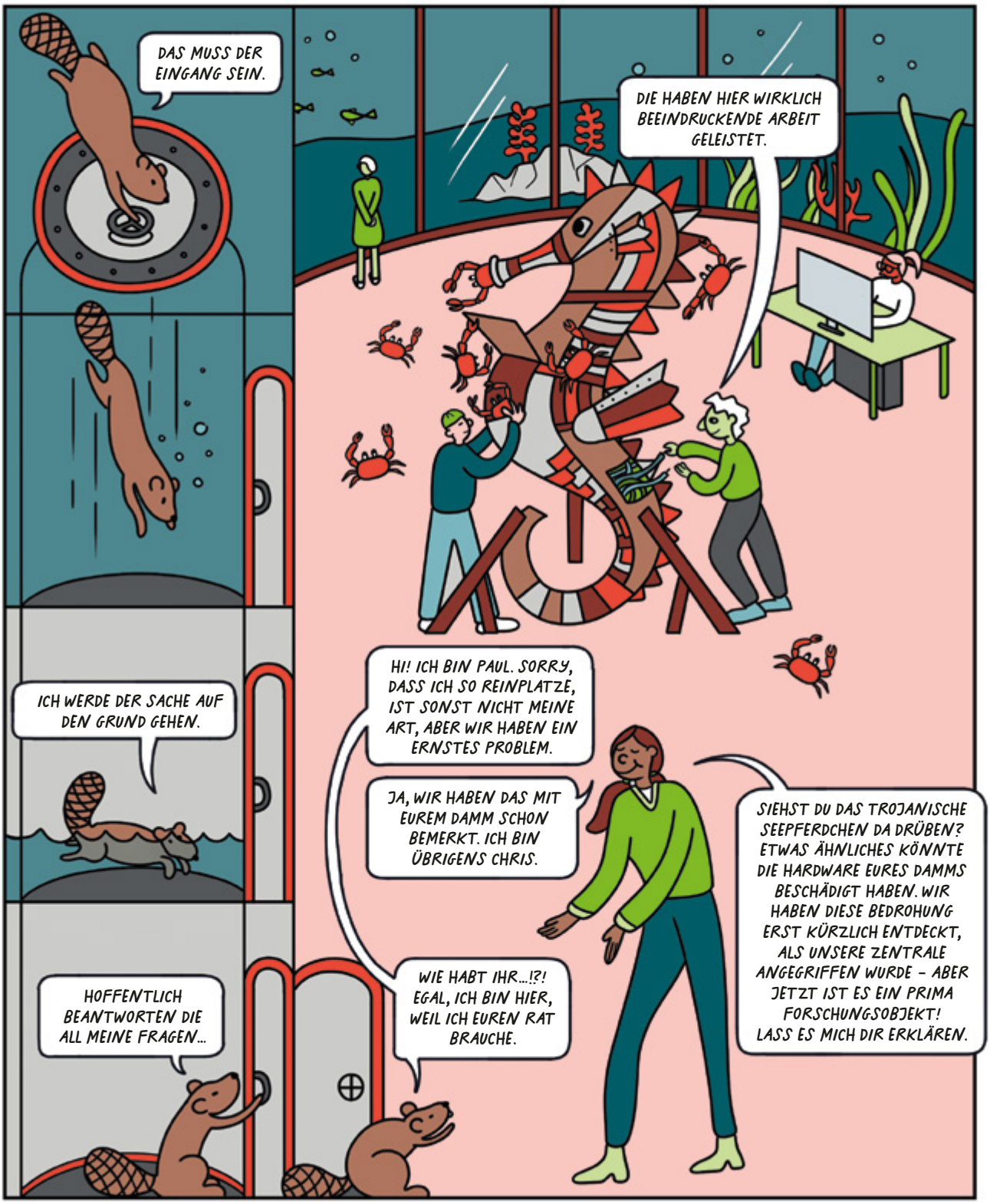
Inhalt

CASA BACKGROUND
CASA steht für „Cyber Security in the Age of Large-Scale Adversaries“ und wird als Exzellenzcluster (EXC) im Rahmen der Exzellenzstrategie der DFG in Deutschland gefördert. Ziel ist es, nachhaltige Sicherheit gegen komplexe, groß angelegte Angriffe zu ermöglichen. Dazu erforscht ein interdisziplinäres Team nicht nur technische, sondern auch menschliche Faktoren und Zusammenhänge. Das Exzellenzcluster ist an der Ruhr-Universität Bochum angesiedelt.

casa.rub.de

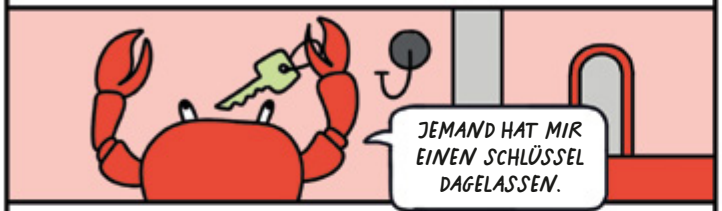
CHALLENGE 4

PLATTFORM-TROJANER



Zuallererst ist es extrem schwierig, solche Manipulationen zu entdecken, und oft unmöglich, sie zu beheben.

Zweitens können Manipulationen auf Hardware-Ebene alle Sicherheitsmechanismen auf höherer Ebene ausschalten.



Schließlich können solche Angriffe Millionen von Geräten, wie zum Beispiel Netzwerk-Router, schwächen.

CASA WIKI

Hacker sind Menschen mit fortgeschrittenen Kenntnissen über Hardware und Software: White-Hat-Hacker suchen nach Schwachstellen, um sie zu entschärfen. Black-Hat-Hacker hingegen nutzen sie für böswillige Zwecke aus.

Ein **Mikrochip** ist ein kleines elektronisches Bauteil, das viele Funktionen ausführen kann – z.B. das Speichern und Verarbeiten von Informationen. Mikrochips sind elementare Bestandteile von Smartphones, Autos, Flugzeugen und vielen anderen Geräten.

Ein **Hardware-Trojaner** ist eine schädliche Modifikation in einem Mikrochip oder elektronischen Gerät. Er wird nach der Herstellung von Dritten eingefügt, um die Funktionalität oder Sicherheit zu beeinträchtigen. Der Name bezieht sich auf die griechische Sage vom Trojanischen Pferd.

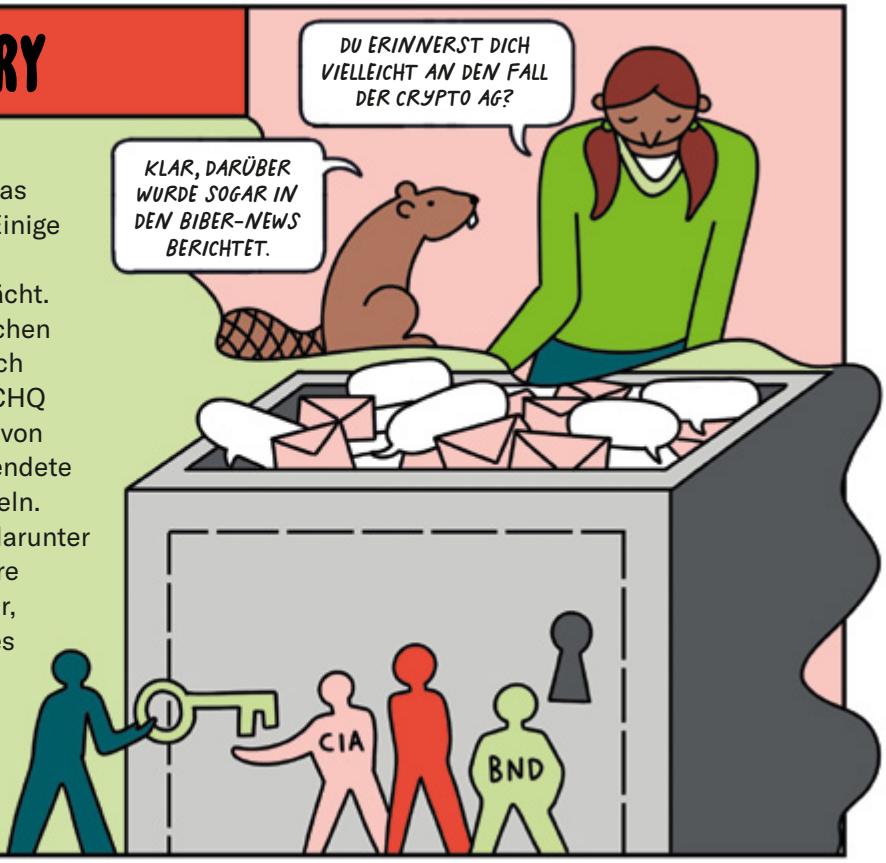
Beim **Hardware Reverse Engineering** wird ein elektronisches Gerät (z.B. ein Mikrochip) zerlegt, um dessen Aufbau und Funktionsweise zu verstehen. Dadurch können Urheberrechtsverletzungen oder Hardware-Trojaner entdeckt werden.

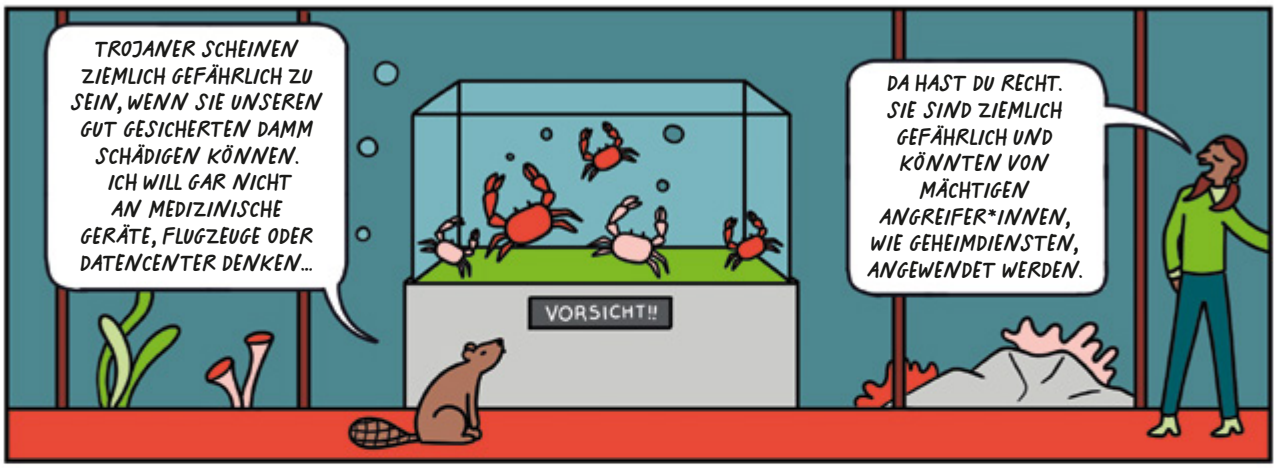
Kognitive Obfuskation erschwert das Reverse Engineering von Hardware. Zunächst werden menschliche Denkstrategien bei der Hardware-Analyse untersucht, um diesen dann gezielt entgegenzuwirken und so den Diebstahl geistigen Eigentums zu verhindern.

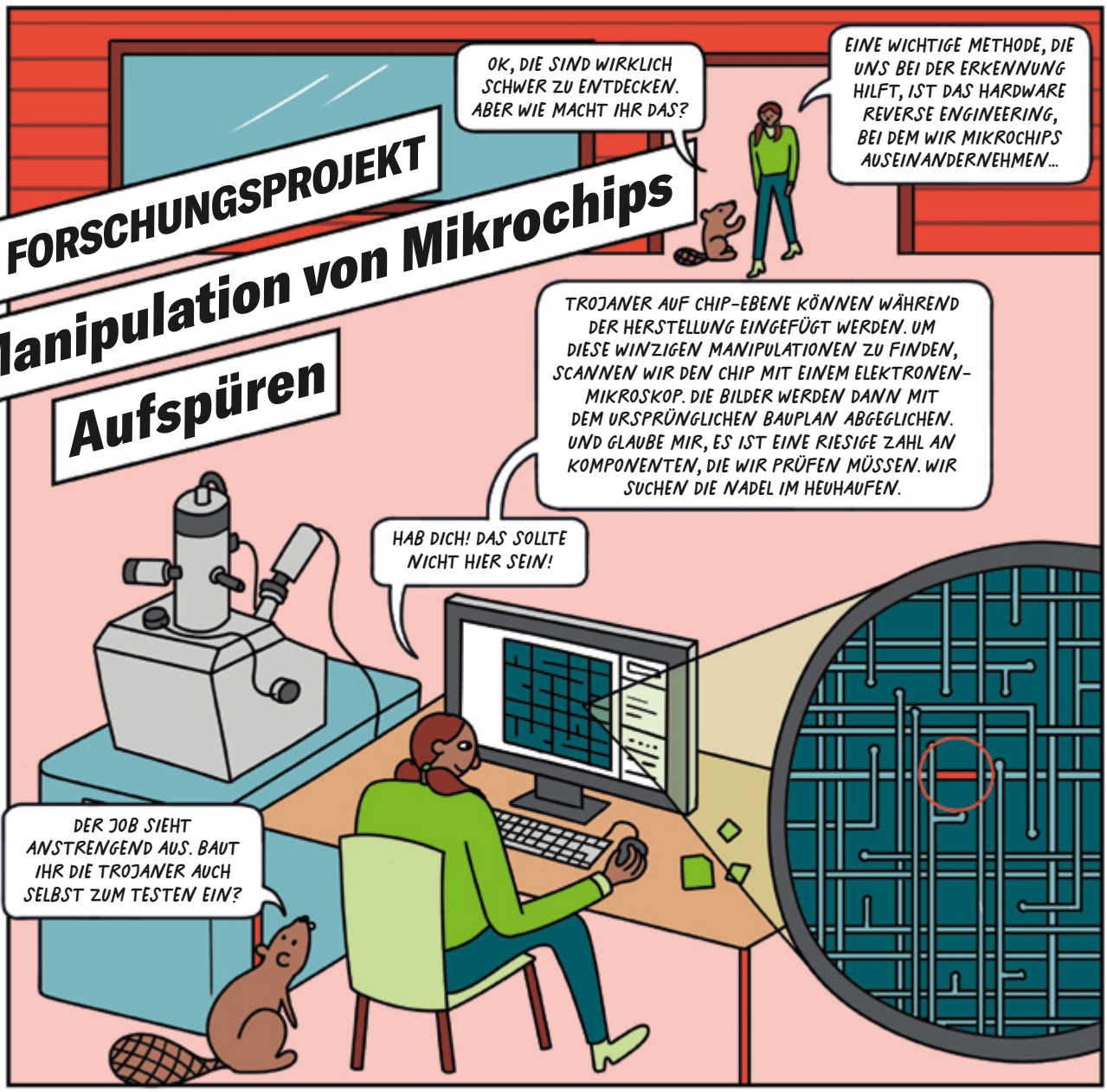
Microcode ist ein aktualisierbarer Bestandteil moderner CPUs, um Probleme in Chips nachträglich beheben zu können. Die Design-Details sind meist Betriebsgeheimnisse. Die Aktualisierbarkeit ist nützlich, birgt aber die Gefahr schädlicher Eingriffe.

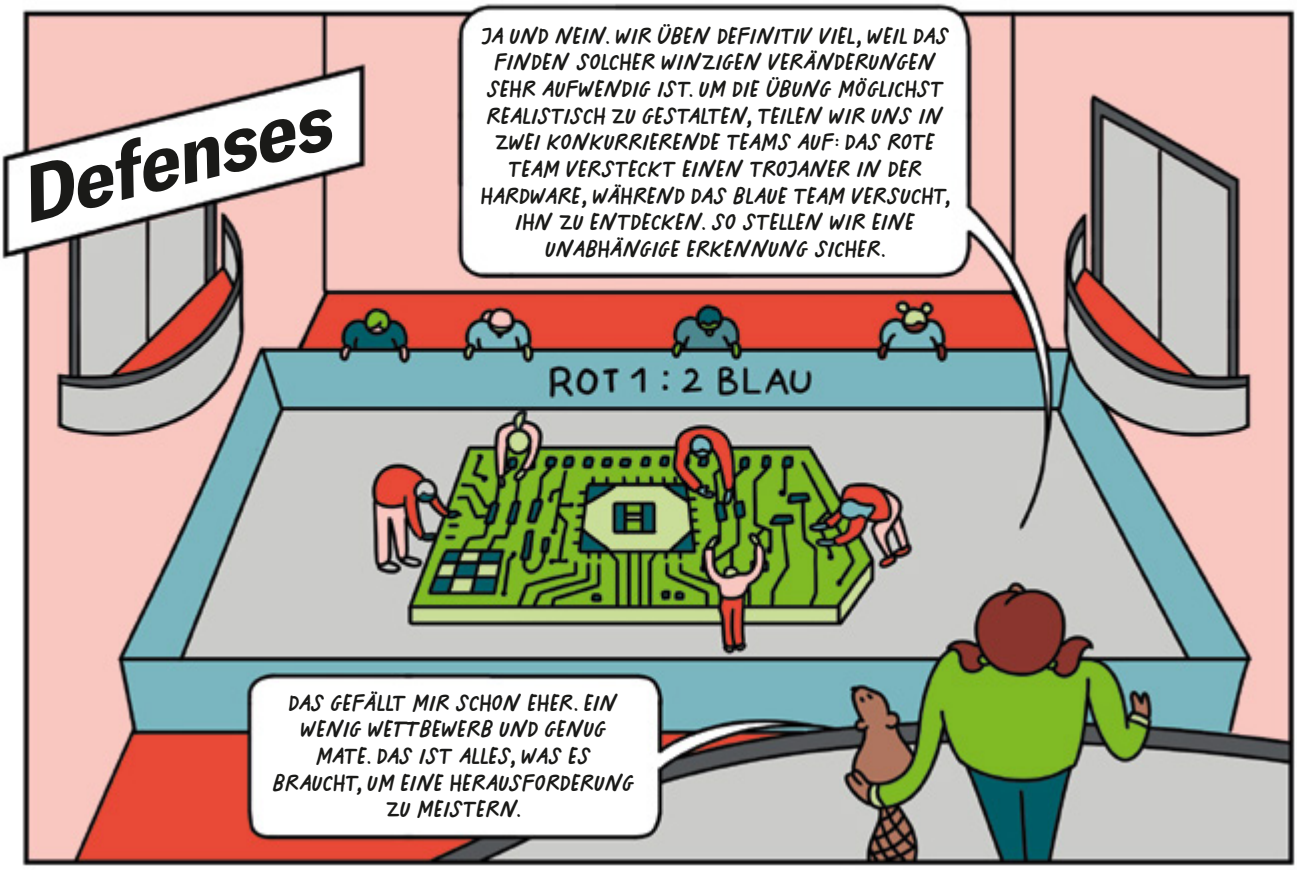
REAL LIFE STORY

Die Crypto AG war ein Schweizer Unternehmen, das Chiffriergeräte herstellte. Einige Geräte wurden absichtlich durch Hintertüren geschwächt. Dies ermöglichte es westlichen Geheimdiensten (namentlich der CIA, dem britischen GCHQ und dem deutschen BND), von anderen Nutzer*innen gesendete Nachrichten zu entschlüsseln. Mehr als hundert Länder, darunter der Iran, Indien und mehrere lateinamerikanische Länder, waren davon betroffen. Dies ist ein Paradebeispiel für das Umgehen von Sicherheitsmechanismen auf einer unteren Systemebene.




TROJANER SCHEINEN ZIEMLICH GEFÄHRLICH ZU SEIN, WENN SIE UNSEREN GUT GESICHERTEN DAMM SCHÄDIGEN KÖNNEN. ICH WILL GAR NICHT AN MEDIZINISCHE GERÄTE, FLUGZEUGE ODER DATENCENTER DENKEN...
VORSICHT!!
DA HAST DU RECHT. SIE SIND ZIEMLICH GEFÄHRLICH UND KÖNNTEN VON MÄCHTIGEN ANGREIFER*INNEN, WIE GEHEIMDIENSTEN, ANGEWENDET WERDEN.

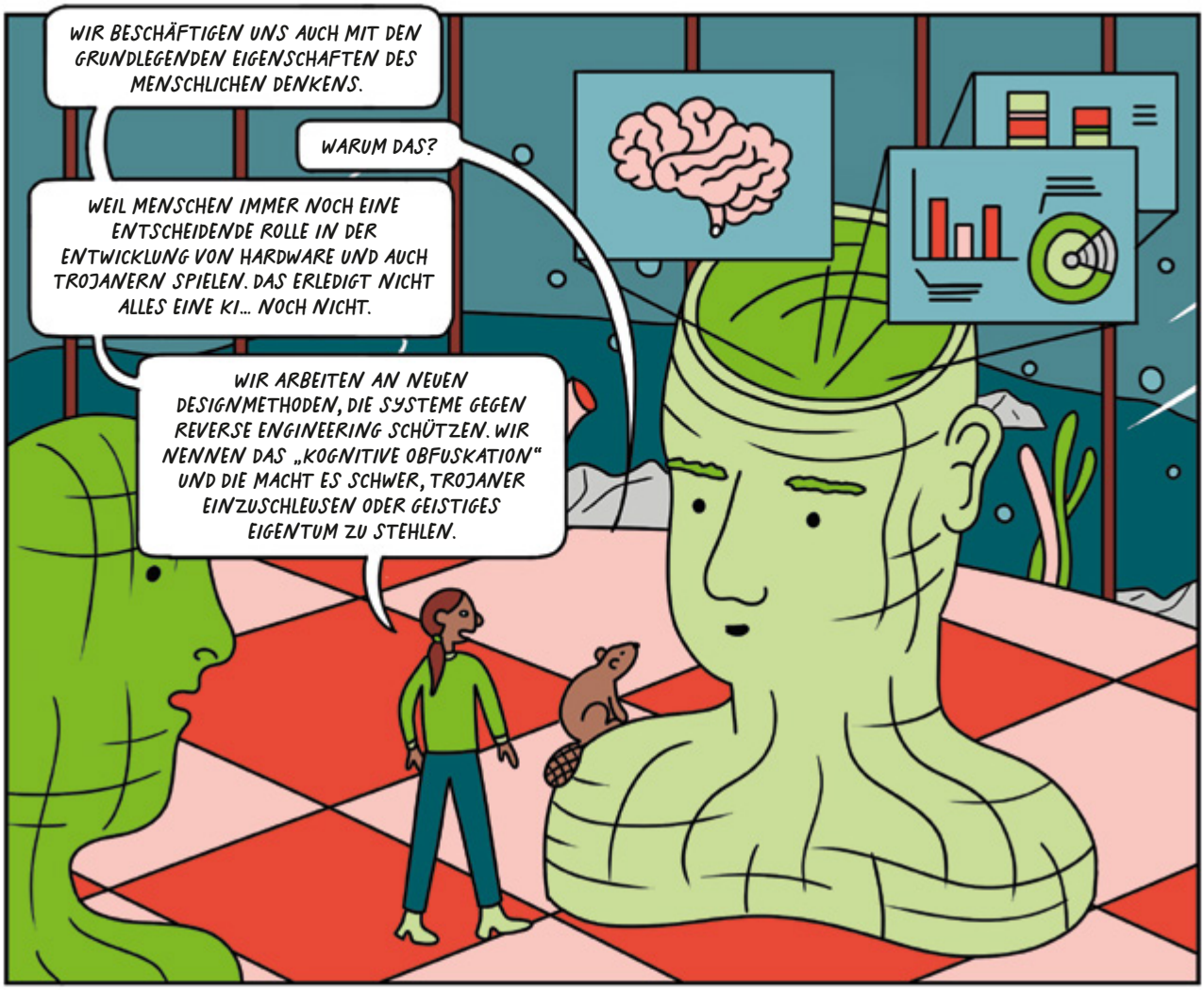

FORSCHUNGSPROJEKT
Manipulation von Mikrochips Aufspüren
OK, DIE SIND WIRKLICH SCHWER ZU ENTDECKEN. ABER WIE MACHT IHR DAS?
EINE WICHTIGE METHODE, DIE UNS BEI DER ERKENNUNG HILFT, IST DAS HARDWARE REVERSE ENGINEERING, BEI DEM WIR MIKROCHIPS AUSEINANDERNEHMEN...
TROJANER AUF CHIP-EBENE KÖNNEN WÄHREND DER HERSTELLUNG EINGEFÜGT WERDEN. UM DIESE WINZIGEN MANIPULATIONEN ZU FINDEN, SCANNEN WIR DEN CHIP MIT EINEM ELEKTRONEN-MIKROSKOP. DIE BILDER WERDEN DANN MIT DEM URSPRÜNGLICHEN BAUPLAN ABGEGLICHEN. UND GLAUBE MIR, ES IST EINE RIESIGE ZAHL AN KOMPONENTEN, DIE WIR PRÜFEN MÜSSEN. WIR SUCHEN DIE NADEL IM HEUHAUFEN.
HAB DICH! DAS SOLLTE NICHT HIER SEIN!
DER JOB SIEHT ANSTRENGEND AUS. BAUT IHR DIE TROJANER AUCH SELBST ZUM TESTEN EIN?


Defenses
JA UND NEIN. WIR ÜBEN DEFINITIV VIEL, WEIL DAS FINDEN SOLCHER WINZIGEN VERÄNDERUNGEN SEHR AUFWENDIG IST. UM DIE ÜBUNG MÖGLICHST REALISTISCH ZU GESTALTEN, TEILEN WIR UNS IN ZWEI KONKURRIERENDE TEAMS AUF: DAS ROTE TEAM VERSTECKT EINEN TROJANER IN DER HARDWARE, WÄHREND DAS BLAUE TEAM VERSUCHT, IHN ZU ENTDECKEN. SO STELLEN WIR EINE UNABHÄNGIGE ERKENNUNG SICHER.
ROT 1 : 2 BLAU
DAS GEFÄLLT MIR SCHON EHER. EIN WENIG WETTBEWERB UND GENUG MATE. DAS IST ALLES, WAS ES BRAUCHT, UM EINE HERAUSFORDERUNG ZU MEISTERN.


MAN MUSS OFT WIE EIN BÖSARTIGER HACKER DENKEN, UM ERFOLGREICHE SICHERHEITSFORSCHUNG ZU BETREIBEN.


ABER ES GIBT AUCH ANDERE MÖGLICHKEITEN, HARDWARE ZU HACKEN. SELBST CHIPS BRAUCHEN AB UND AN EIN UPDATE. BEI CPUS GESCHIEHT DIES DURCH MICROCODE, DER ALS EINE ART SOFTWARE AUF UNTERSTER EBENE ANGESEHEN WERDEN KANN.

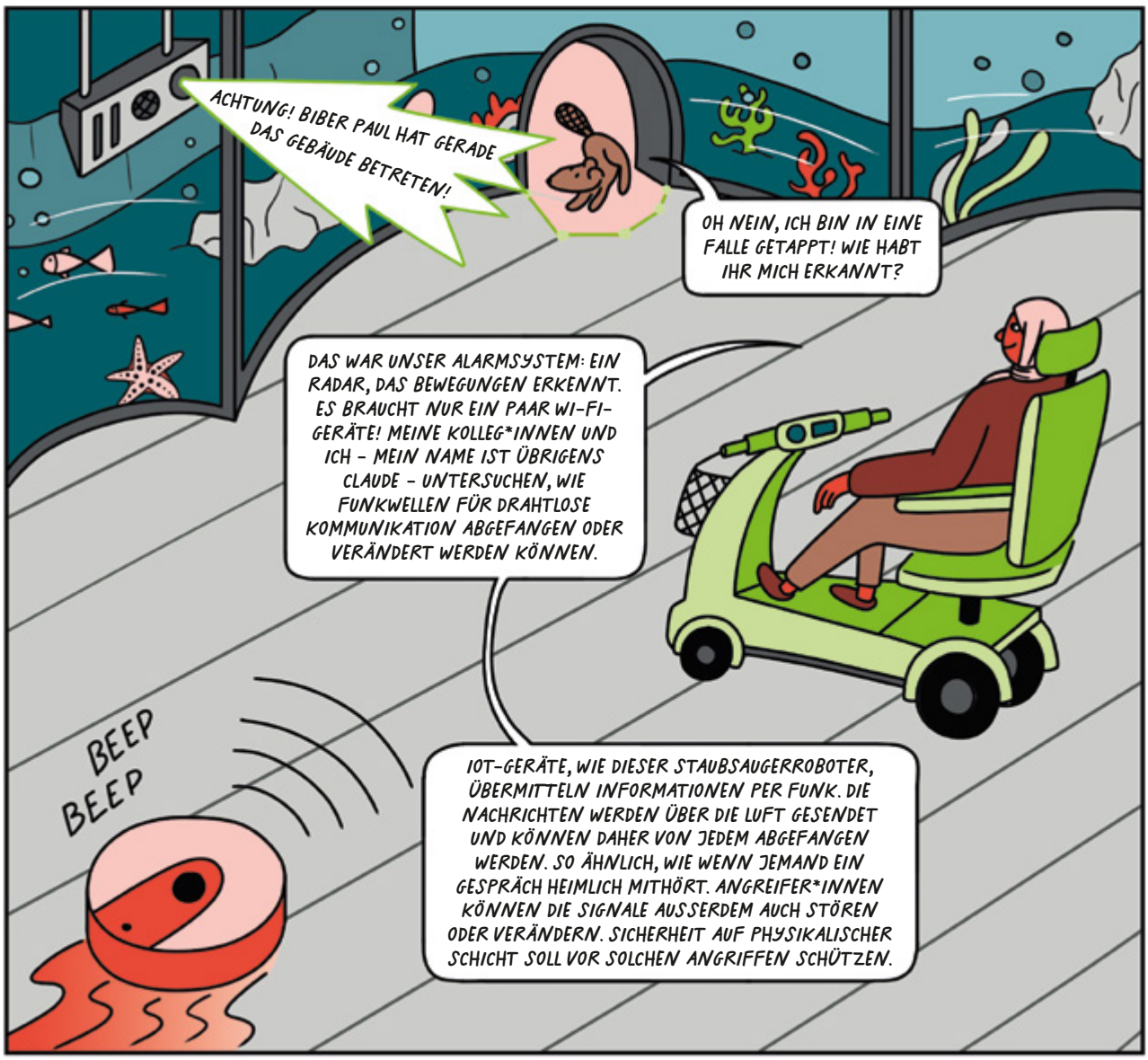

UND CODE IST MÄCHTIG, WIE WIR ALLE WISSEN. ER IST DAS HERZSTÜCK DER CPU. SELBST SICHERHEITSUPDATES KÖNNEN DAZU GENUTZT WERDEN, DIE SENSIBELSTEN BEREICHE EINES COMPUTERS MIT SCHADCODE ZU INFIZIEREN. DU WILLST NICHT, DASS DAS MIT EINEM HERZSCHRITTMACHER PASSIERT, ODER!?!

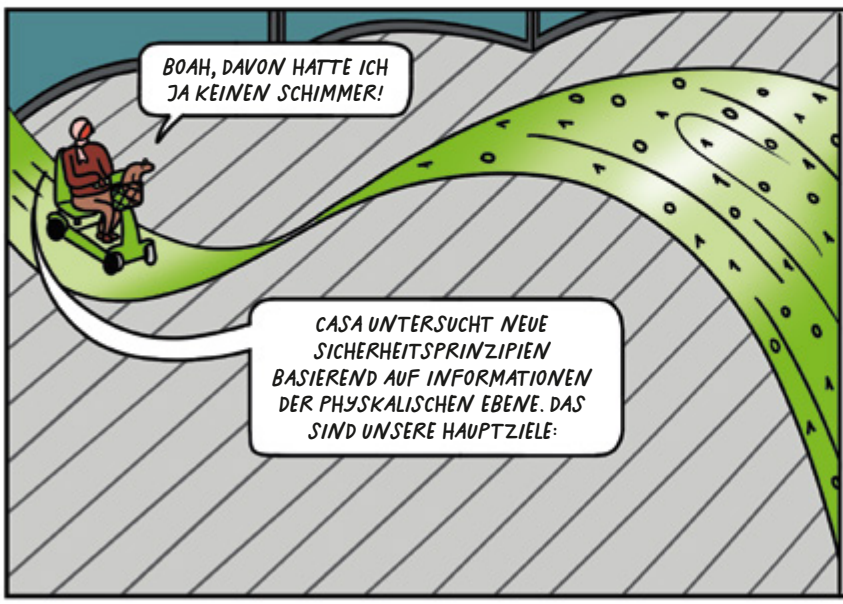

WIR BESCHÄFTIGEN UNS AUCH MIT DEN GRUNDLEGENDEN EIGENSCHAFTEN DES MENSCHLICHEN DENKENS.
WARUM DAS?
WEIL MENSCHEN IMMER NOCH EINE ENTSCHEIDENDE ROLLE IN DER ENTWICKLUNG VON HARDWARE UND AUCH TROJANERN SPIELEN. DAS ERLEDIGT NICHT ALLES EINE KI… NOCH NICHT.
WIR ARBEITEN AN NEUEN DESIGNMETHODEN, DIE SYSTEME GEGEN REVERSE ENGINEERING SCHÜTZEN. WIR NENNEN DAS „KOGNITIVE OBFUSKATION“ UND DIE MACHT ES SCHWER, TROJANER EINZUSCHLEUSEN ODER GEISTIGES EIGENTUM ZU STEHLEN.


GLAUBST DU, DASS EIN HARDWARE-TROJANER UNSEREN DAMM INFILTRIERT HAT?
SCHON MÖGLICH, ABER ES GIBT NOCH MEHR MÖGLICHKEITEN. VIELLEICHT WURDE DAS HOLZ FÜR DEN DAMM DURCH EIN ANDERES MATERIAL ERSETZT, OHNE DASS DU ES BEMERKT HAST. AM BESTEN FRAGST DU UNSERE KOLLEG*INNEN, DIE SICH MIT DER SICHERHEIT AUF PHYSIKALISCHER EBENE BEFASSEN. SIE SUCHEN NACH LÖSUNGEN, UM SOLCHE MANIPULATIONEN ZU ERKENNEN.
DANKE VIELMALS! ICH HAB ECHT VIEL GELERNT!
ÜBRIGENS: WIR NENNEN IHR GEBÄUDE DIE SCHATZKAMMER. DU WIRST SICHER HERAUSFINDEN, WESHALB.

PHYSICAL-LAYER SICHERHEIT

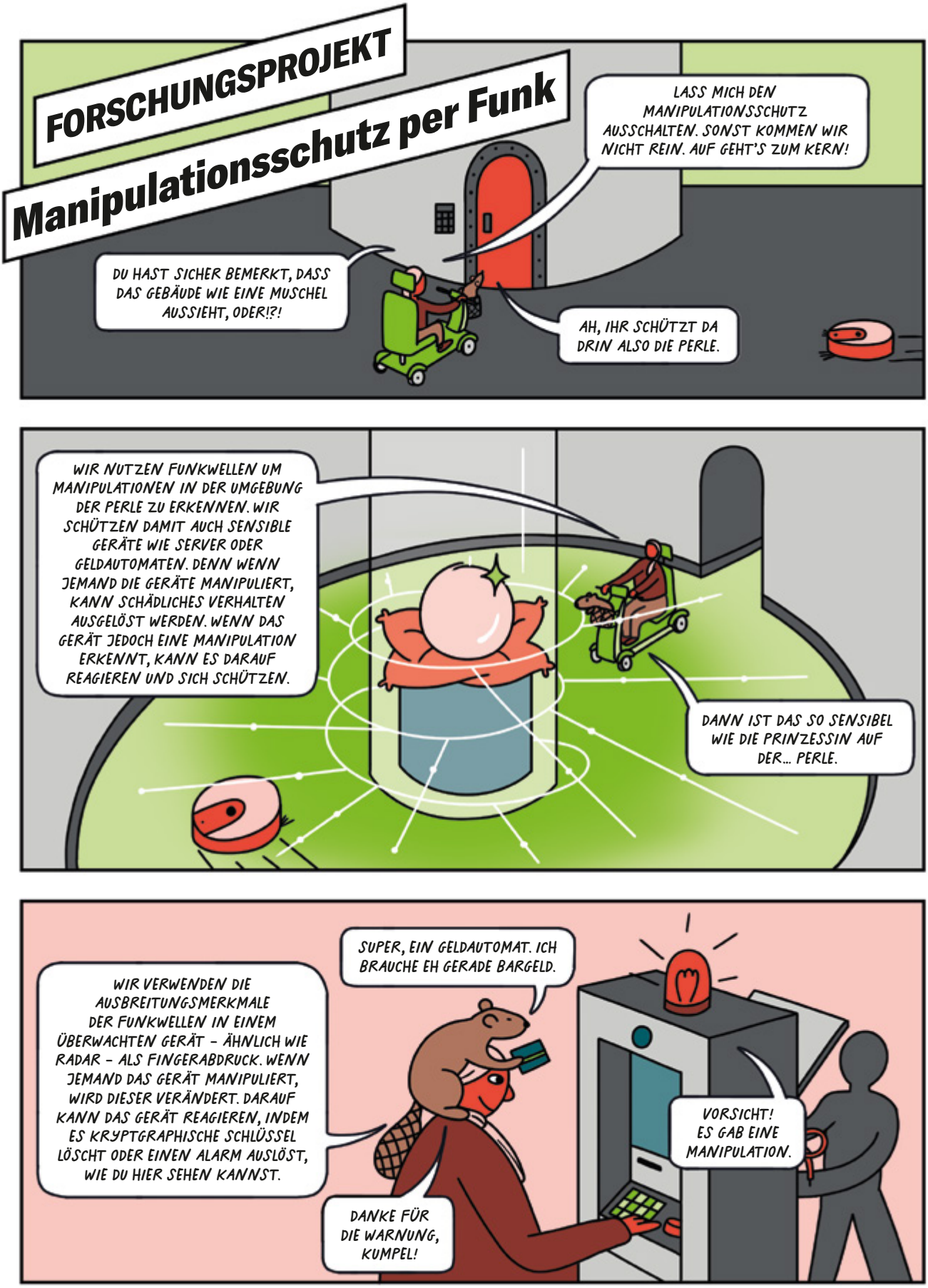
CHALLENGE 5





FORSCHUNGSZIELE

1. Erforschung neuer Techniken für sichere Kommunikationskanäle
2. Gestaltung und Entwicklung sicherer Funk-Systeme
3. Entwicklung drahtloser Sensorsysteme zur Überwachung der physischen Integrität von Computersystemen
4. Untersuchung der Aspekte der Privatsphäre von drahtlosen Sensorsystemen


FORSCHUNGSPROJEKT
Manipulationsschutz per Funk
DU HAST SICHER BEMERKT, DASS DAS GEBÄUDE WIE EINE MUSCHEL AUSSIEHT, ODER!?!
LASS MICH DEN MANIPULATIONSSCHUTZ AUSSCHALTEN. SONST KOMMEN WIR NICHT REIN. AUF GEHT'S ZUM KERN!
AH, IHR SCHÜTZT DA DRIN ALSO DIE PERLE.
WIR NUTZEN FUNKWELLEN UM MANIPULATIONEN IN DER UMGEBUNG DER PERLE ZU ERKENNEN. WIR SCHÜTZEN DAMIT AUCH SENSIBLE GERÄTE WIE SERVER ODER GELDAUTOMATEN. DENN WENN JEMAND DIE GERÄTE MANIPULIERT, KANN SCHÄDLICHES VERHALTEN AUSGELÖST WERDEN. WENN DAS GERÄT JEDOCH EINE MANIPULATION ERKENNT, KANN ES DARAUF REAGIEREN UND SICH SCHÜTZEN.
DANN IST DAS SO SENSIBEL WIE DIE PRINZESSIN AUF DER... PERLE.
WIR VERWENDEN DIE AUSBREITUNGSMERKMALE DER FUNKWELLEN IN EINEM ÜBERWACHTEN GERÄT – ÄHNLICH WIE RADAR – ALS FINGERABDRUCK. WENN JEMAND DAS GERÄT MANIPULIERT, WIRD DIESER VERÄNDERT. DARAUF KANN DAS GERÄT REAGIEREN, INDEM ES KRYPTGRAPHISCHE SCHLÜSSEL LÖSCHT ODER EINEN ALARM AUSLÖST, WIE DU HIER SEHEN KANNST.
SUPER, EIN GELDAUTOMAT. ICH BRAUCHE EH GERADE BARGELD.
VORSICHT! ES GAB EINE MANIPULATION.
DANKE FÜR DIE WARNUNG, KUMPEL!

CASA WIKI

Bei der **drahtlosen Sensorik** werden Informationen über die physische Umgebung aus gewöhnlichen drahtlosen Kommunikationssignalen abgeleitet (ähnlich wie beim Radar).

Der **Funkkanal** ist die Kombination aller physikalischen Effekte eines drahtlosen Signals auf dem Weg von einem Sender zu einem Empfänger. Hier eine Analogie aus dem akustischen Bereich: Wenn eine Person spricht, kann eine zweite Person diese hören, aber gedämpft (weniger laut) und mit zusätzlichem Hall aus dem Raum (aufgrund von Reflektionen). Der drahtlose Kanal ist wie ein Fingerabdruck der physikalischen Umgebung.

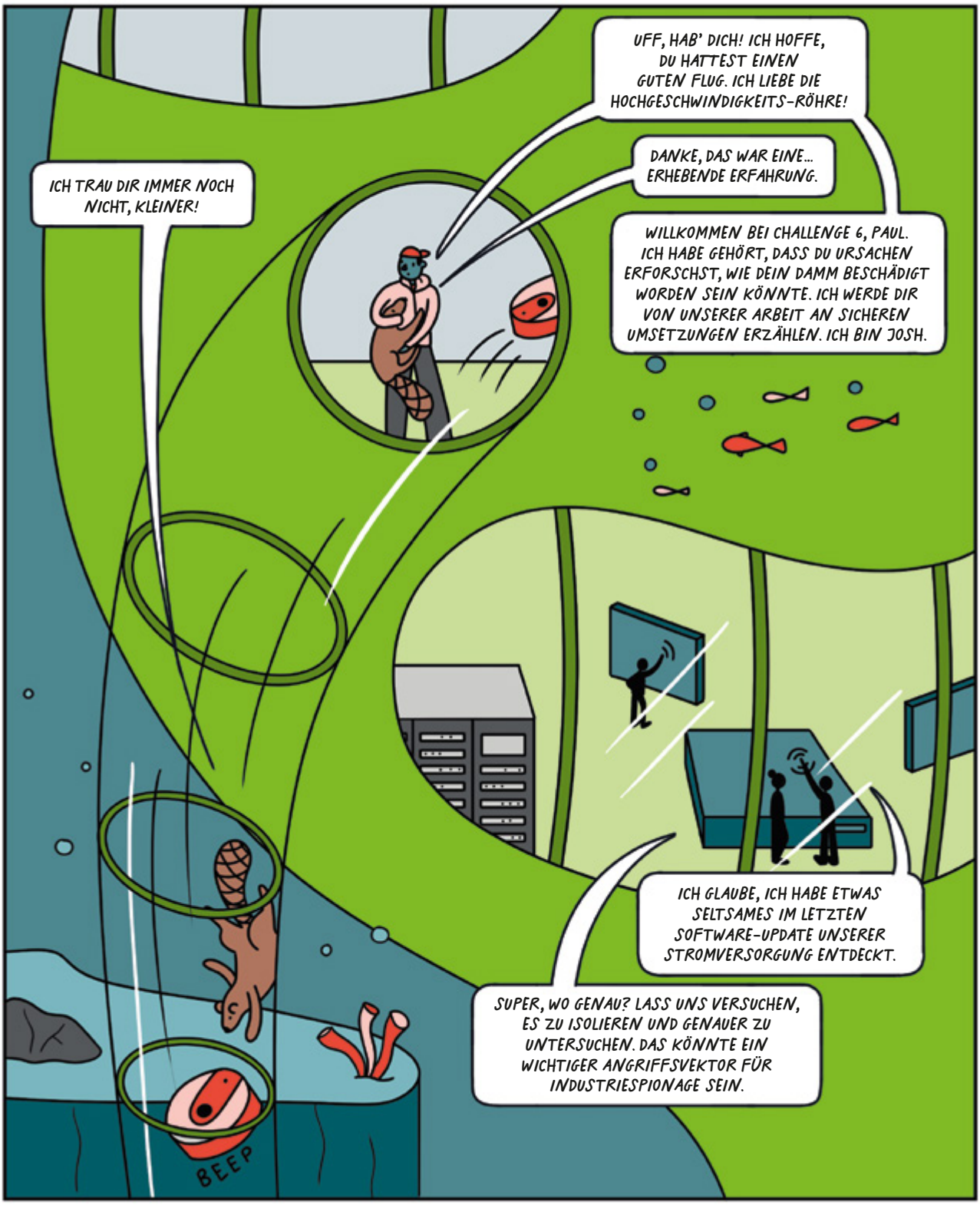
Die **Manipulationserkennung** beschreibt die Verarbeitung einiger Sensordaten (z. B. durch die Beobachtung von Funkkanälen), um unbefugte physikalische Veränderungen einer Umgebung zu erkennen, die möglicherweise auf einen physikalischen Angriff hindeuten.

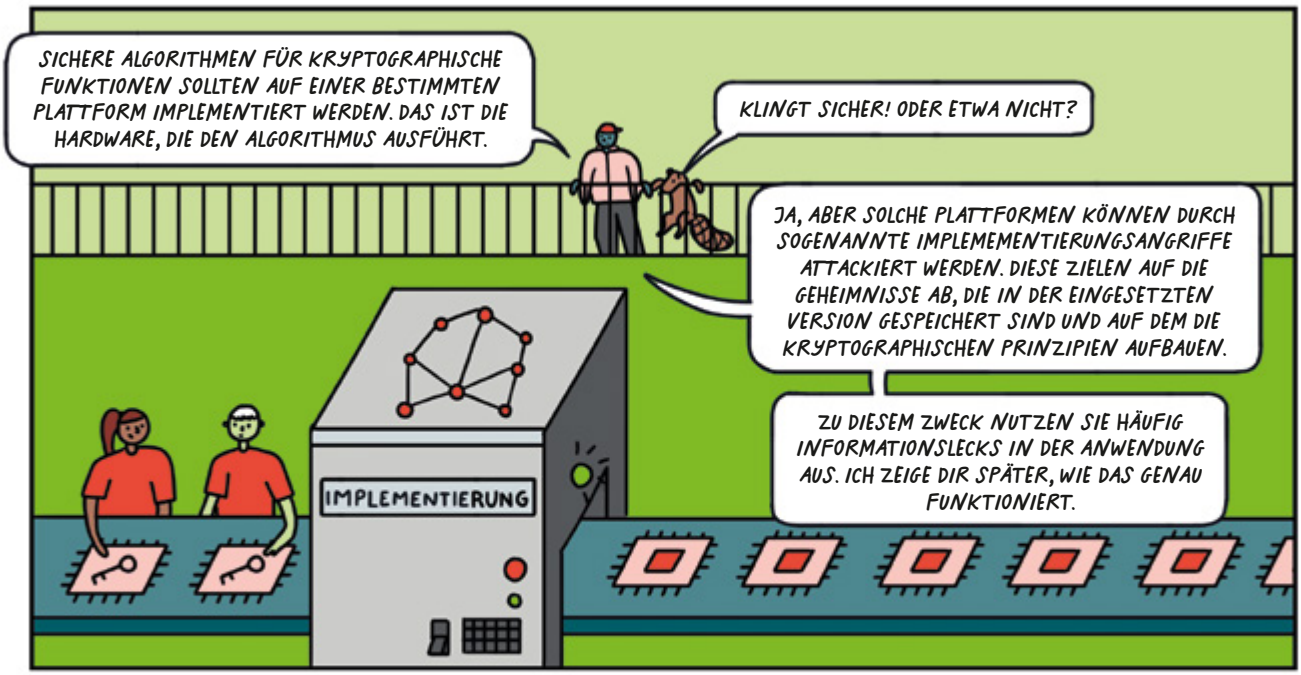
Intelligente reflektierende Oberflächen sind digital konfigurierbare Reflektoren für Funkwellen, die zur Veränderung von Funksignalen verwendet werden können. Diese Technologie wird wahrscheinlich in künftige drahtlose 6G-Kommunikationssysteme integriert werden.

Bei der **Erkennung menschlicher Bewegungen** werden drahtlose Sensoren eingesetzt, um die Anwesenheit von Personen zu identifizieren, wobei möglicherweise deren Privatsphäre verletzt wird. Zu den fortgeschritteneren Anwendungen der drahtlosen Sensorik gehören außerdem die Erkennung von Aktivitäten und Gesten sowie die Überwachung von Vitaldaten.

WEITERENTWICKLUNG SICHERER IMPLEMENTIERUNGEN

CHALLENGE 6



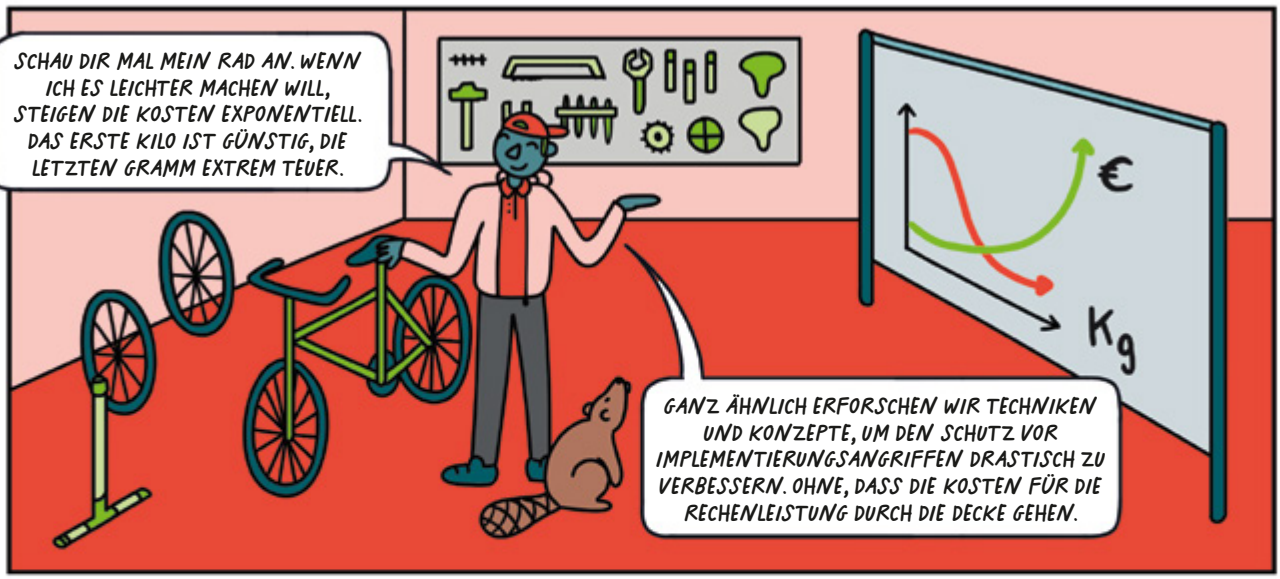


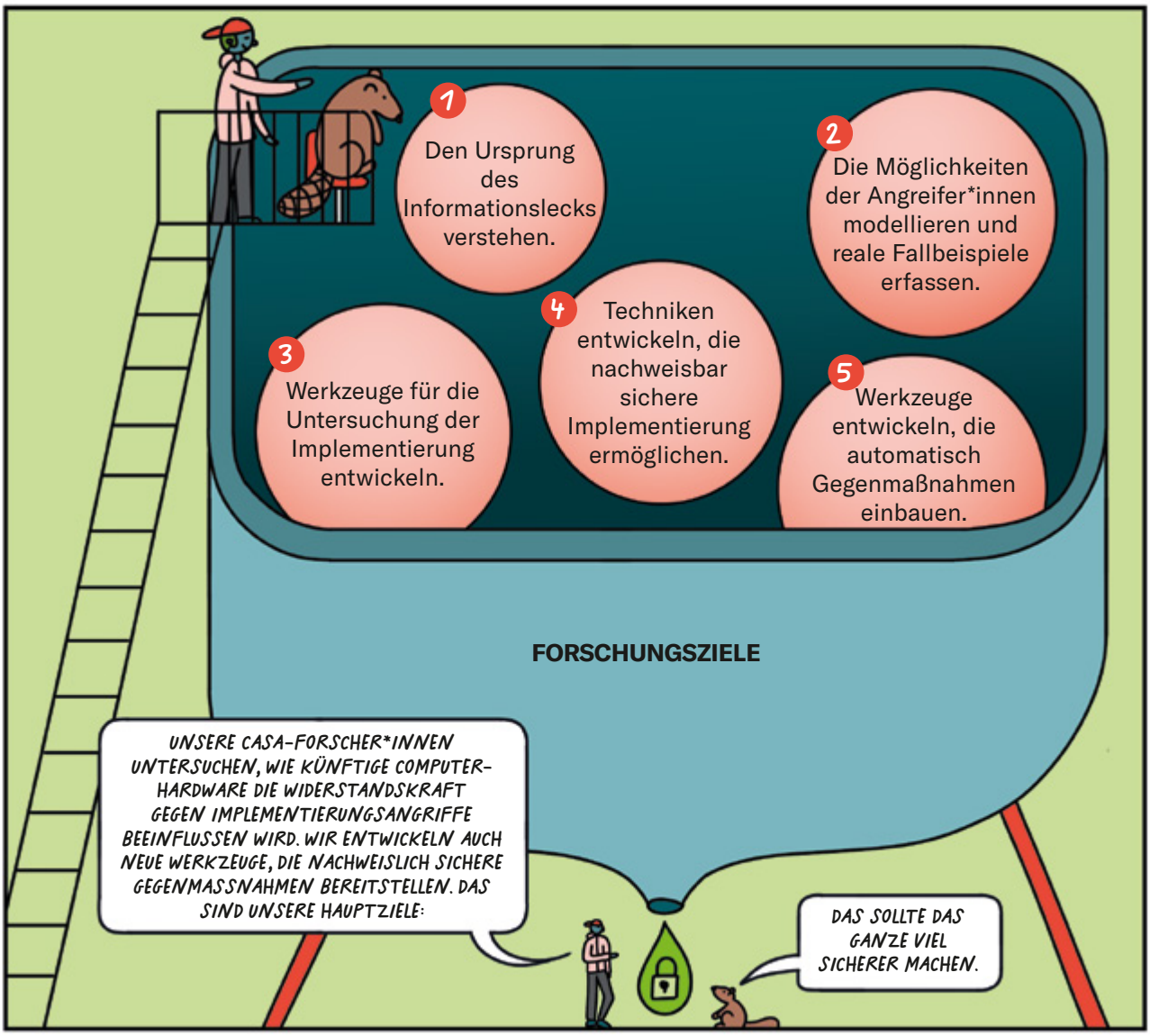
CASA WIKI

Kryptographische Primitive sind mathematische Algorithmen, die als grundlegende Bausteine in Sicherheitsprotokollen dienen. Sie sorgen dafür, dass geschützte Daten weder gelesen noch manipuliert werden können und dass sie tatsächlich vom angegebenen Absender stammen.

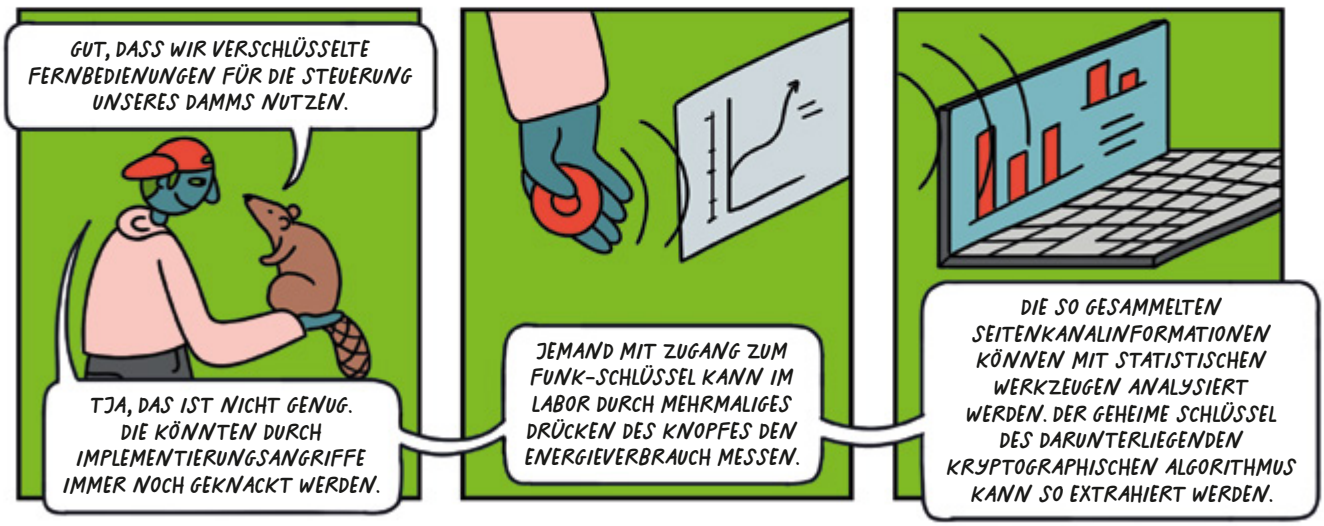
Eine **Implementierung** ist eine Umsetzung eines Algorithmus in Form eines Programms (Software) oder eines elektronischen Geräts (Hardware). Bei Implementierungsangriffen wird daher versucht, die Umsetzung des kryptographischen Algorithmus zu knacken und nicht die Kryptographie selbst.

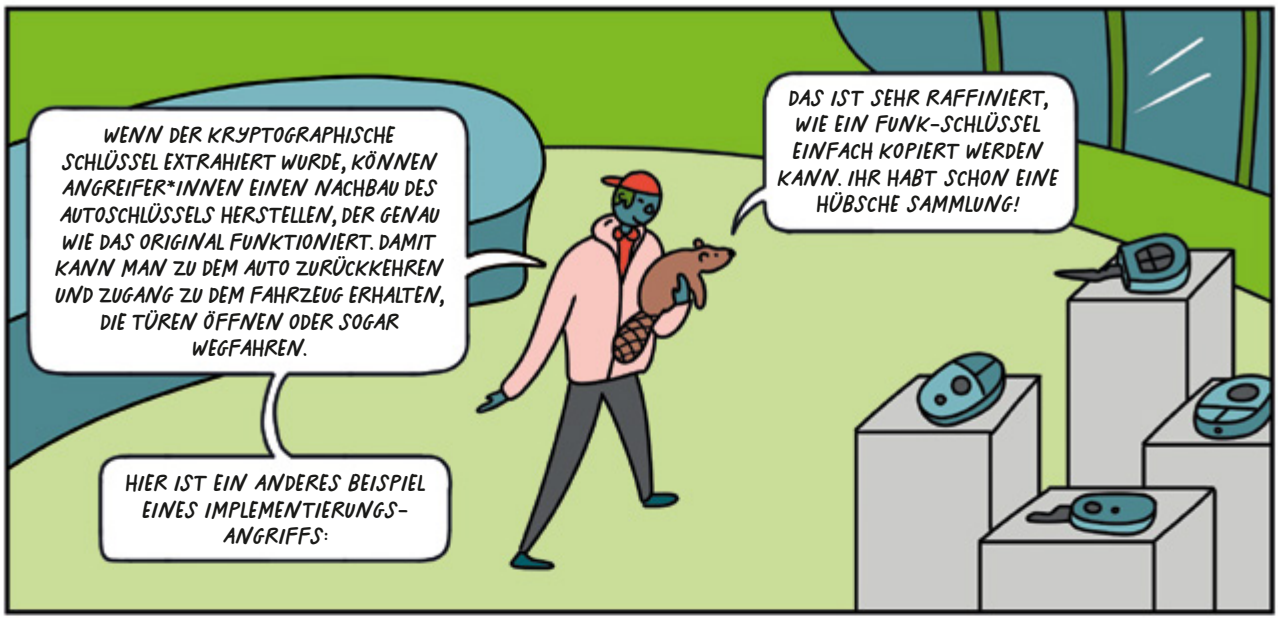
Die **Seitenkanalanalyse** nutzt unbeabsichtigte physikalische Eigenschaften (z. B. Stromverbrauch, elektromagnetische Strahlung oder Reaktionszeit) eines elektronischen Geräts aus.


SCHAU DIR MAL MEIN RAD AN. WENN ICH ES LEICHTER MACHEN WILL, STEIGEN DIE KOSTEN EXPONENTIELL. DAS ERSTE KILO IST GÜNSTIG, DIE LETZTEN GRAMM EXTREM TEUER.
€
Kg
GANZ ÄHNLICH ERFORSCHEN WIR TECHNIKEN UND KONZEPTE, UM DEN SCHUTZ VOR IMPLEMENTIERUNGSANGRIFFEN DRASTISCH ZU VERBESSERN. OHNE, DASS DIE KOSTEN FÜR DIE RECHENLEISTUNG DURCH DIE DECKE GEHEN.


1
Den Ursprung des Informationslecks verstehen.
2
Die Möglichkeiten der Angreifer*innen modellieren und reale Fallbeispiele erfassen.
3
Werkzeuge für die Untersuchung der Implementierung entwickeln.
4
Techniken entwickeln, die nachweisbar sichere Implementierung ermöglichen.
5
Werkzeuge entwickeln, die automatisch Gegenmaßnahmen einbauen.
FORSCHUNGSZIELE
UNSERE CASA-FORSCHER*INNEN UNTERSUCHEN, WIE KÜNFTIGE COMPUTER-HARDWARE DIE WIDERSTANDSKRAFT GEGEN IMPLEMENTIERUNGSANGRIFFE BEEINFLUSSEN WIRD. WIR ENTWICKELN AUCH NEUE WERKZEUGE, DIE NACHWEISLICH SICHERE GEGENMASSNAHMEN BEREITSTELLEN. DAS SIND UNSERE HAUPTZIELE:
DAS SOLLTE DAS GANZE VIEL SICHERER MACHEN.

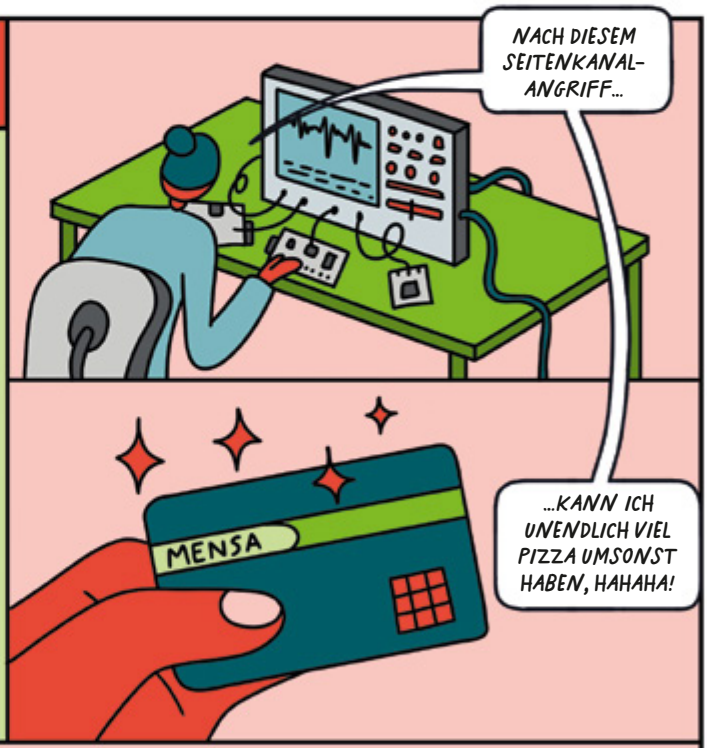
FORSCHUNGSPROJEKT
Funk-Autoschlüssel

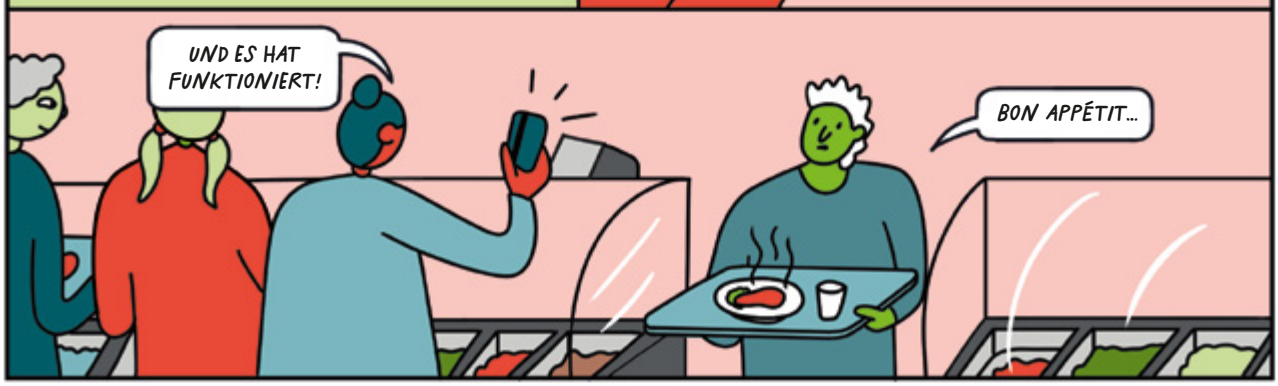


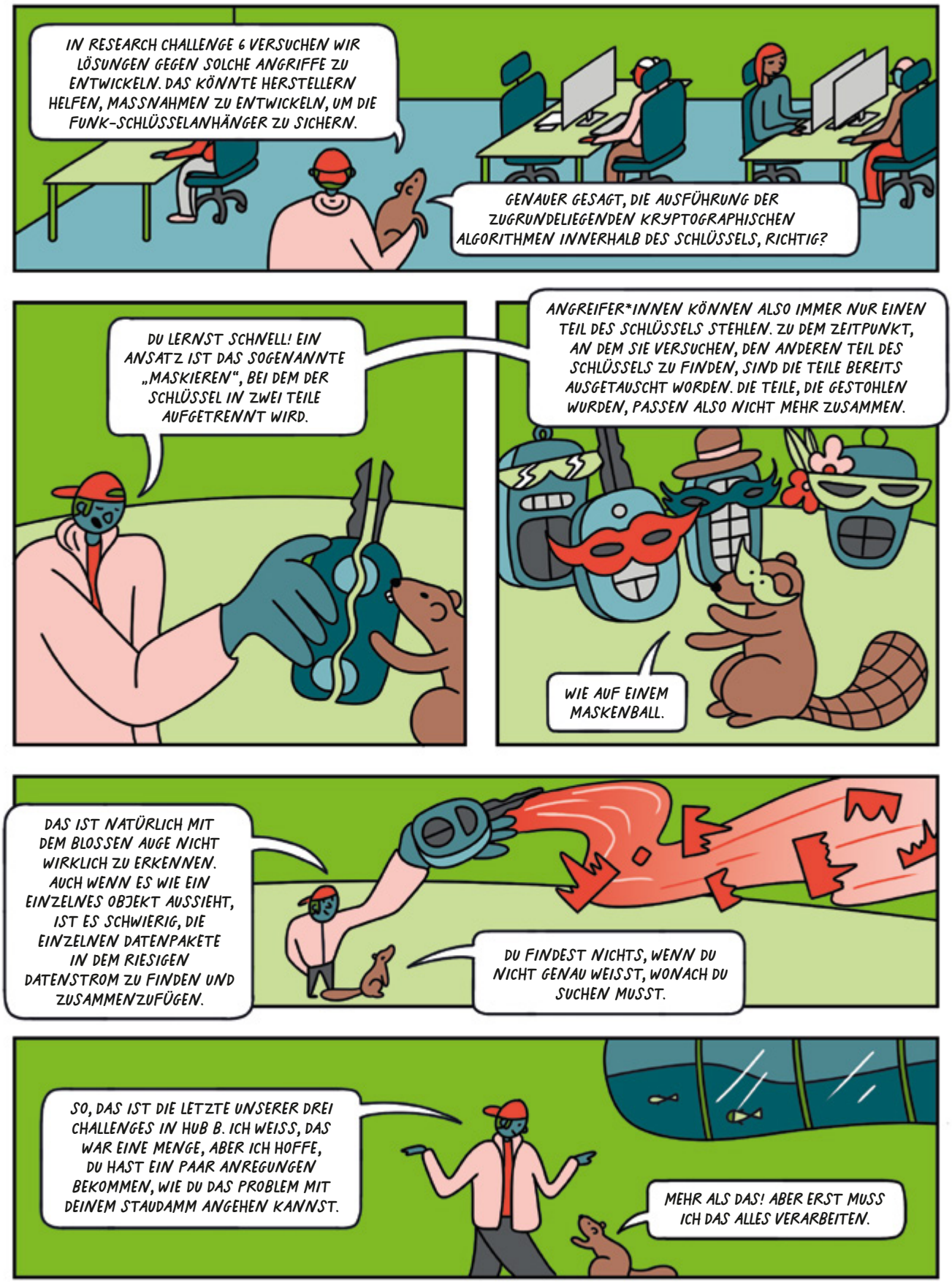


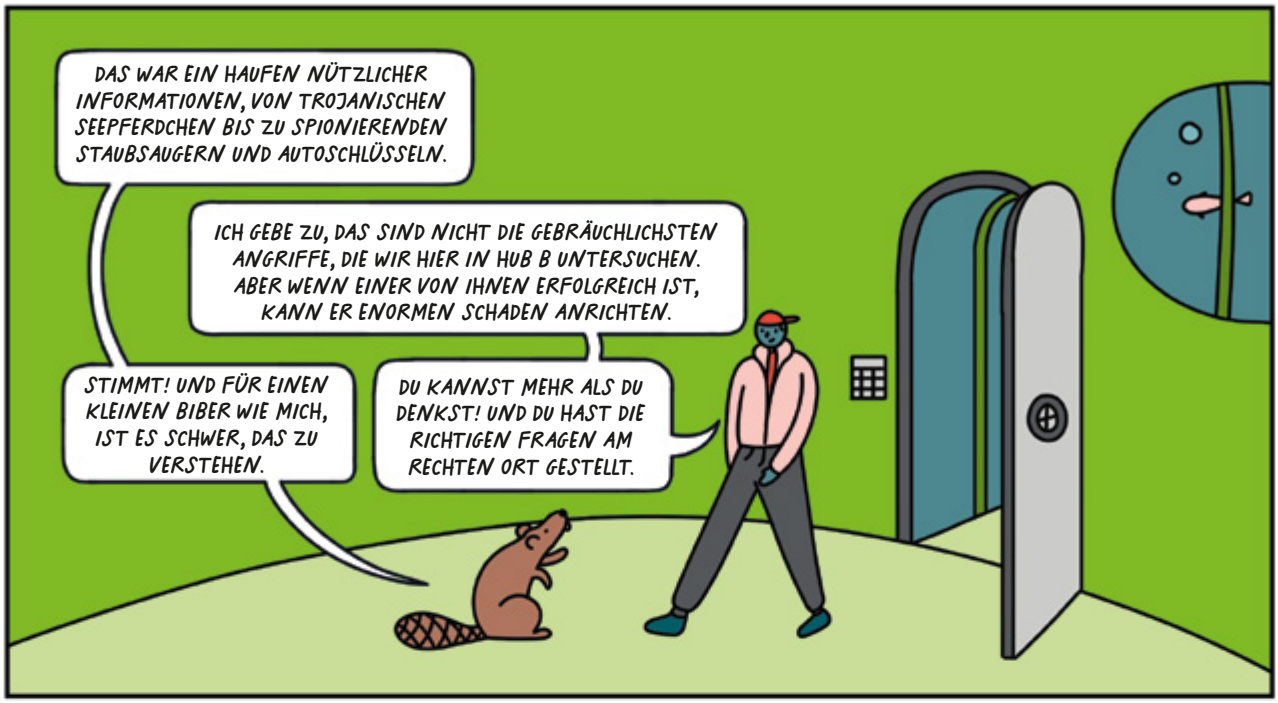
REAL LIFE STORY

In einem Experiment gelang es Forscher*innen der Ruhr-Universität Bochum, die Mensakarten der Uni zu manipulieren und Daten auszulesen. Sie untersuchten den verwendeten Chip und stellten durch Messung der elektromagnetischen Abstrahlung beim kontaktlosen Bezahlen fest, dass alle Karten denselben geheimen Schlüssel nutzten. Dadurch war es leicht, die gespeicherten Informationen zu entschlüsseln und das Guthaben in Sekundenbruchteilen zu ändern. Fehlende Sicherheitsmaßnahmen im Backend ermöglichten es schließlich, mit den manipulierten Karten problemlos zu bezahlen.






IN RESEARCH CHALLENGE 6 VERSUCHEN WIR LÖSUNGEN GEGEN SOLCHE ANGRIFFE ZU ENTWICKELN. DAS KÖNNTE HERSTELLERN HELFEN, MASSNAHMEN ZU ENTWICKELN, UM DIE FUNK-SCHLÜSSELANHÄNGER ZU SICHERN.
GENAUER GESAGT, DIE AUSFÜHRUNG DER ZUGRUNDELIEGENDEN KRYPTOGRAPHISCHEN ALGORITHMEN INNERHALB DES SCHLÜSSELS, RICHTIG?
DU LERNST SCHNELL! EIN ANSATZ IST DAS SOGENANNTE „MASKIEREN“, BEI DEM DER SCHLÜSSEL IN ZWEI TEILE AUFGETRENNT WIRD.
ANGREIFER*INNEN KÖNNEN ALSO IMMER NUR EINEN TEIL DES SCHLÜSSELS STEHLEN. ZU DEM ZEITPUNKT, AN DEM SIE VERSUCHEN, DEN ANDEREN TEIL DES SCHLÜSSELS ZU FINDEN, SIND DIE TEILE BEREITS AUSGETAUSCHT WORDEN. DIE TEILE, DIE GESTOHLEN WURDEN, PASSEN ALSO NICHT MEHR ZUSAMMEN.
WIE AUF EINEM MASKENBALL.
DAS IST NATÜRLICH MIT DEM BLOSSEN AUGE NICHT WIRKLICH ZU ERKENNEN. AUCH WENN ES WIE EIN EINZELNES OBJEKT AUSSIEHT, IST ES SCHWIERIG, DIE EINZELNEN DATENPAKETE IN DEM RIESIGEN DATENSTROM ZU FINDEN UND ZUSAMMENZUFÜGEN.
DU FINDEST NICHTS, WENN DU NICHT GENAU WEISST, WONACH DU SUCHEN MUSST.
SO, DAS IST DIE LETZTE UNSERER DREI CHALLENGES IN HUB B. ICH WEISS, DAS WAR EINE MENGE, ABER ICH HOFFE, DU HAST EIN PAAR ANREGUNGEN BEKOMMEN, WIE DU DAS PROBLEM MIT DEINEM STAUDAMM ANGEHEN KANNST.
MEHR ALS DAS! ABER ERST MUSS ICH DAS ALLES VERARBEITEN.


DAS WAR EIN HAUFEN NÜTZLICHER INFORMATIONEN, VON TROJANISCHEN SEEPFERDCHEN BIS ZU SPIONIERENDEN STAUBSAUGERN UND AUTOSCHLÜSSELN.
ICH GEBE ZU, DAS SIND NICHT DIE GEBRÄUCHLICHSTEN ANGRIFFE, DIE WIR HIER IN HUB B UNTERSUCHEN. ABER WENN EINER VON IHNEN ERFOLGREICH IST, KANN ER ENORMEN SCHADEN ANRICHTEN.
STIMMT! UND FÜR EINEN KLEINEN BIBER WIE MICH, IST ES SCHWER, DAS ZU VERSTEHEN.
DU KANNST MEHR ALS DU DENKST! UND DU HAST DIE RICHTIGEN FRAGEN AM RECHTEN ORT GESTELLT.


OH MANN! ICH HAB VIEL ZU TUN, WENN ICH NACH HAUSE KOMME. SO VIELE SCHLUPFLÖCHER ZU STOPFEN.


ABER WARUM SOLLTEN MÄCHTIGE ANGREIFER*INNEN UNSEREN KLEINEN DAMM INS VISIER NEHMEN? VIELLEICHT NUR EIN MISSVERSTÄNDNIS?


HEY, DU FAULPELZ! WIR HABEN EIN ERNSTES PROBLEM UND DU SCHMÖKERST IN DER NEUESTEN ZEITSCHRIFT?
ES IST DIE SONDERAUSGABE DES WISSENSCHAFTSMAGAZINS RUBIN ZU IT-SICHERHEIT!
UND DER STAUDAMM?


EIN PAAR SKRIPT-KIDDIES HABEN MIT DER HARDWARE HERUMGESPIELT. NACHDEM SIE DEN ANGERICHTETEN SCHADEN BEMERKT HABEN, HABEN SIE MICH INS VERTRAUEN GEZOGEN. VIEL LÄRM UM (FAST) NICHTS.
NAJA, WENIGSTENS KÖNNEN WIR UNS JETZT GEGEN ZUKÜNFTIGE ERNSTHAFTE ANGRIFFE WAPPNEN...

ÜBER CASA

CASA: Cyber Security in the Age of Large-Scale Adversaries wurde 2019 gegründet und ist das einzige Exzellenzcluster im Bereich IT-Sicherheit in Deutschland. Von der Deutschen Forschungsgemeinschaft (DFG) wird CASA mit 30 Millionen Euro über sieben Jahre hinweg gefördert, um ausgezeichnete Forschungsbedingungen zu garantieren.
Bei CASA arbeitet eine Kerngruppe führender Forscher*innen mit einem klaren Fokus auf Sicherheit und Datenschutz eng mit ausgewählten Spitzenforscher*innen aus hochrelevanten Nachbardisziplinen zusammen. Dabei deckt das Team sämtliche Disziplinen ab, die erforderlich sind, um die anspruchsvollen Forschungsprobleme im Bereich der modernen IT-Sicherheit zu bewältigen, darunter Informatik, Mathematik, Elektrotechnik und Psychologie.

CASA ist am Horst-Görtz-Institut für IT-Sicherheit (hgi.rub.de) angesiedelt, einem wegweisenden Forschungsinstitut in Deutschland. Außerdem arbeitet CASA eng mit dem Max-Planck-Institut für Sicherheit und Privatsphäre in Bochum (mpi-sp.org) und zahlreichen weiteren Instituten und Universitäten zusammen.

Was ist ein „Exzellenzcluster“?
Mit der Förderlinie „Exzellenzcluster“ werden international wettbewerbsfähige Forschungszentren an Universitäten oder Universitätsverbünden in Deutschland projektbezogen für einen Zeitraum von sieben Jahren gefördert. Innerhalb dieser Cluster arbeiten Wissenschaftler*innen aus verschiedenen Disziplinen und Institutionen gemeinsam an einem Forschungsprojekt. Die Förderung ermöglicht es ihnen, sich intensiv auf ihr Forschungsziel zu konzentrieren, wissenschaftlichen Nachwuchs auszubilden und internationale Spitzenforscher*innen zu gewinnen.

casa.rub.de

TECHNISCHER BACKGROUND

Die in diesem Comic vorgestellten Konzepte und Methoden wurden von den am Exzellenzcluster CASA mitwirkenden Forscher*innen entwickelt. Die Originalveröffentlichungen sind online verfügbar und geben detaillierte Einblicke in ihre Forschung. Zusätzlich veröffentlichen wir zu vielen Publikationen den Quellcode und weitere Forschungsergebnisse. Bei Fragen stehen wir gerne zur Verfügung: info@casa.rub.de

PUBLIKATIONEN

Nils Albartus, Clemens Nasenberg, Florian Stolz, Marc Fyrbiak, Christof Paar, Russell Tessier, **On the Design and Misuse of Microcoded (Embedded) Processors — A Cautionary Note**, USENIX: Usenix Security Symposium, 2021.

Endres Puschner, Thorben Moos, Steffen Becker, Christian Kison, Amir Moradi, Christof Paar, **Red Team vs. Blue Team: A Real-World Hardware Trojan Detection Case Study Across Four Modern CMOS Technology Generations**, IEEE Symposium on Security and Privacy (SP), 2023.

Paul Staat, Simon Mulzer, Stefan Roth, Veelasha Moonsamy, Markus Heinrichs, Rainer Kronberger, Aydin Sezgin, Christof Paar, **IRShield: A Countermeasure Against Adversarial Physical-Layer Wireless Sensing**, IEEE Symposium on Security and Privacy (SP), 2022.

Paul Staat, Johannes Tobisch, Christian Zenger, Christof Paar, **Anti-Tamper Radio: System-Level Tamper Detection for Computing Systems**, IEEE Symposium on Security and Privacy (SP), 2022.

David Knichel, Amir Moradi, Nicolai Müller, Pascal Sasdrich, **Automated Generation of Masked Hardware**, IACR Transactions on Cryptographic Hardware and Embedded Systems, 2022(1), pp. 589–629.

David Knichel, Pascal Sasdrich, Amir Moradi, **SILVER — Statistical Independence and Leakage Verification**, In: Advances in Cryptology – ASIACRYPT 2020. Lecture Notes in Computer Science, Vol. 12491, Springer.

CASA HUB B

1. Auflage 2024

Redaktion
Annika Gödde (CASA/Ruhr-Universität Bochum)
Niels Jansen (Ellery Studio)
Christof Paar (CASA/Max-Planck-Institut für Sicherheit und Privatsphäre)
Nils Albartus (Max-Planck-Institut für Sicherheit und Privatsphäre)
Steffen Becker (CASA/Ruhr-Universität Bochum)
Julian Speith (Max-Planck-Institut für Sicherheit und Privatsphäre)
Veelasha Moonsamy (CASA/Ruhr-Universität Bochum)
Stefan Roth (CASA/Ruhr-Universität Bochum)
Aydin Sezgin (CASA/Ruhr-Universität Bochum)
Paul Staat (Max-Planck-Institut für Sicherheit und Privatsphäre)
Johannes Tobisch (Max-Planck-Institut für Sicherheit und Privatsphäre)
Tim Güneysu (CASA/Ruhr-Universität Bochum)
Amir Moradi (CASA/Ruhr-Universität Bochum)
Pascal Sasdrich (CASA/Ruhr-Universität Bochum)

Ellery Studio
Illustration: Lucia Cordero, Hannah Schrage
Design: Dorota Orlof
Projektmanagement: Pawel Leyk

Umschlaggestaltung
Hannah Schrage

Druck
Schmidt, Ley + Wiegandt GmbH + Co. KG, Lünen, www.slw-medien.de

Herausgeber
CASA: Cyber Security in the Age of Large-Scale Adversaries
Universitätsstraße 150
44780 Bochum

hgi-presse@rub.de
casa.rub.de

Scan den QR-Code, um zur digitalen Version dieses Comics und zu den Comics (Englisch/Deutsch) der anderen Research HUBs zu gelangen:

Auf Englisch sind folgende Comics erschienen:

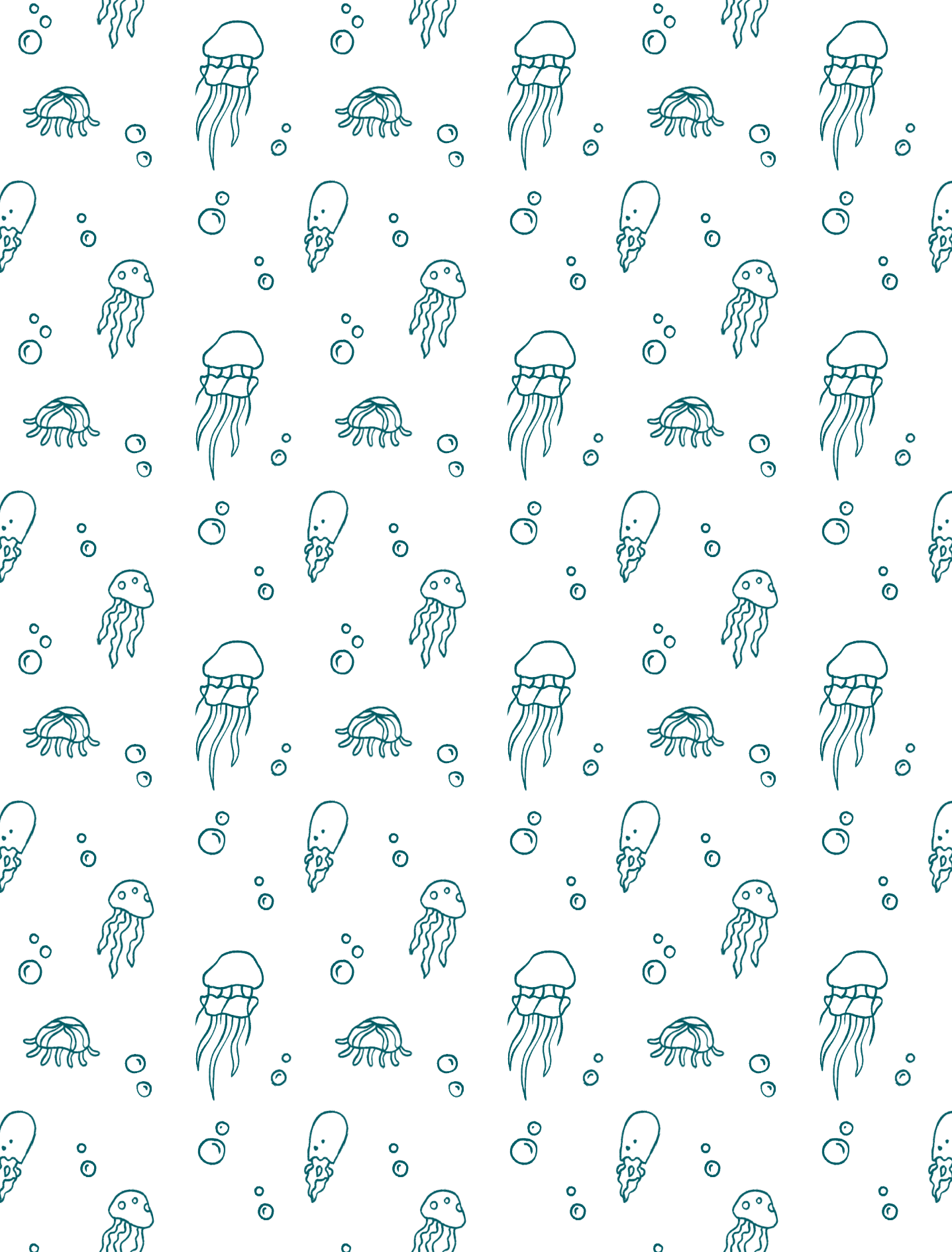
- The Secrets of HUB A and the Traces of the Cookies
- A Deep Dive Into HUB B and the Swirl of Embedded Security
- What's the Fuzz About HUB C and the Missing Carrots?
- HUB D and the Rumble in the Jungle of Usability

CASA
Cyber Security in the Age of Large-Scale Adversaries

Gefördert durch
DFG Deutsche Forschungsgemeinschaft

RUHR UNIVERSITÄT BOCHUM
RUB

ellery studio



EGAL OB HARDWARE-TROJANER ODER SEITENKANALANGRIFFE – AUCH HARDWARE KANN DAS ZIEL VON ANGRIFFEN WERDEN. WENN GERÄTE IN DIE HÄNDE MÖGLICHER BÖSWILLIGER NUTZER*INNEN GELANGEN, ERGEBEN SICH ZAHLREICHE MÖGLICHKEITEN, IN SOLCHE VERMEINTLICH SICHEREN SYSTEME EINZUDRINGEN.

FOLGE DEM FURCHTLOSEN BIBER PAUL AUF SEINEM TAUCHGANG IN DIE FORSCHUNGSWELT VON CASAS HUB B. WIRD ER DAS GEHEIMNIS DES BESCHÄDIGTEN DAMMS SEINER FAMILIE LÖSEN? SIND SIE ZUR ZIELSCHEIBE MÄCHTIGER ANGREIFER*INNEN GEWORDEN?

FINDE ES HERAUS!