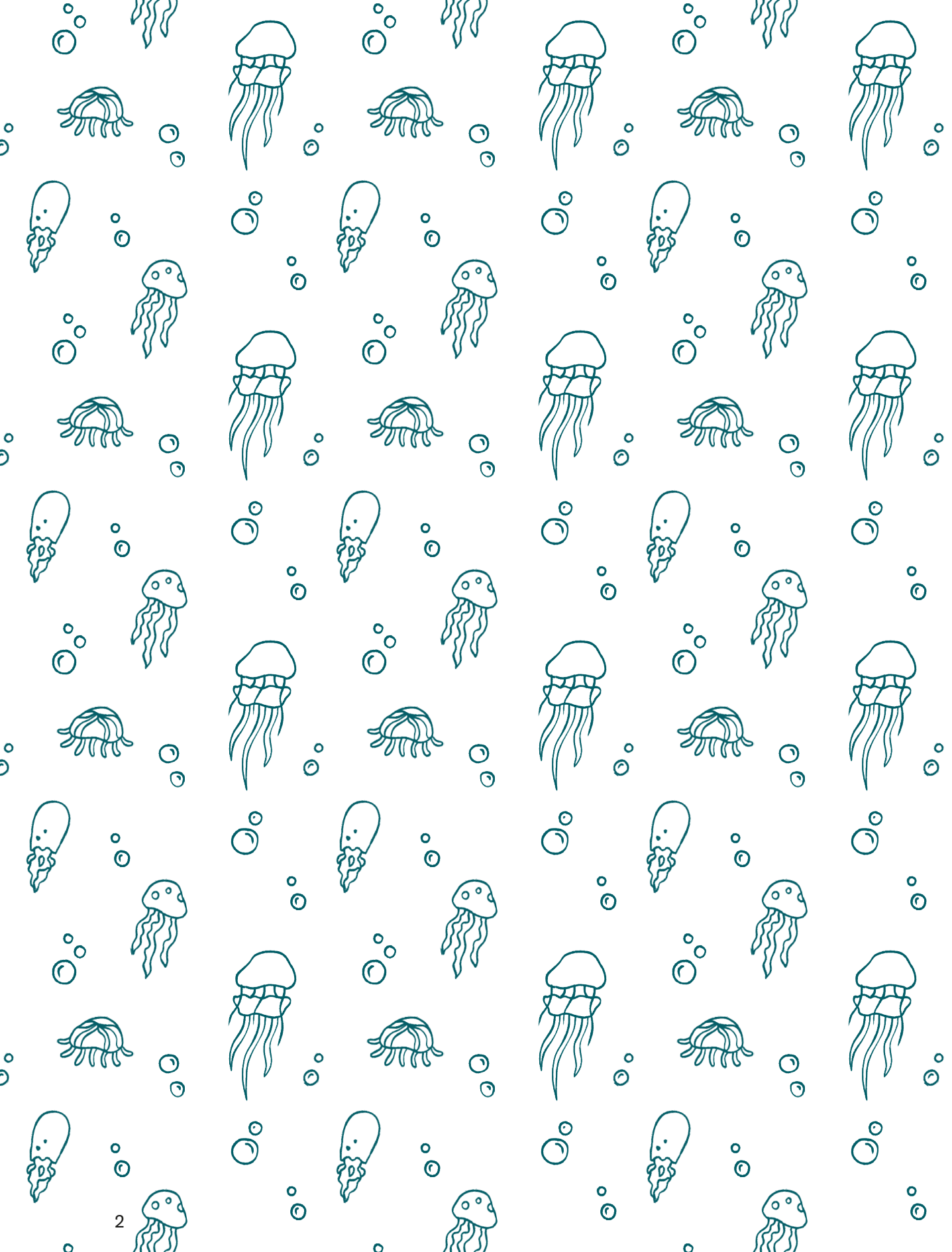
CASA UNIVERSE

A DEEP DIVE INTO HUB B AND THE SWIRL OF EMBEDDED SECURITY

A JOURNEY INTO THE DEPTHS OF HARDWARE SECURITY AND THE RESEARCH WORLD OF CASA



A DEEP DIVE INTO HUB B AND THE SWIRL OF EMBEDDED SECURITY

A JOURNEY INTO THE DEPTHS
OF HARDWARE SECURITY AND
THE RESEARCH WORLD OF CASA

CASA
CYBER SECURITY IN THE AGE
OF LARGE-SCALE ADVERSARIES

CASA

Cyber Security in the Age of Large-Scale Adversaries

Outstanding scientists within the Cluster of Excellence “CASA - Cyber Security in the Age of Large-Scale Adversaries” research and develop strong and sustainable countermeasures against powerful cyber attackers, with a particular focus on nation-state attackers. Research in CASA is characterized by a highly interdisciplinary approach that examines not only technical issues, but also the interplay between human behavior and IT security. This unique, holistic approach forms the basis for excellent IT security research.

CASA unites four main research areas:

HUB A “Future Cryptography”: Researching future cryptography and developing quantum-resistant approaches with provable security.

HUB B “Embedded Security”: Tackling the task of strengthening the security of embedded systems at the hardware level by investigating the interaction of security systems with their physical environment.

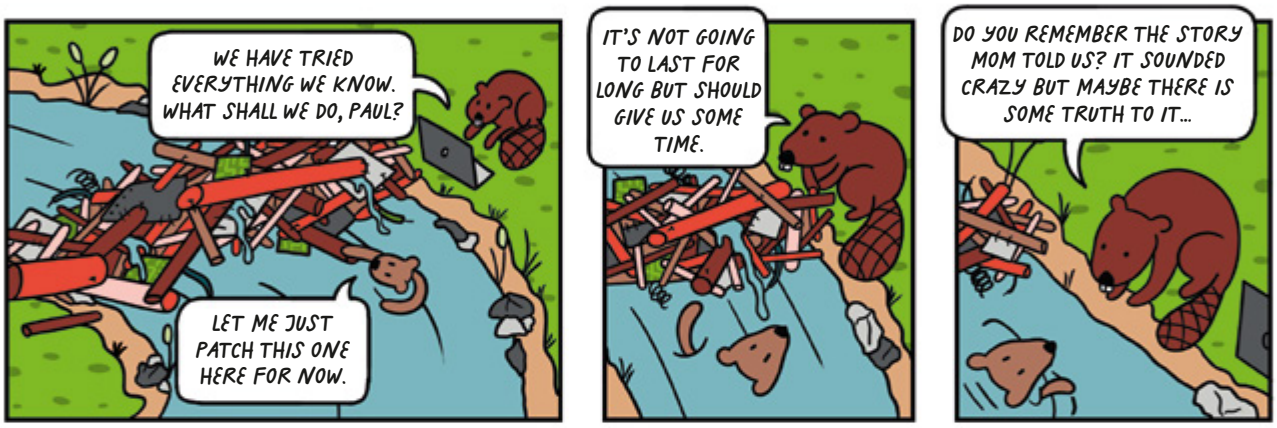
HUB C “Secure Systems”: Developing secure and efficient systems at the software level. Machine Learning is one of the many methods used to explore and expand this field.

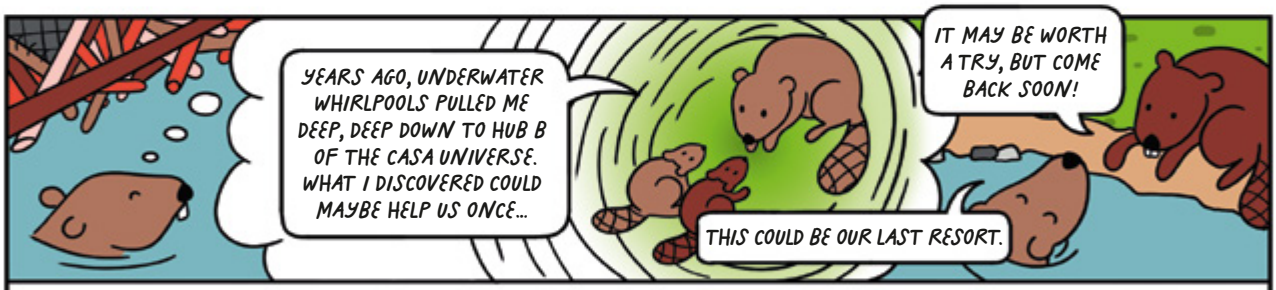
HUB D “Usability”: Focusing on usable security and privacy and researching the interface between humans and technology.

Each HUB addresses specific major research challenges that have been carefully selected to address security issues critical to the protection against large-scale attackers. The challenges of HUB B are:

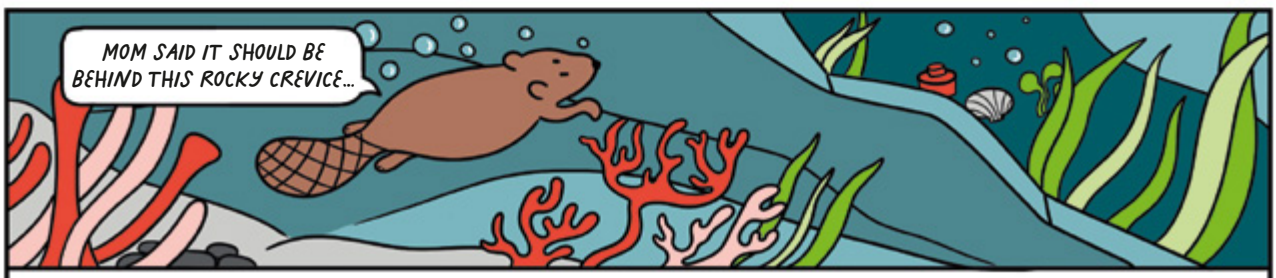
Research Challenge 4: Platform Trojans
Research Challenge 5: Physical-Layer Security
Research Challenge 6: Next-Generation Implementation Security

Deep in a river valley of the CASA Universe, beaver brothers Paul and Carl are struggling to secure their dam. The wooden structure has a disturbance and they are running out of ideas.

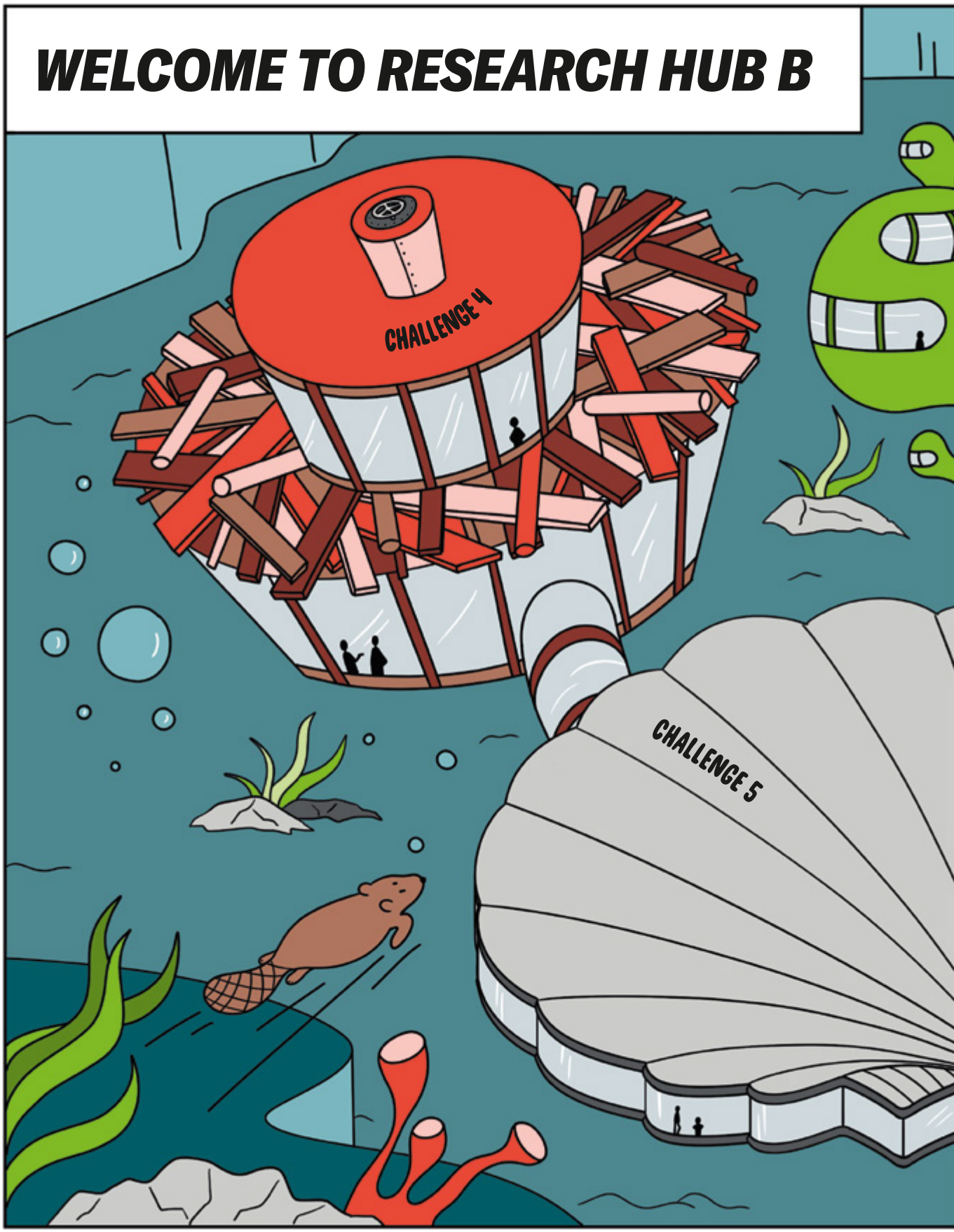


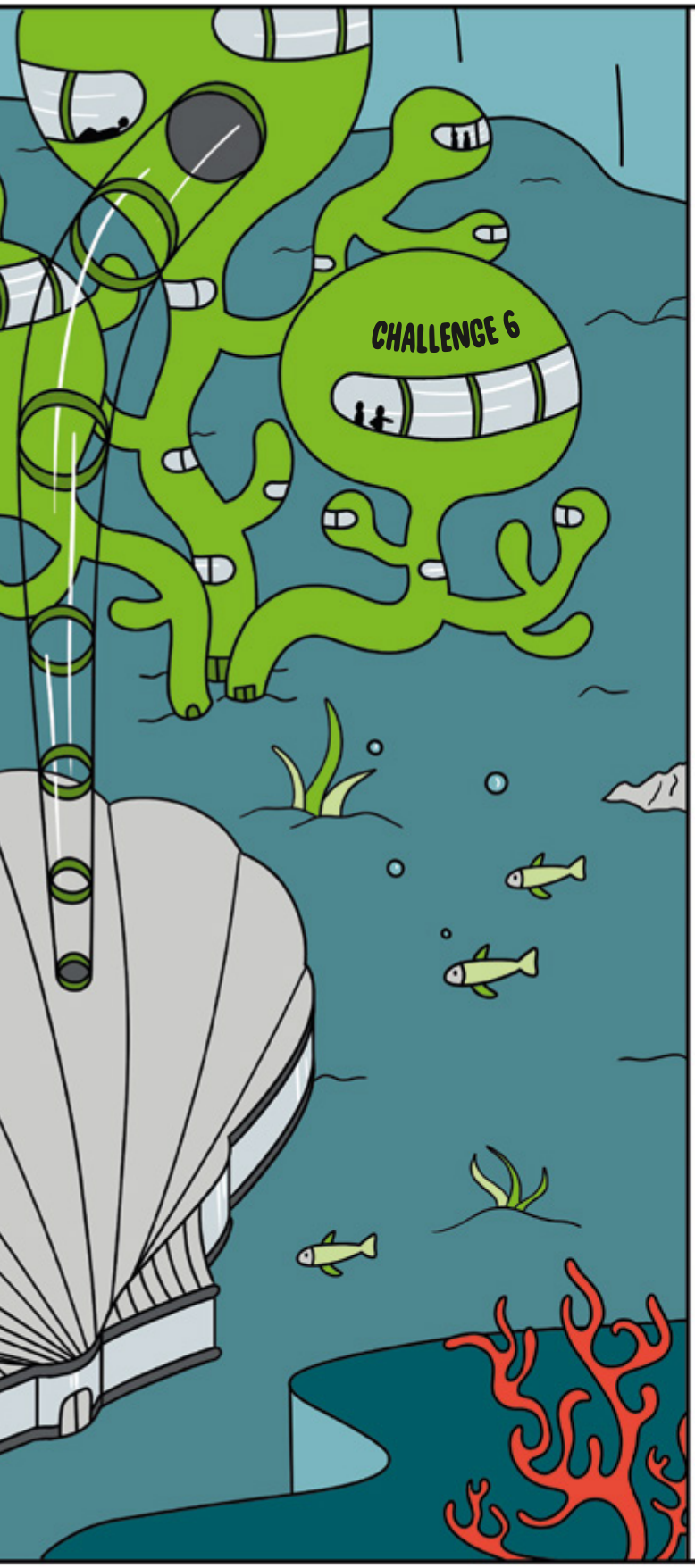


That's when they remember a story they were told long ago, about a place hidden in the depths of the river. A place that may hold solutions to the siblings' problem.



Paul takes a deep breath and dives: Nothing will stop the desperate beaver from saving his dam architecture.


WELCOME TO RESEARCH HUB B
CHALLENGE 4
CHALLENGE 5



Content

CHALLENGE 4

Platform Trojans

What do Hardware Trojans look like? How can we defend against them?

CHALLENGE 5

Physical-Layer Security

How to construct new security building blocks from wireless radio signals?

CHALLENGE 6

Next-Generation Implementation Security

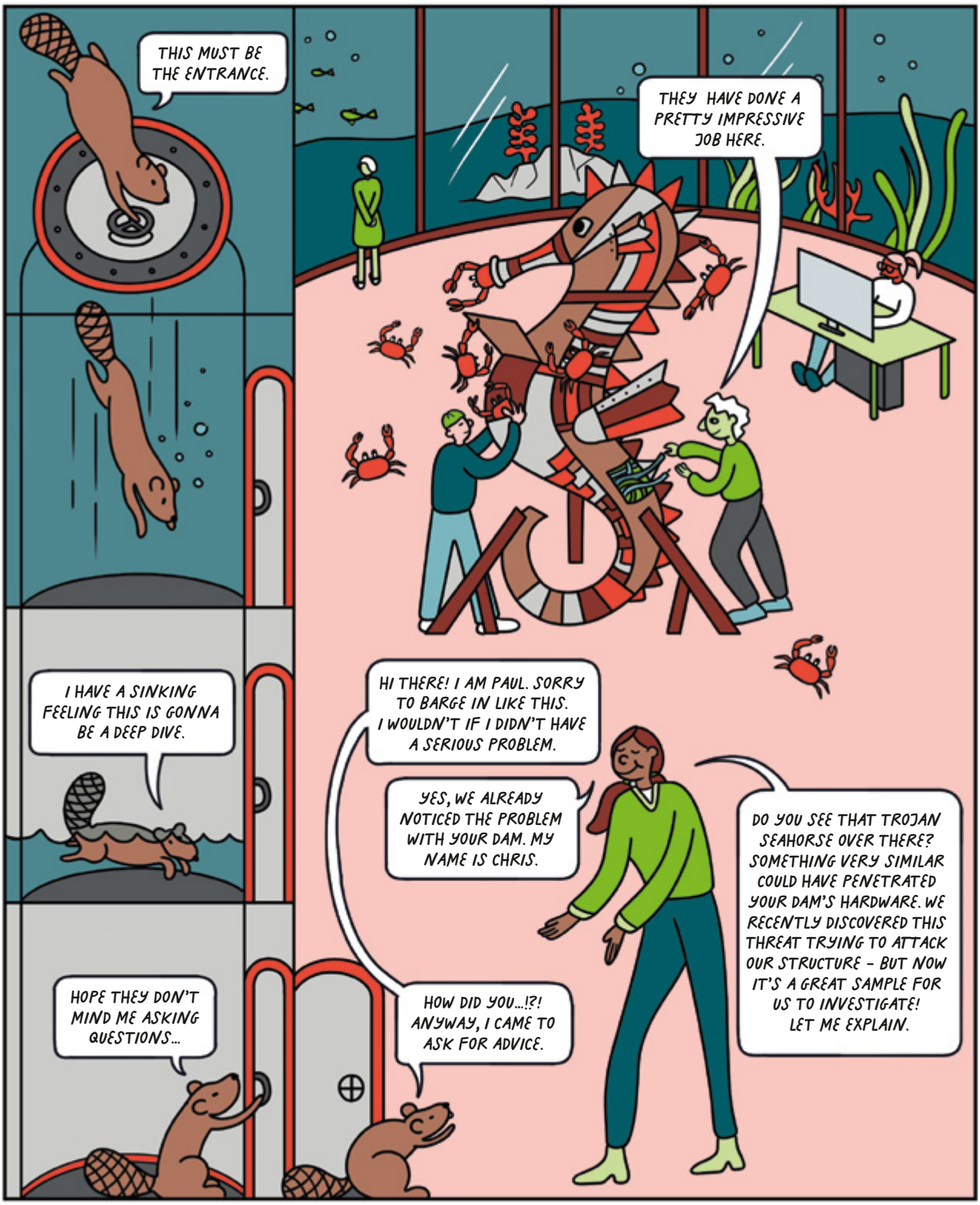
How can we secure future computers against attacks that exploit the ways how crypto is implemented?

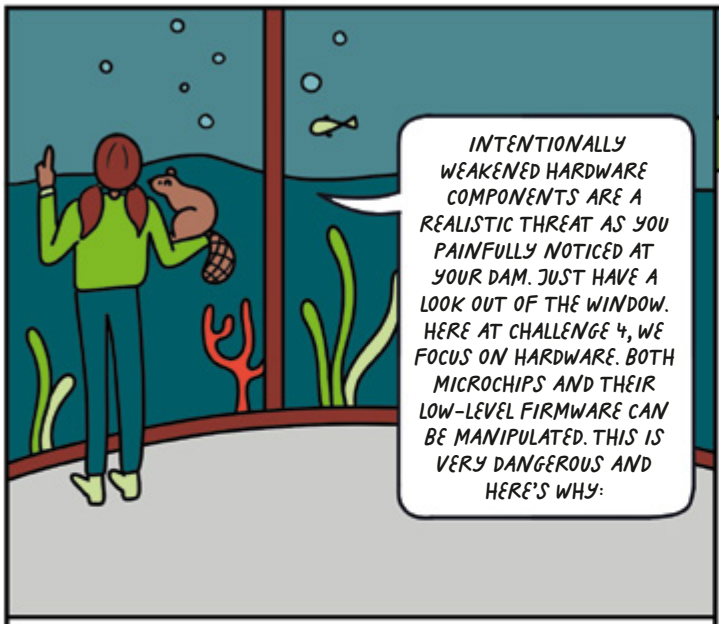
CASA BACKGROUND

CASA stands for ‘Cyber Security in the Age of Large-Scale Adversaries’ and is funded as a Cluster of Excellence (EXC) within the Excellence Strategy of the DFG in Germany. Its goal is to enable sustainable security against sophisticated large-scale attacks. Therefore, an interdisciplinary team explores not only technical, but also social factors and implications. The Cluster of Excellence is located at Ruhr University Bochum.

casa.rub.de

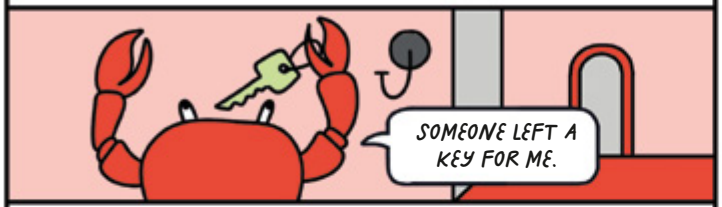
PLATFORM CHALLENGE 4 TROJANS



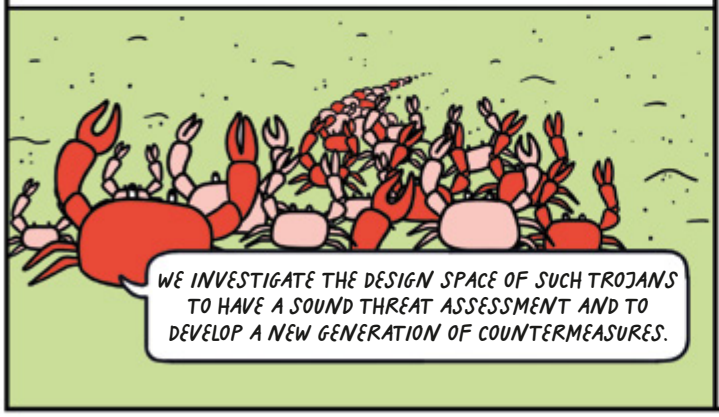


Firstly, it can be extremely difficult to detect such manipulations and it is often impossible to remove them.

Secondly, low-level manipulations can disable all other higher-level security mechanisms.



Finally, such attacks can compromise millions of devices, for example, in the case of network routers.



CASA WIKI

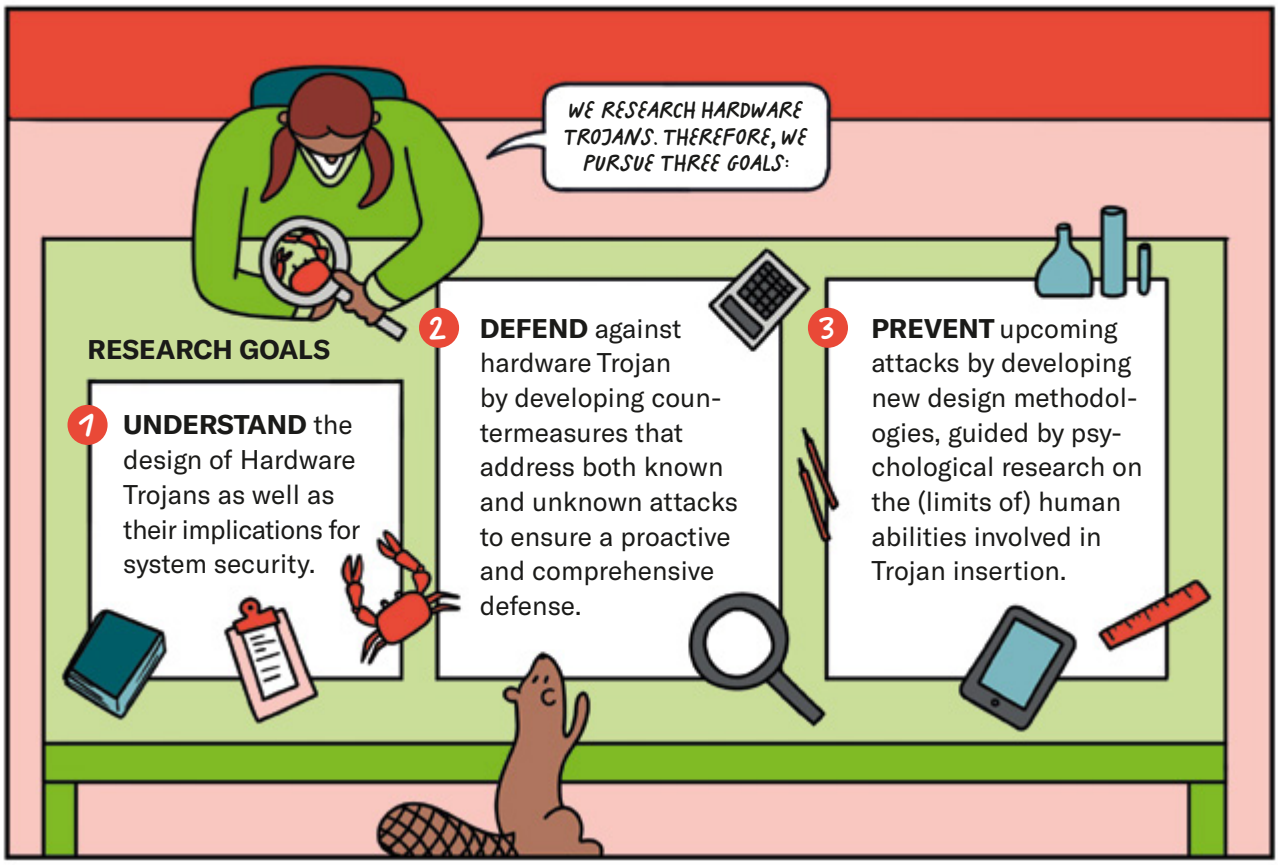
A Hardware Trojan is a malicious modification or insertion of circuitry into an Integrated Circuit (IC) or electronic device. It is performed post-design by an entity other than the original designer to compromise the security or functionality of the device. The name refers to the Greek 'Trojan Horse' tale.

A Microchip is a small electronic device made of semiconductor materials that performs various functions such as the processing and storing of information. Microchips are integral parts of smartphones, cars, planes and lots of other devices.

Hardware Reverse Engineering is the process of taking apart a physical device (e.g. a microchip) to understand its design and functionality. Applications (of hardware reverse engineering) include the detection of intellectual property infringement or Hardware Trojans.

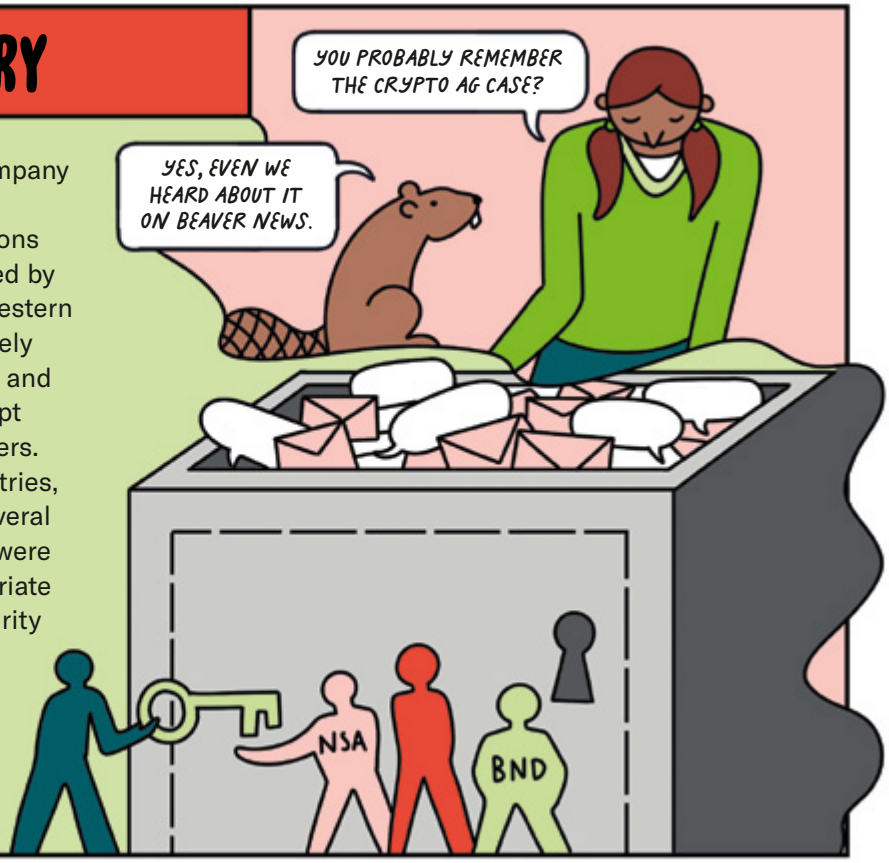
Hackers are people with advanced knowledge of hardware and software. So-called white-hat hackers seek out vulnerabilities in order to mitigate them. Black-hat hackers, on the other hand, exploit them for malicious goals.

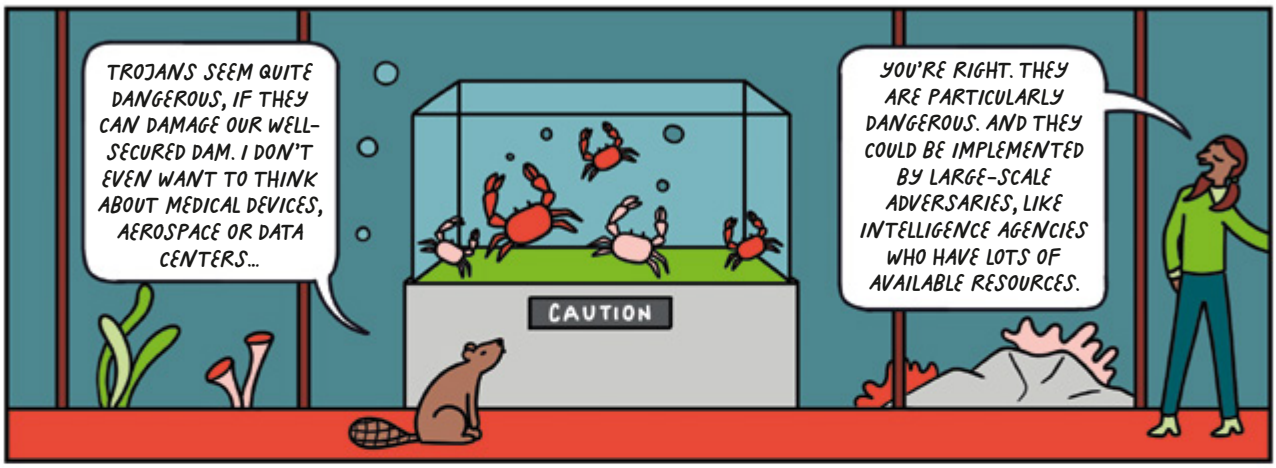
Microcode is an updatable part of modern CPUs. It was invented to solve issues in computer chips after deployment as in 1994 Intel had to recall an entire CPU series due to a bug. The microcode design details are typically company secrets. While this updatability is useful, it also opens a potential door for harmful interference.



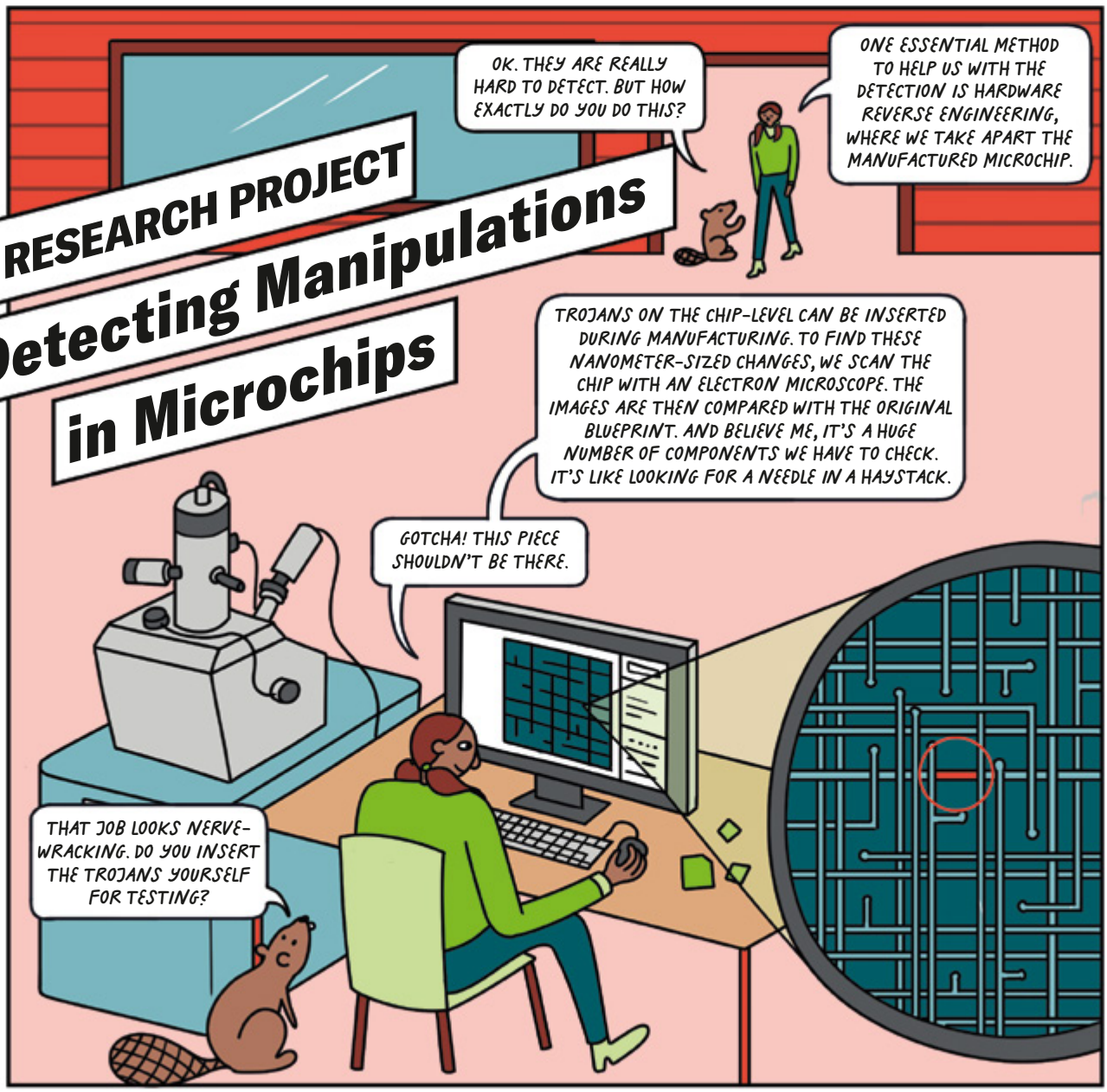
REAL LIFE STORY

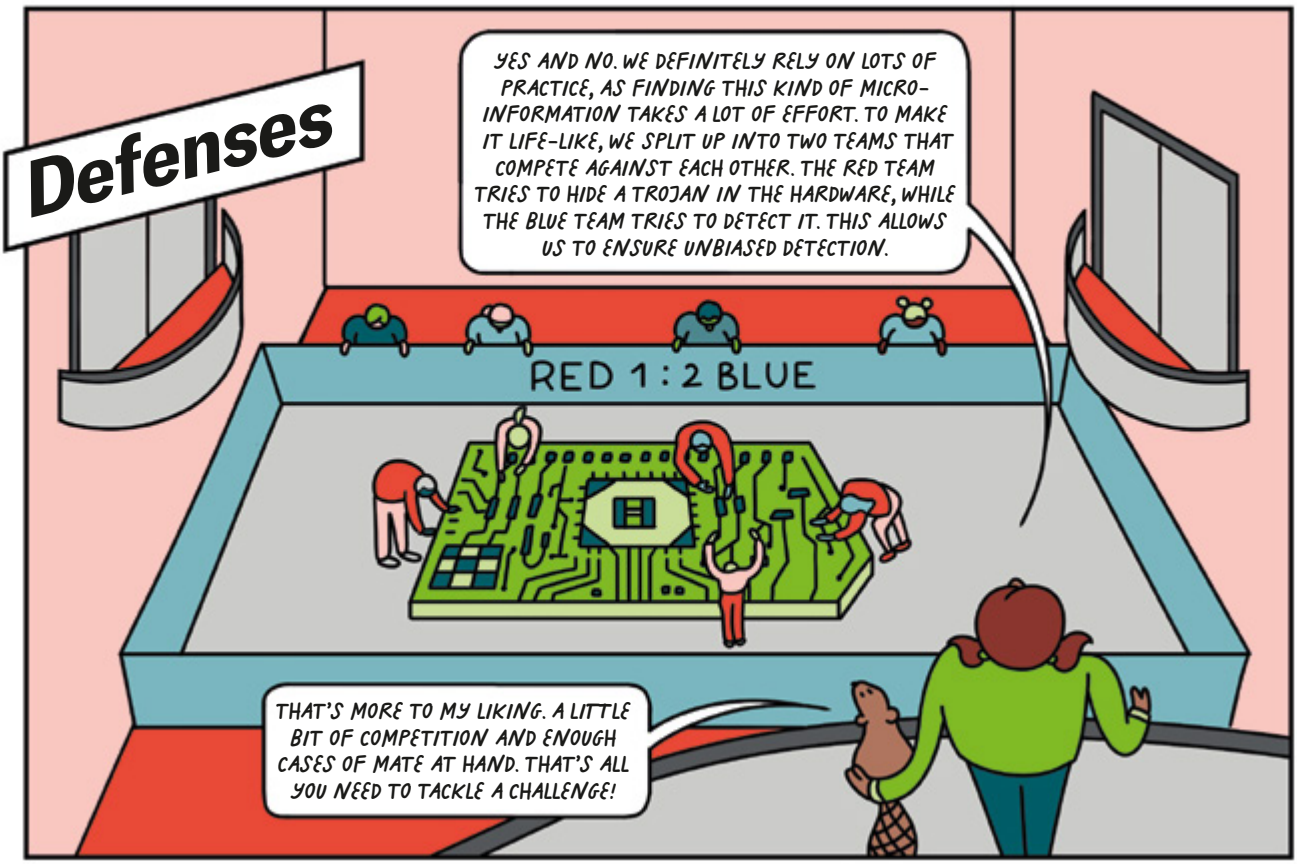
Crypto AG was a Swiss company that manufactured analog cipher devices. Some versions were intentionally weakened by backdoors. This allowed Western intelligence agencies (namely the CIA, the British GCHQ, and the German BND) to decrypt messages sent by other users. More than a hundred countries, such as Iran, India, and several Latin American countries, were affected. This is an appropriate example of bypassing security mechanisms at the hardware level.

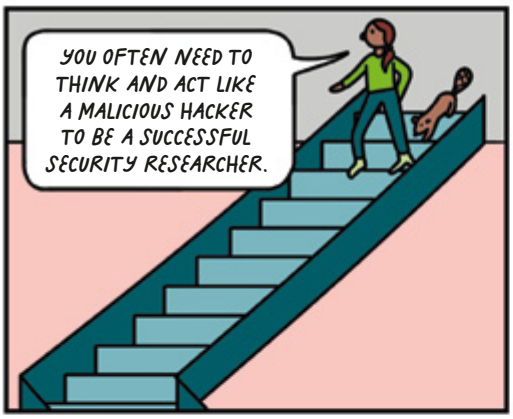


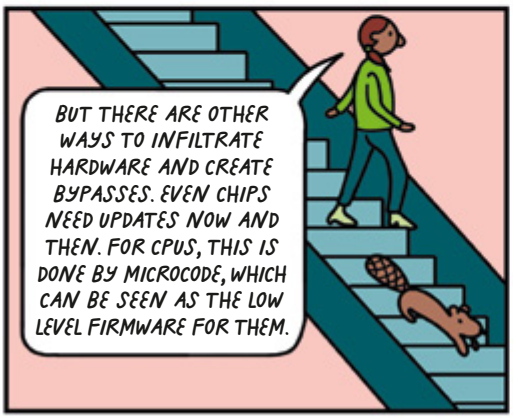


RESEARCH PROJECT
Detecting Manipulations in Microchips

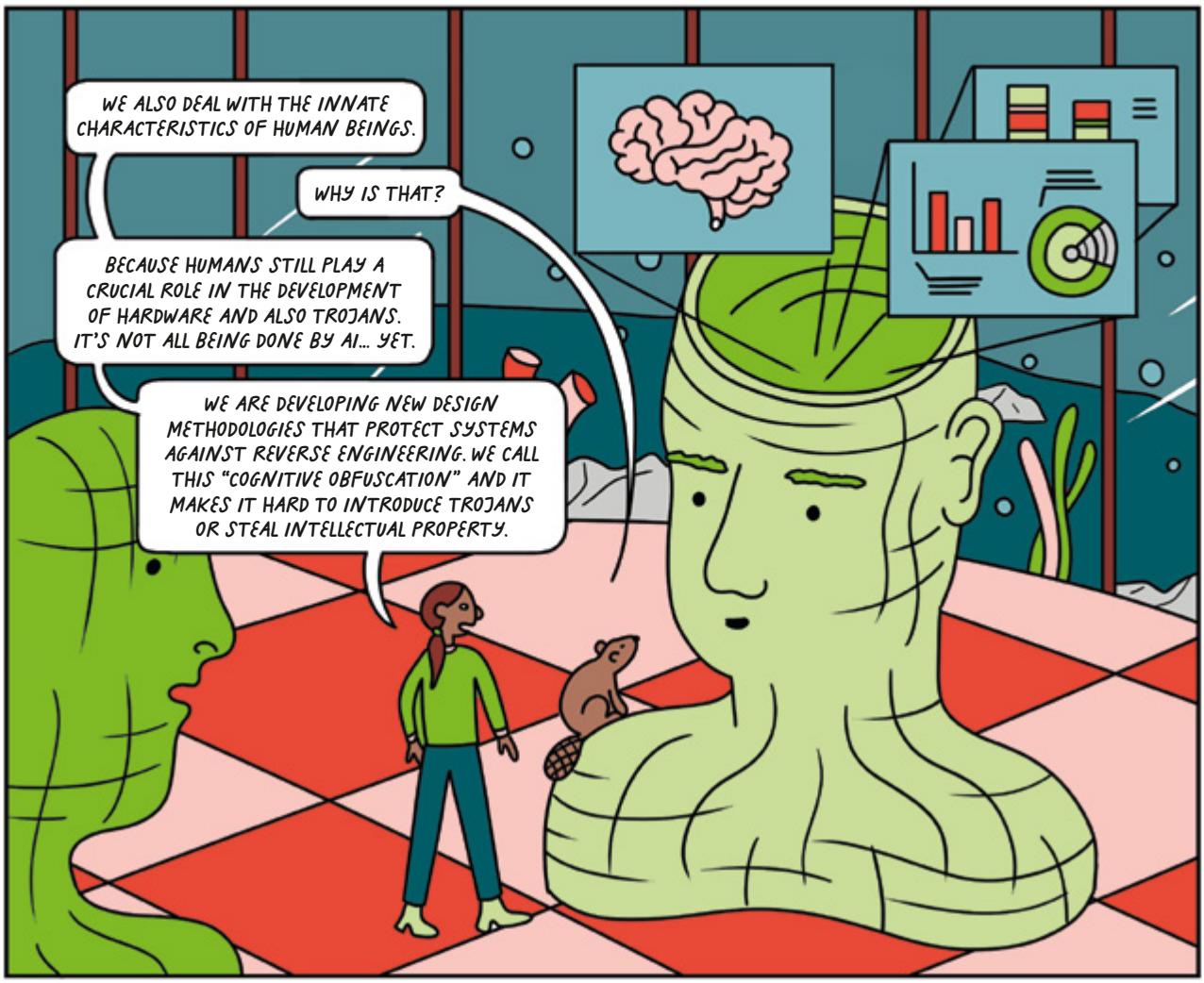



Defenses
YES AND NO. WE DEFINITELY RELY ON LOTS OF PRACTICE, AS FINDING THIS KIND OF MICRO-INFORMATION TAKES A LOT OF EFFORT. TO MAKE IT LIFE-LIKE, WE SPLIT UP INTO TWO TEAMS THAT COMPETE AGAINST EACH OTHER. THE RED TEAM TRIES TO HIDE A TROJAN IN THE HARDWARE, WHILE THE BLUE TEAM TRIES TO DETECT IT. THIS ALLOWS US TO ENSURE UNBIASED DETECTION.
RED 1 : 2 BLUE
THAT'S MORE TO MY LIKING. A LITTLE BIT OF COMPETITION AND ENOUGH CASES OF MATE AT HAND. THAT'S ALL YOU NEED TO TACKLE A CHALLENGE!


YOU OFTEN NEED TO THINK AND ACT LIKE A MALICIOUS HACKER TO BE A SUCCESSFUL SECURITY RESEARCHER.


BUT THERE ARE OTHER WAYS TO INFILTRATE HARDWARE AND CREATE BYPASSES. EVEN CHIPS NEED UPDATES NOW AND THEN. FOR CPUS, THIS IS DONE BY MICROCODE, WHICH CAN BE SEEN AS THE LOW LEVEL FIRMWARE FOR THEM.

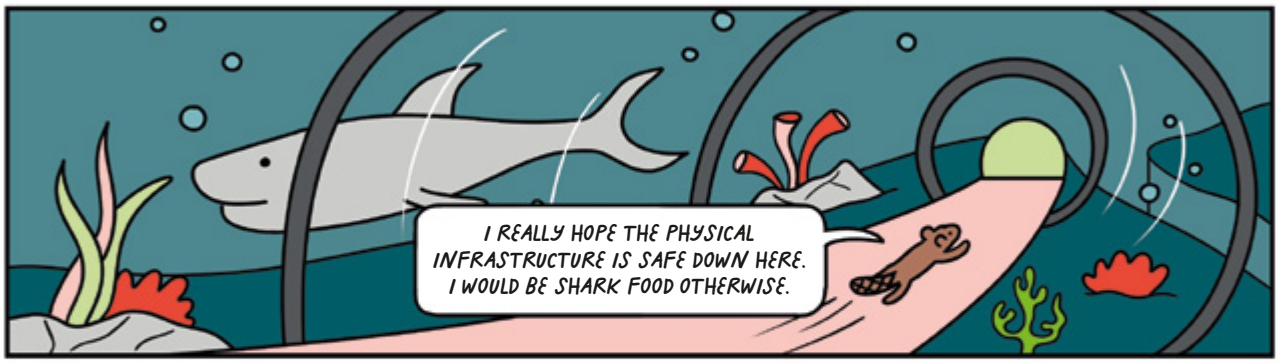

AND CODE IS LAW AS WE ALL KNOW. IT IS AT THE HEART OF THE CPU. EVEN A SECURITY UPDATE CAN BE USED TO INJECT MALICIOUS CODE INTO THE MOST SENSITIVE AREAS OF A COMPUTER SYSTEM. YOU WOULDN'T WANT YOUR PACEMAKER CORRUPTED, WOULD YOU!?!

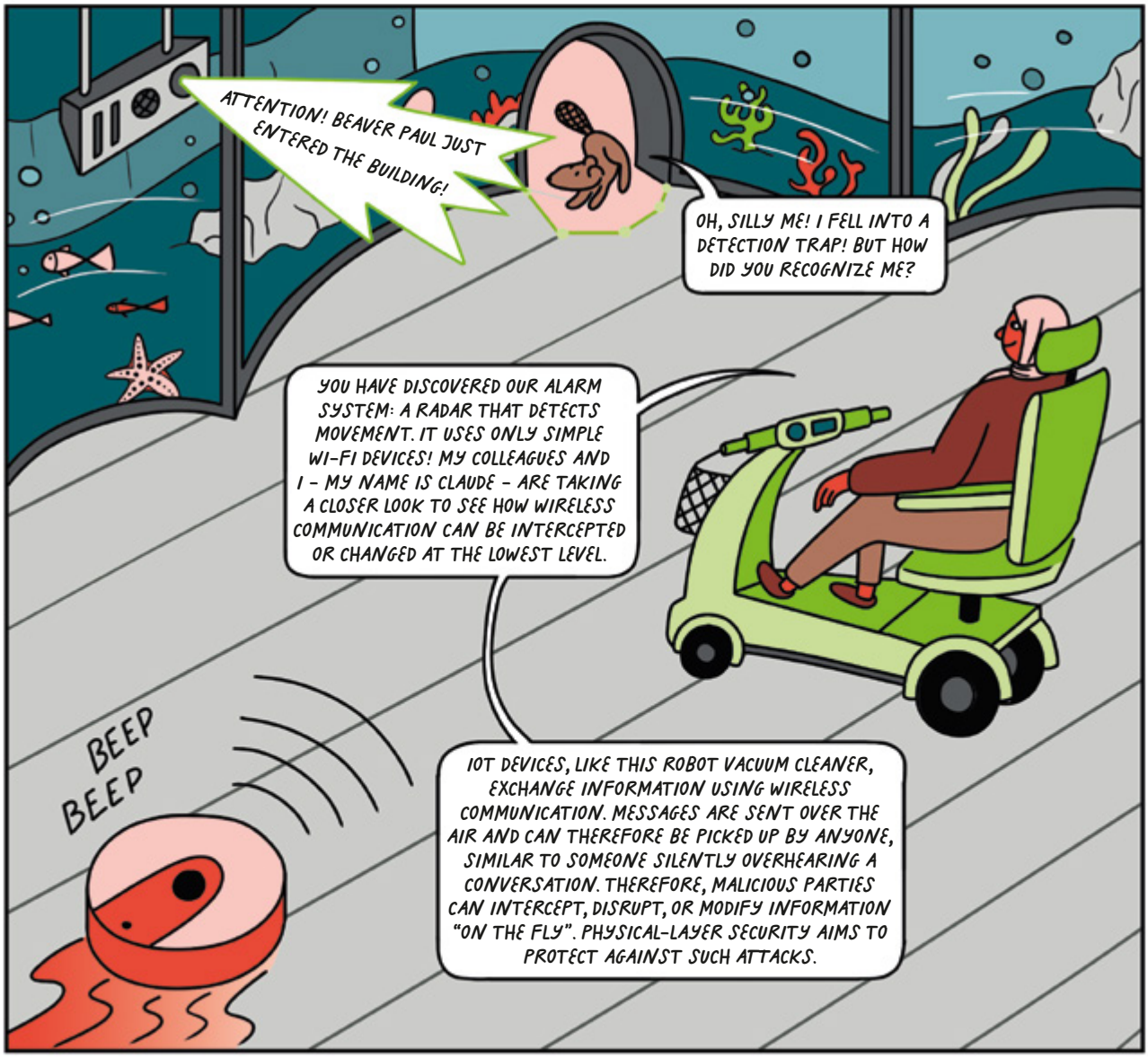

WE ALSO DEAL WITH THE INNATE CHARACTERISTICS OF HUMAN BEINGS.
WHY IS THAT?
BECAUSE HUMANS STILL PLAY A CRUCIAL ROLE IN THE DEVELOPMENT OF HARDWARE AND ALSO TROJANS. IT'S NOT ALL BEING DONE BY AI... YET.
WE ARE DEVELOPING NEW DESIGN METHODOLOGIES THAT PROTECT SYSTEMS AGAINST REVERSE ENGINEERING. WE CALL THIS "COGNITIVE OBFUSCATION" AND IT MAKES IT HARD TO INTRODUCE TROJANS OR STEAL INTELLECTUAL PROPERTY.

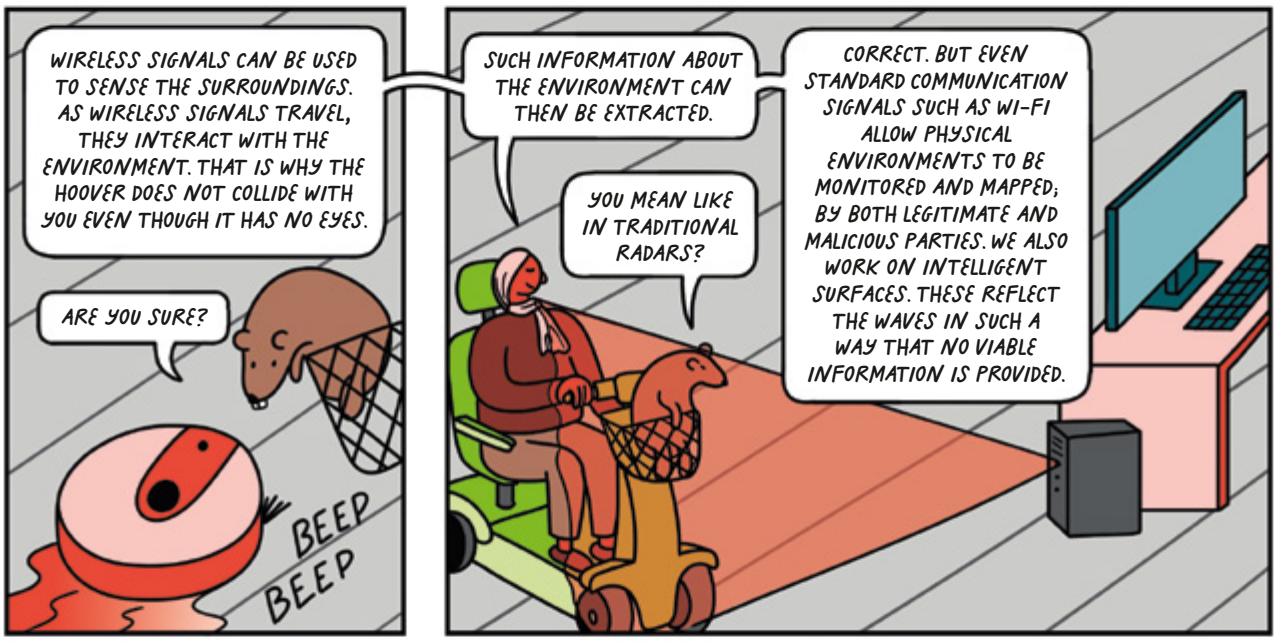

SO DO YOU THINK IT'S A HARDWARE TROJAN THAT INFILTRATED OUR DAM?
IT IS NOT UNLIKELY, BUT THERE ARE MORE POSSIBILITIES. PERHAPS THE TIMBER SUPPLY FOR THE DAM WAS REPLACED BY DAMAGED MATERIAL WITHOUT YOU NOTICING. IT IS BEST TO ASK OUR PALS WHO DEAL WITH PHYSICAL-LAYER SECURITY. THEY INVESTIGATE SOLUTIONS TO DETECT SUCH MANIPULATIONS.
THANK YOU SO MUCH! I DEFINITELY LEARNED A LOT!
BY THE WAY, WE CALL THEIR BUILDING THE TREASURE CHAMBER. YOU SOON WILL FIND OUT WHY.

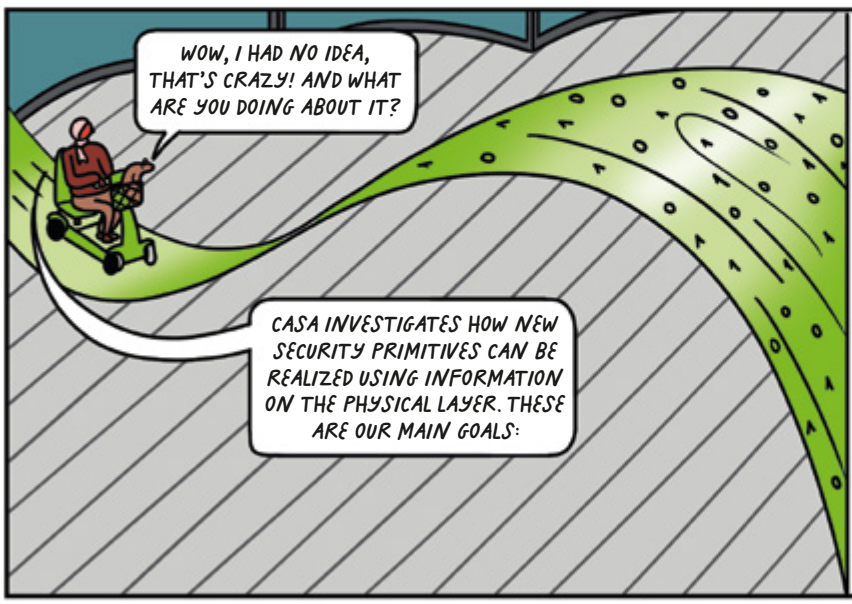
PHYSICAL-LAYER SECURITY

CHALLENGE 5



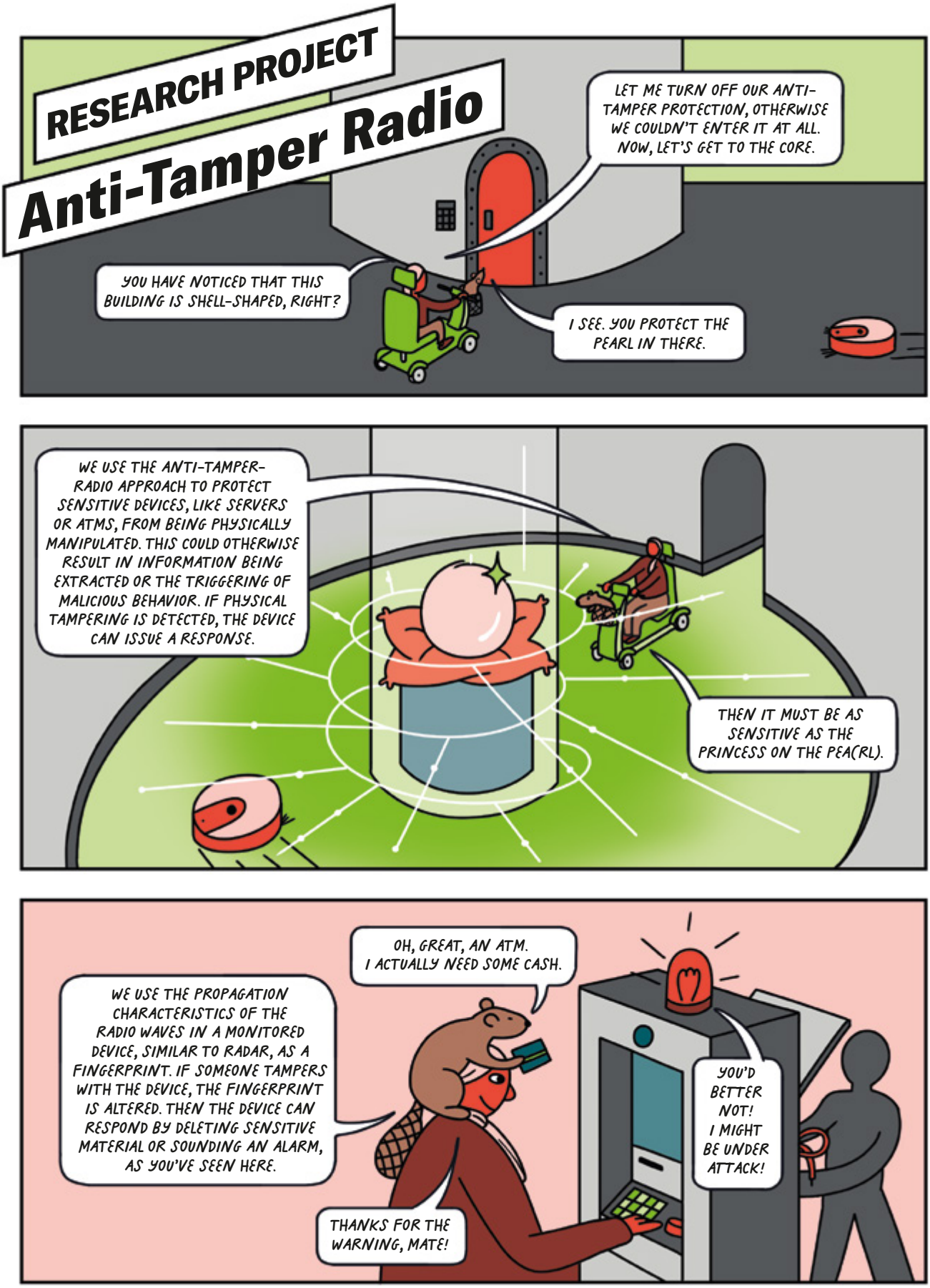






RESEARCH GOALS

1. Investigate novel techniques for securing communication channels.
2. Design and build next-generation secure wireless communication.
3. Investigate wireless sensing systems to monitor the physical integrity of computing systems.
4. Investigate privacy aspects of wireless sensing.


RESEARCH PROJECT
Anti-Tamper Radio
LET ME TURN OFF OUR ANTI-TAMPER PROTECTION, OTHERWISE WE COULDN'T ENTER IT AT ALL. NOW, LET'S GET TO THE CORE.
YOU HAVE NOTICED THAT THIS BUILDING IS SHELL-SHAPED, RIGHT?
I SEE. YOU PROTECT THE PEARL IN THERE.
WE USE THE ANTI-TAMPER-RADIO APPROACH TO PROTECT SENSITIVE DEVICES, LIKE SERVERS OR ATMS, FROM BEING PHYSICALLY MANIPULATED. THIS COULD OTHERWISE RESULT IN INFORMATION BEING EXTRACTED OR THE TRIGGERING OF MALICIOUS BEHAVIOR. IF PHYSICAL TAMPERING IS DETECTED, THE DEVICE CAN ISSUE A RESPONSE.
THEN IT MUST BE AS SENSITIVE AS THE PRINCESS ON THE PEA(RL).
WE USE THE PROPAGATION CHARACTERISTICS OF THE RADIO WAVES IN A MONITORED DEVICE, SIMILAR TO RADAR, AS A FINGERPRINT. IF SOMEONE TAMPERS WITH THE DEVICE, THE FINGERPRINT IS ALTERED. THEN THE DEVICE CAN RESPOND BY DELETING SENSITIVE MATERIAL OR SOUNDING AN ALARM, AS YOU'VE SEEN HERE.
OH, GREAT, AN ATM. I ACTUALLY NEED SOME CASH.
YOU'D BETTER NOT! I MIGHT BE UNDER ATTACK!
THANKS FOR THE WARNING, MATE!

CASA WIKI

Wireless sensing is the process of inferring information about physical environments from ordinary wireless communication signals (similar to radar).

Wireless channels are the combinations of all physical effects that affect a wireless signal traveling from a transmitter to a receiver. An analogy from the acoustic domain: If one person speaks, a second person may hear that same speech, but attenuated (less loud) and with added reverb from the room (due to reflections). The wireless channel is like a fingerprint of the physical environment.

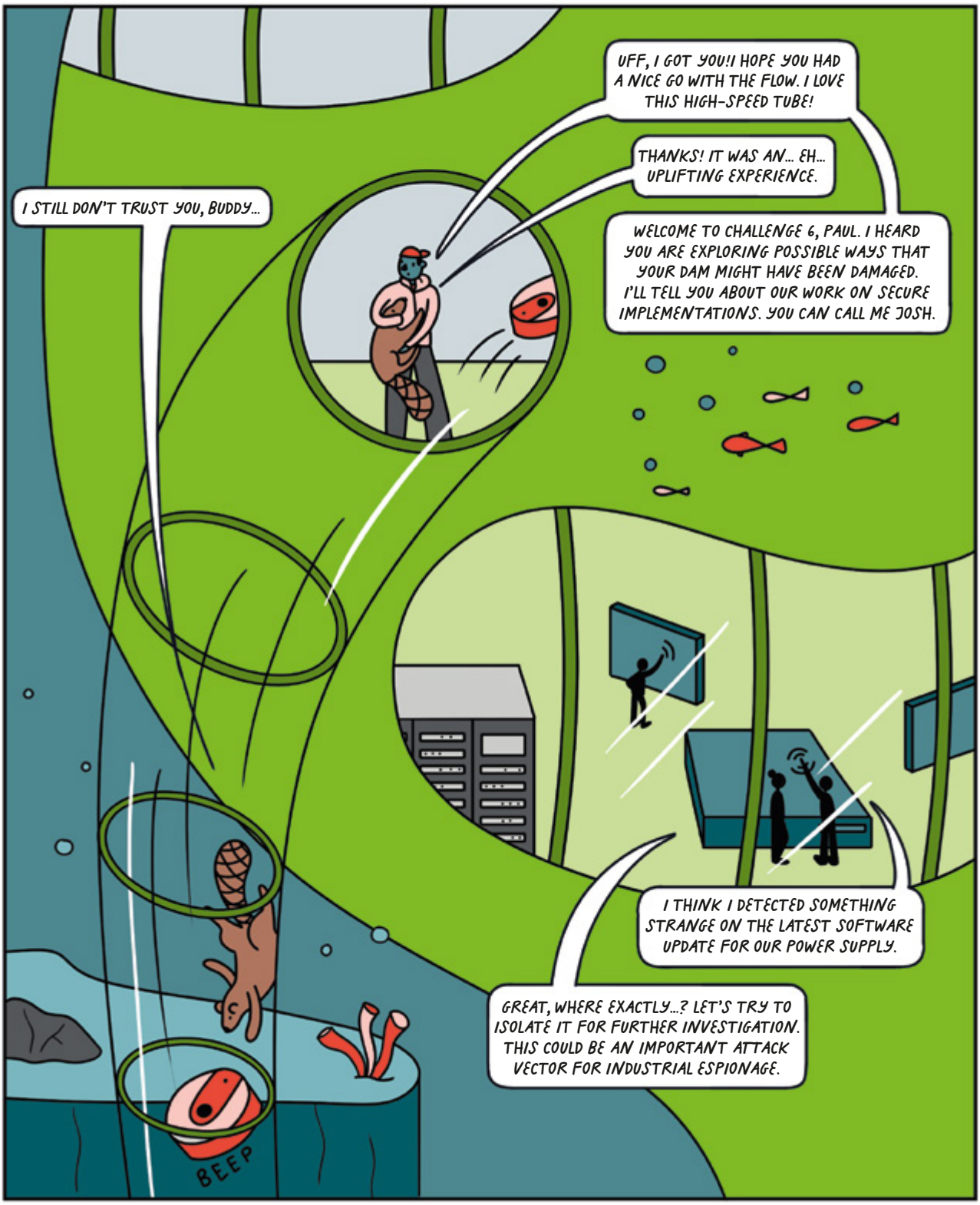
Tamper detection describes the processing of some sensor data (e.g. observing wireless channels) to detect unauthorized physical changes of an environment, possibly indicating a physical attack.

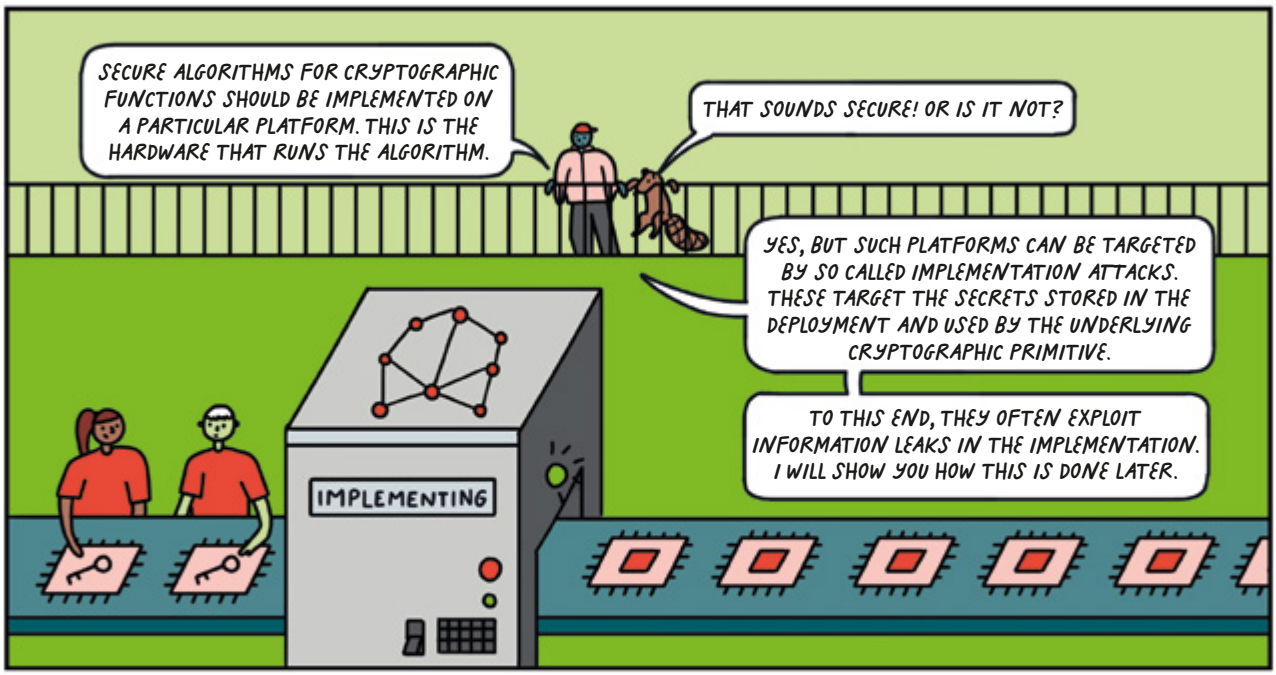
Intelligent reflecting surfaces are digitally configurable reflectors of radio waves that can be used to manipulate wireless signals. The technology is likely to be integrated into future 6G wireless communication systems.

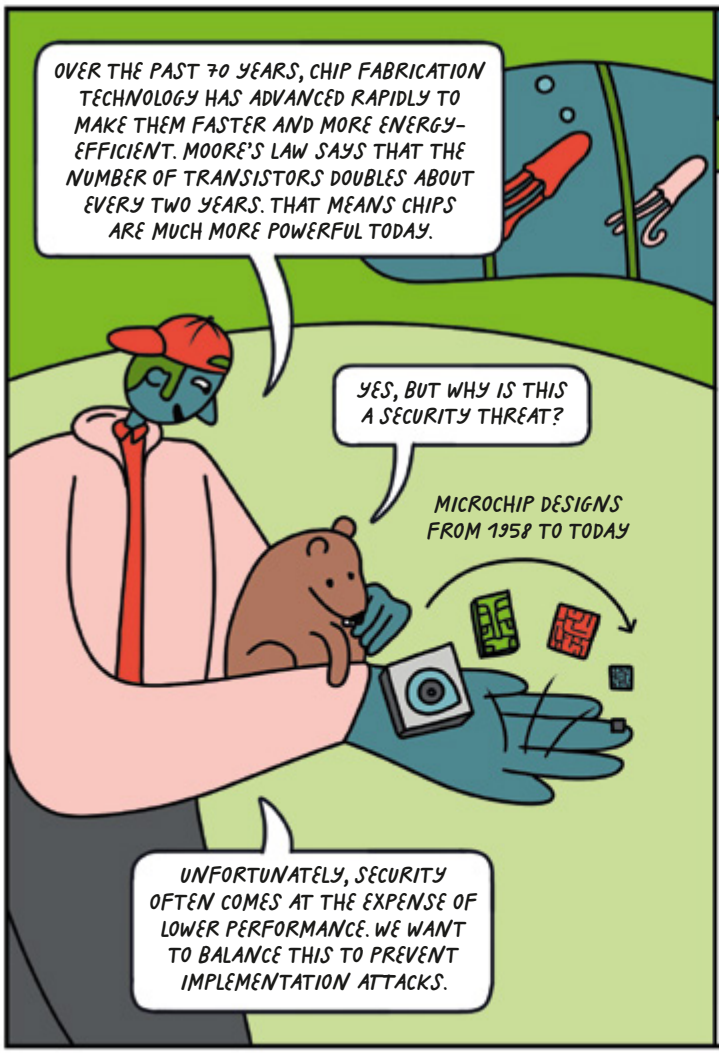
Human motion detection utilizes wireless sensing to identify the presence of individuals, possibly violating their privacy. Apart from that, more advanced applications of wireless sensing include the recognition of activities and gestures as well as vital sign monitoring.

NEXT-GENERATION IMPLEMENTATION SECURITY

CHALLENGE 6





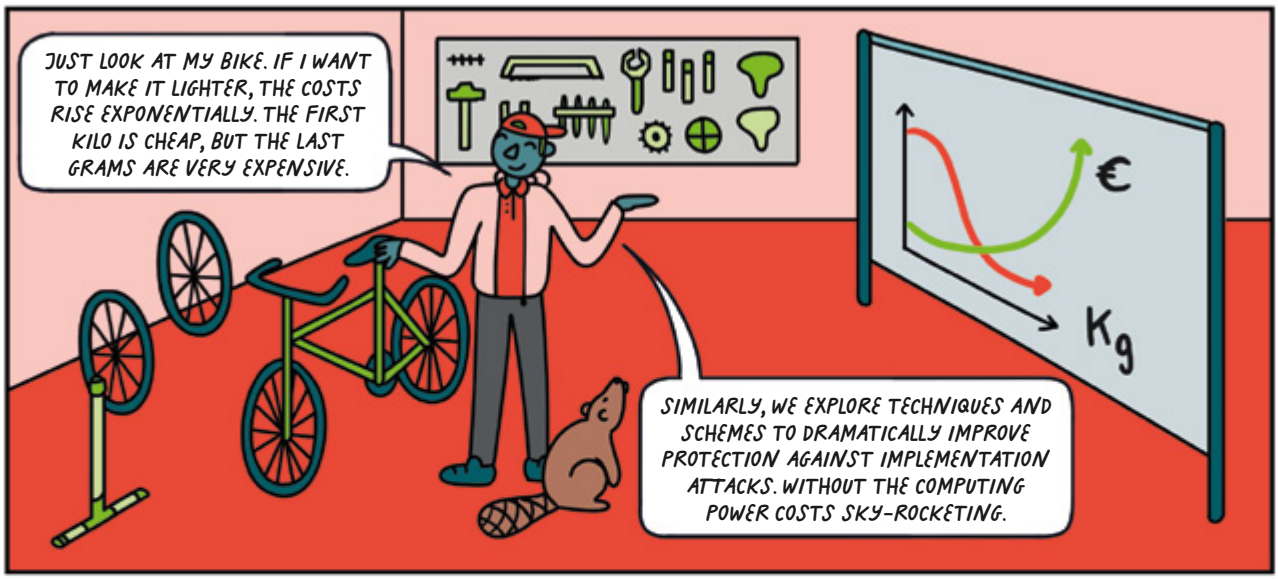


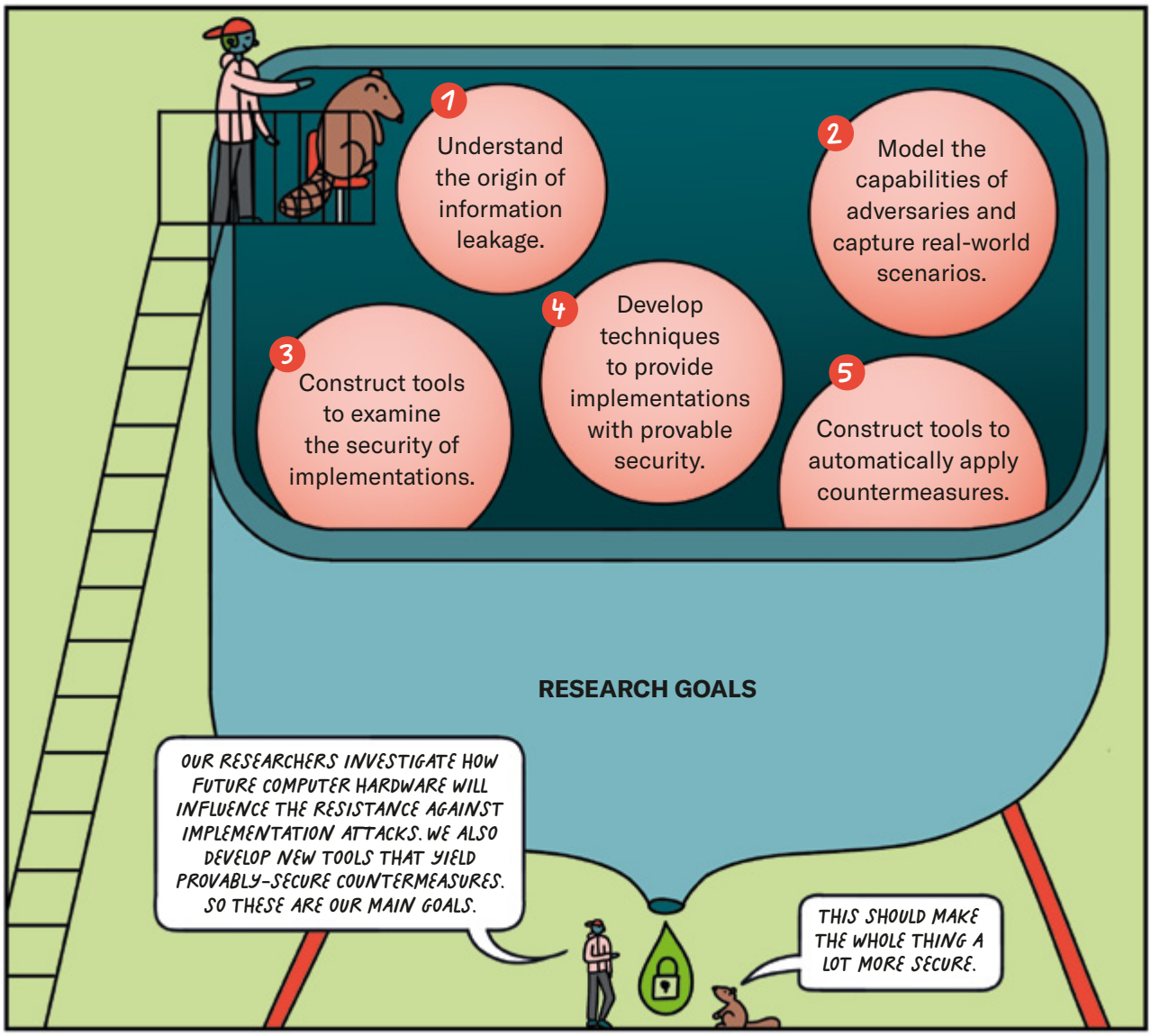
CASA WIKI

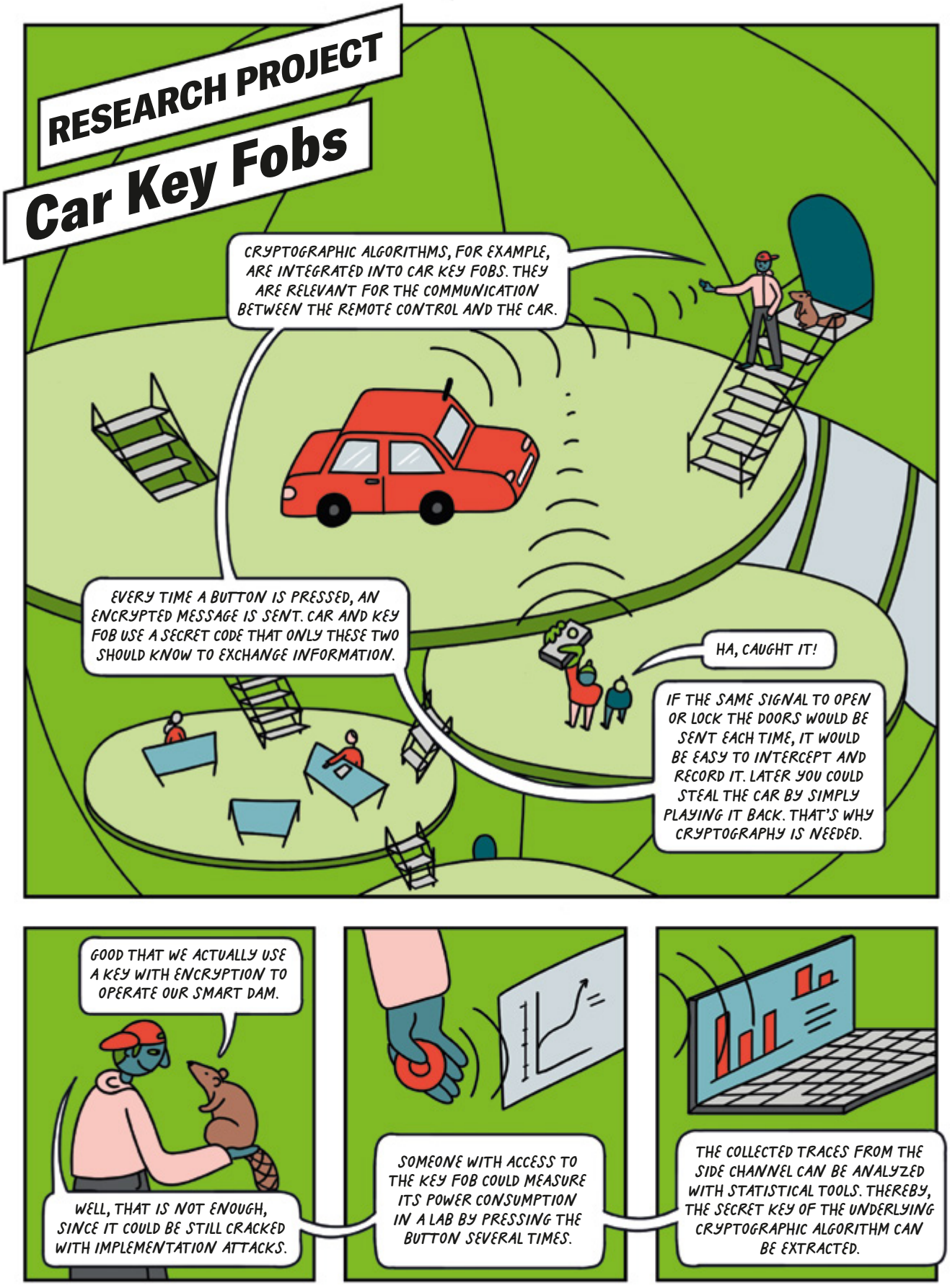
Cryptographic primitives are mathematical algorithms used as fundamental building blocks in security protocols. They ensure that the protected data cannot be read or tampered with and that it actually originates from the entity that claims to have sent it.

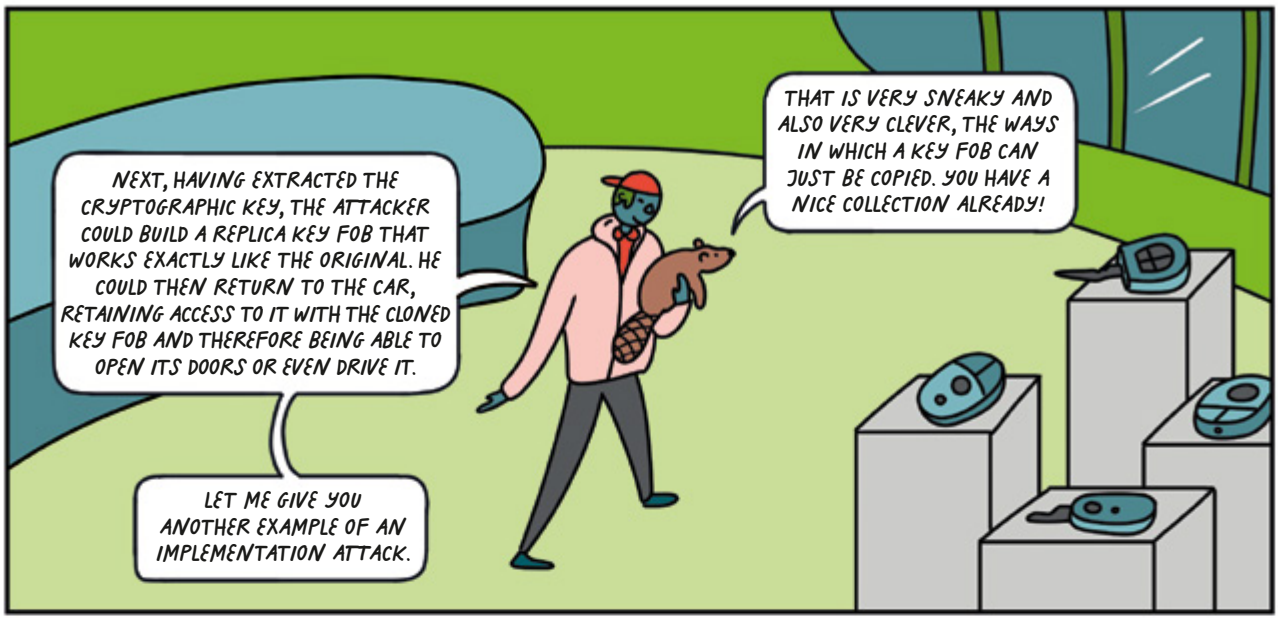
An implementation is a realization of a technical specification or algorithm as a program (software) or electronic device (hardware). For this, implementation attacks attempt to break the realization of the cryptographic algorithm rather than the cryptography itself.

Side-Channel Analysis (SCA) observes and evaluates unintentional physical characteristics (e.g. power consumption, electro-magnetic radiation, or response time) of an electronic device while cryptographic implementations are performed by the target.


JUST LOOK AT MY BIKE. IF I WANT TO MAKE IT LIGHTER, THE COSTS RISE EXPONENTIALLY. THE FIRST KILO IS CHEAP, BUT THE LAST GRAMS ARE VERY EXPENSIVE.
€
Kg
SIMILARLY, WE EXPLORE TECHNIQUES AND SCHEMES TO DRAMATICALLY IMPROVE PROTECTION AGAINST IMPLEMENTATION ATTACKS. WITHOUT THE COMPUTING POWER COSTS SKY-ROCKETING.

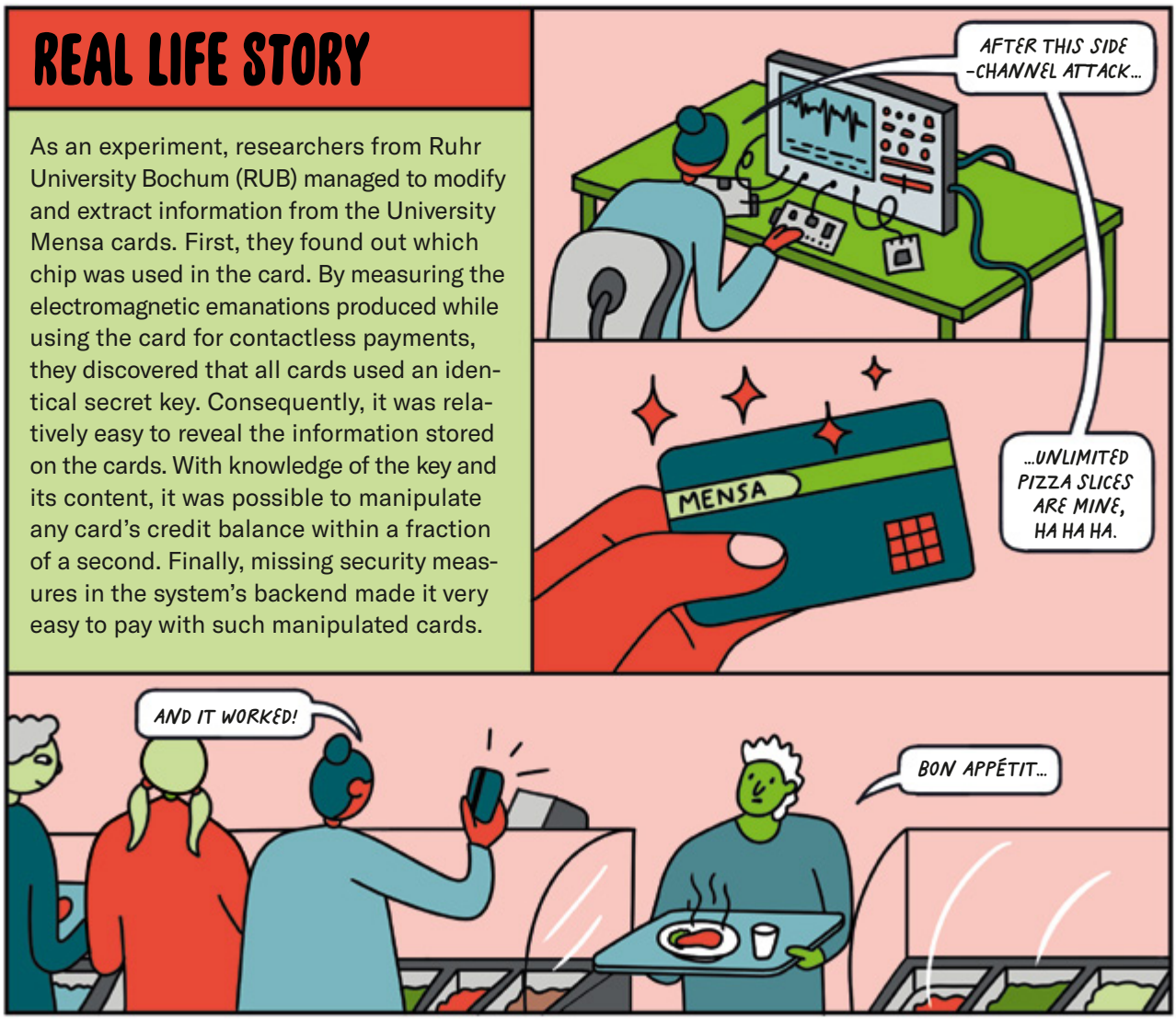

1
Understand the origin of information leakage.
2
Model the capabilities of adversaries and capture real-world scenarios.
3
Construct tools to examine the security of implementations.
4
Develop techniques to provide implementations with provable security.
5
Construct tools to automatically apply countermeasures.
RESEARCH GOALS
OUR RESEARCHERS INVESTIGATE HOW FUTURE COMPUTER HARDWARE WILL INFLUENCE THE RESISTANCE AGAINST IMPLEMENTATION ATTACKS. WE ALSO DEVELOP NEW TOOLS THAT YIELD PROVABLY-SECURE COUNTERMEASURES. SO THESE ARE OUR MAIN GOALS.
THIS SHOULD MAKE THE WHOLE THING A LOT MORE SECURE.

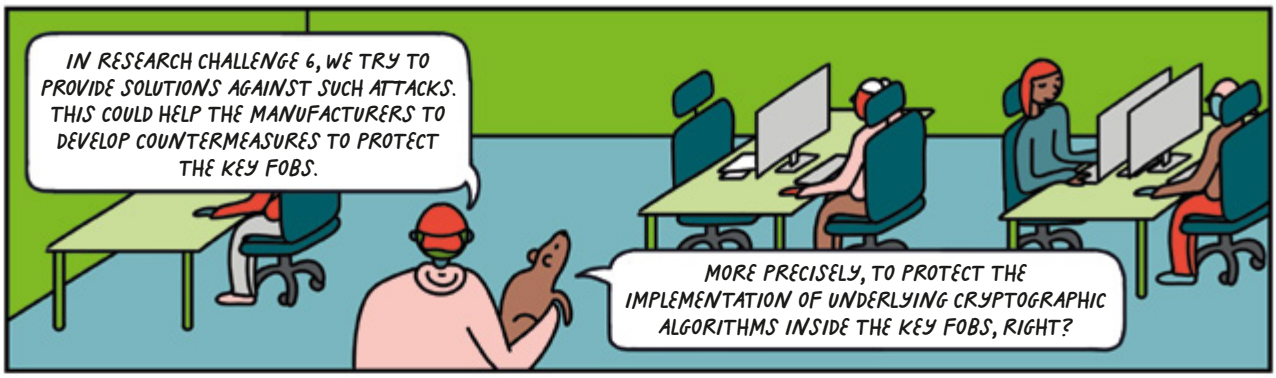

RESEARCH PROJECT
Car Key Fobs
CRYPTOGRAPHIC ALGORITHMS, FOR EXAMPLE, ARE INTEGRATED INTO CAR KEY FOBS. THEY ARE RELEVANT FOR THE COMMUNICATION BETWEEN THE REMOTE CONTROL AND THE CAR.
EVERY TIME A BUTTON IS PRESSED, AN ENCRYPTED MESSAGE IS SENT. CAR AND KEY FOB USE A SECRET CODE THAT ONLY THESE TWO SHOULD KNOW TO EXCHANGE INFORMATION.
HA, CAUGHT IT!
IF THE SAME SIGNAL TO OPEN OR LOCK THE DOORS WOULD BE SENT EACH TIME, IT WOULD BE EASY TO INTERCEPT AND RECORD IT. LATER YOU COULD STEAL THE CAR BY SIMPLY PLAYING IT BACK. THAT'S WHY CRYPTOGRAPHY IS NEEDED.
GOOD THAT WE ACTUALLY USE A KEY WITH ENCRYPTION TO OPERATE OUR SMART DAM.
WELL, THAT IS NOT ENOUGH, SINCE IT COULD BE STILL CRACKED WITH IMPLEMENTATION ATTACKS.
SOMEONE WITH ACCESS TO THE KEY FOB COULD MEASURE ITS POWER CONSUMPTION IN A LAB BY PRESSING THE BUTTON SEVERAL TIMES.
THE COLLECTED TRACES FROM THE SIDE CHANNEL CAN BE ANALYZED WITH STATISTICAL TOOLS. THEREBY, THE SECRET KEY OF THE UNDERLYING CRYPTOGRAPHIC ALGORITHM CAN BE EXTRACTED.

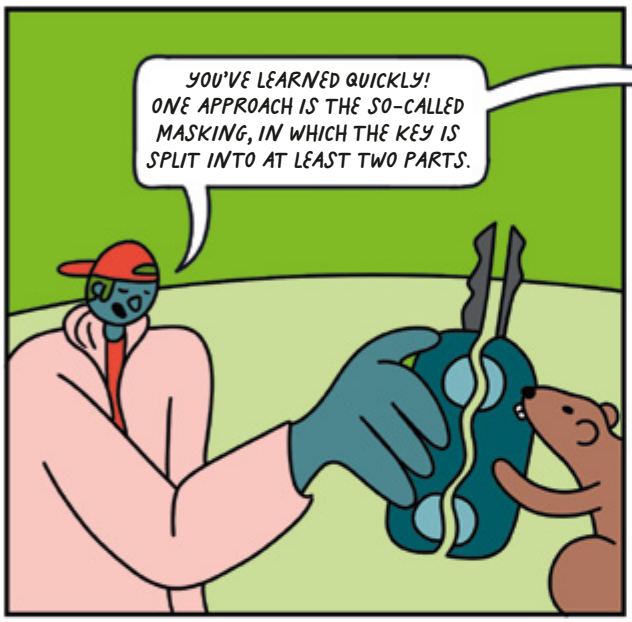


REAL LIFE STORY

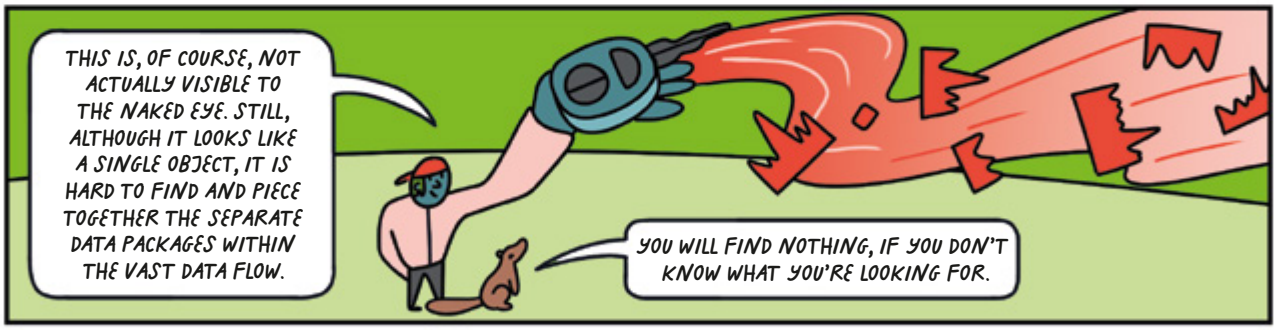
As an experiment, researchers from Ruhr University Bochum (RUB) managed to modify and extract information from the University Mensa cards. First, they found out which chip was used in the card. By measuring the electromagnetic emanations produced while using the card for contactless payments, they discovered that all cards used an identical secret key. Consequently, it was relatively easy to reveal the information stored on the cards. With knowledge of the key and its content, it was possible to manipulate any card's credit balance within a fraction of a second. Finally, missing security measures in the system's backend made it very easy to pay with such manipulated cards.



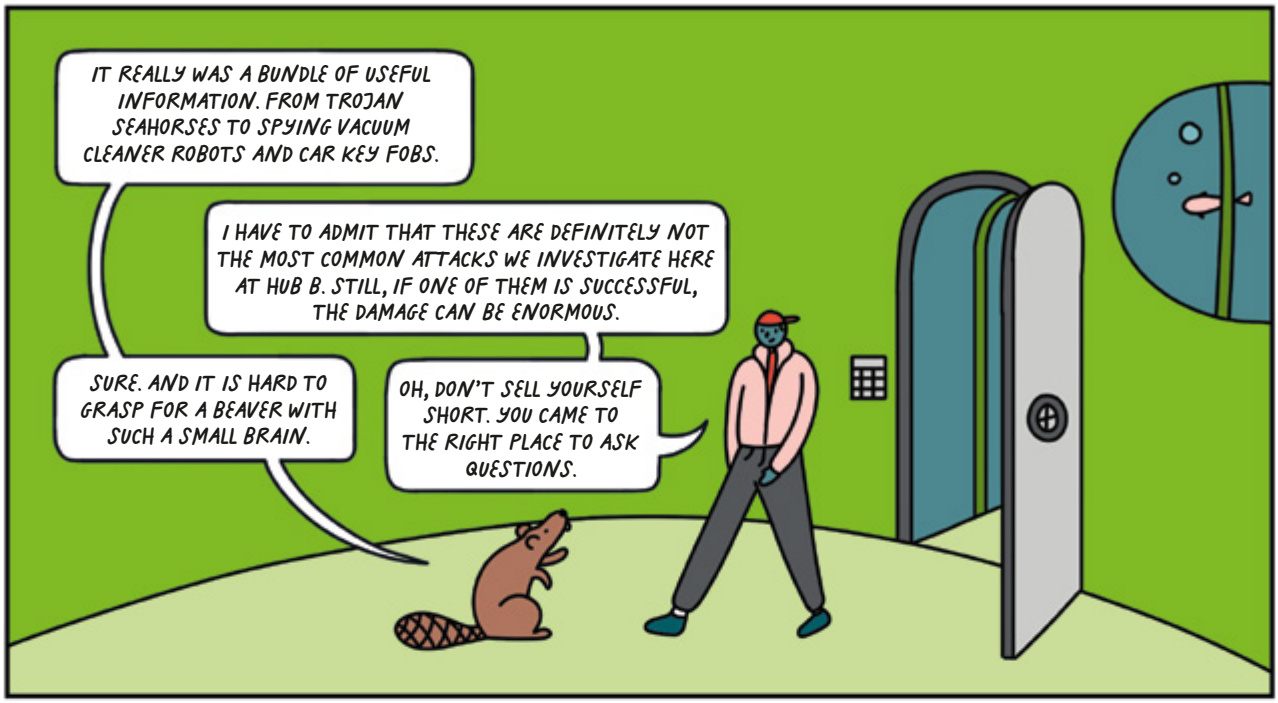

IN RESEARCH CHALLENGE 6, WE TRY TO PROVIDE SOLUTIONS AGAINST SUCH ATTACKS. THIS COULD HELP THE MANUFACTURERS TO DEVELOP COUNTERMEASURES TO PROTECT THE KEY FOBS.
MORE PRECISELY, TO PROTECT THE IMPLEMENTATION OF UNDERLYING CRYPTOGRAPHIC ALGORITHMS INSIDE THE KEY FOBS, RIGHT?


YOU'VE LEARNED QUICKLY! ONE APPROACH IS THE SO-CALLED MASKING, IN WHICH THE KEY IS SPLIT INTO AT LEAST TWO PARTS.

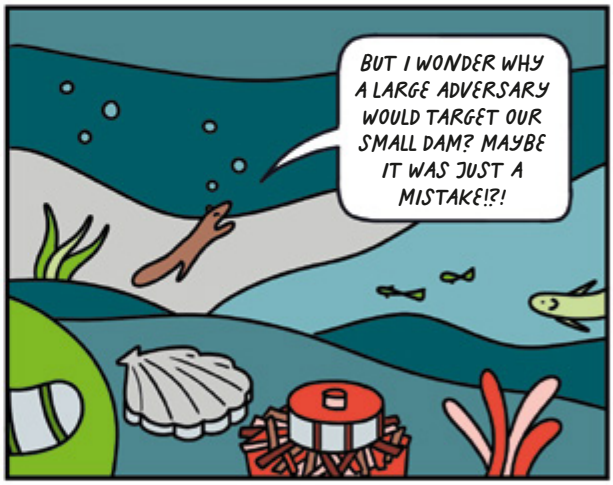

SO THE ATTACKER CAN ONLY STEAL ONE PART OF THE KEY AT A TIME. BY THE TIME HE TRIES TO FIND THE OTHER PART OF THE KEY, THE PARTS HAVE ALREADY BEEN CHANGED. SO THE PARTS HE HAS STOLEN WILL NOT FIT TOGETHER.
LIKE IN A MASKED BALL.


THIS IS, OF COURSE, NOT ACTUALLY VISIBLE TO THE NAKED EYE. STILL, ALTHOUGH IT LOOKS LIKE A SINGLE OBJECT, IT IS HARD TO FIND AND PIECE TOGETHER THE SEPARATE DATA PACKAGES WITHIN THE VAST DATA FLOW.
YOU WILL FIND NOTHING, IF YOU DON'T KNOW WHAT YOU'RE LOOKING FOR.


SO, THIS WAS THE LAST OF OUR THREE CHALLENGES AT HUB B. IT WAS A LOT, I KNOW, BUT I HOPE YOU GOT SOME INSPIRATION ON HOW TO SOLVE THE CHALLENGES WITH YOUR DAM.
MORE THAN THAT! STILL, I HAVE TO PROCESS IT ALL FIRST.


IT REALLY WAS A BUNDLE OF USEFUL INFORMATION. FROM TROJAN SEAHORSES TO SPYING VACUUM CLEANER ROBOTS AND CAR KEY FOBS.
I HAVE TO ADMIT THAT THESE ARE DEFINITELY NOT THE MOST COMMON ATTACKS WE INVESTIGATE HERE AT HUB B. STILL, IF ONE OF THEM IS SUCCESSFUL, THE DAMAGE CAN BE ENORMOUS.
SURE. AND IT IS HARD TO GRASP FOR A BEAVER WITH SUCH A SMALL BRAIN.
OH, DON'T SELL YOURSELF SHORT. YOU CAME TO THE RIGHT PLACE TO ASK QUESTIONS.


OH MAN! I HAVE A LOT TO DO WHEN I GET HOME. SO MANY POTENTIAL LOOPHOLES TO CHECK.


BUT I WONDER WHY A LARGE ADVERSARY WOULD TARGET OUR SMALL DAM? MAYBE IT WAS JUST A MISTAKE!?!


HEY YOU, SLACKER! WE HAVE A SERIOUS PROBLEM, AND YOU'RE BROWSING THE NEWEST TRASH MAGAZINE?
IT IS THE SPECIAL ISSUE OF THE SCIENCE MAGAZINE RUBIN ON IT SECURITY.
BUT WHAT ABOUT THE DAM?


IT TURNED OUT THAT OUR SCRIPT-KIDDIES WERE TINKERING WITH THE HARDWARE. AFTER NOTICING THEY DAMAGED IT, THEY MADE A RESPONSIBLE DISCLOSURE TO ME. MUCH ADO ABOUT ALMOST NOTHING.
WELL, AT LEAST WE CAN NOW PREPARE OURSELVES AGAINST ANY SERIOUS ATTACKS IN THE FUTURE...

ABOUT CASA

CASA: Cyber Security in the Age of Large-Scale Adversaries was established in 2019. It is the only Cluster of Excellence in the field of computer security in Germany. CASA is funded by a grant from the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) worth about 30 million Euros, which ensures excellent research conditions.

CASA brings together a core group of principal investigators, chosen with a strong focus on security and privacy, with selected top-level researchers from highly relevant neighboring disciplines. The team covers the full scope needed to tackle the challenging research problems in modern computer security; namely computer science, mathematics, electrical engineering, and psychology.

CASA is hosted by the Horst Görtz Institute for IT Security (hgi.rub.de/en), a pioneering research center in Germany. Furthermore, CASA collaborates strongly with the Max Planck Institute for Security and Privacy in Bochum (mpi-sp.org) and several other institutes and universities.

What is a "Cluster of Excellence"?
With the funding line "Clusters of Excellence", internationally competitive research centers at universities or university alliances in Germany are provided with project-based funding for a period of 7 years. Within the clusters, scientists from different disciplines and institutions work together on a research project. The funding gives them the opportunity to concentrate intensively on their research goal, to train young scientists and to recruit international top researchers.

casa.rub.de

TECHNICAL BACKGROUND

The concepts and methods presented in this comic were developed by researchers involved in the Cluster of Excellence CASA. If you are interested in more details, you can find the original publications online. These scientific papers explain the results in more detail. For many publications we also publish the source code and other research artifacts. Please reach out to us, if you have questions: info@casa.rub.de

PUBLICATIONS

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

2nd edition 2024

Editorial team
Annika Gödde (CASA/Ruhr University Bochum)
Niels Jansen (Ellery Studio)
Christof Paar (CASA/Max Planck Institute
for Security and Privacy)
Nils Albartus (Max Planck Institute for Security
and Privacy)
Steffen Becker (CASA/Ruhr University Bochum)
Julian Speith (Max Planck Institute for Security
and Privacy)
Veelasha Moonsamy (CASA/Ruhr University
Bochum)
Stefan Roth (CASA/Ruhr University Bochum)
Aydin Sezgin (CASA/Ruhr University Bochum)
Paul Staat (Max Planck Institute for Security
and Privacy)
Johannes Tobisch (Max Planck Institute for Security
and Privacy)
Tim Güneysu (CASA/Ruhr University Bochum)
Amir Moradi (CASA/Ruhr University Bochum)
Pascal Sasdrich (CASA/Ruhr University Bochum)

Ellery Studio
Illustrations: Lucia Cordero, Hannah Schrage
Design: Dorota Orlof
Project Management: Pawel Leyk

Cover image
Hannah Schrage

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

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

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

Scan to access the digital version of our comic:

Also published in this series:

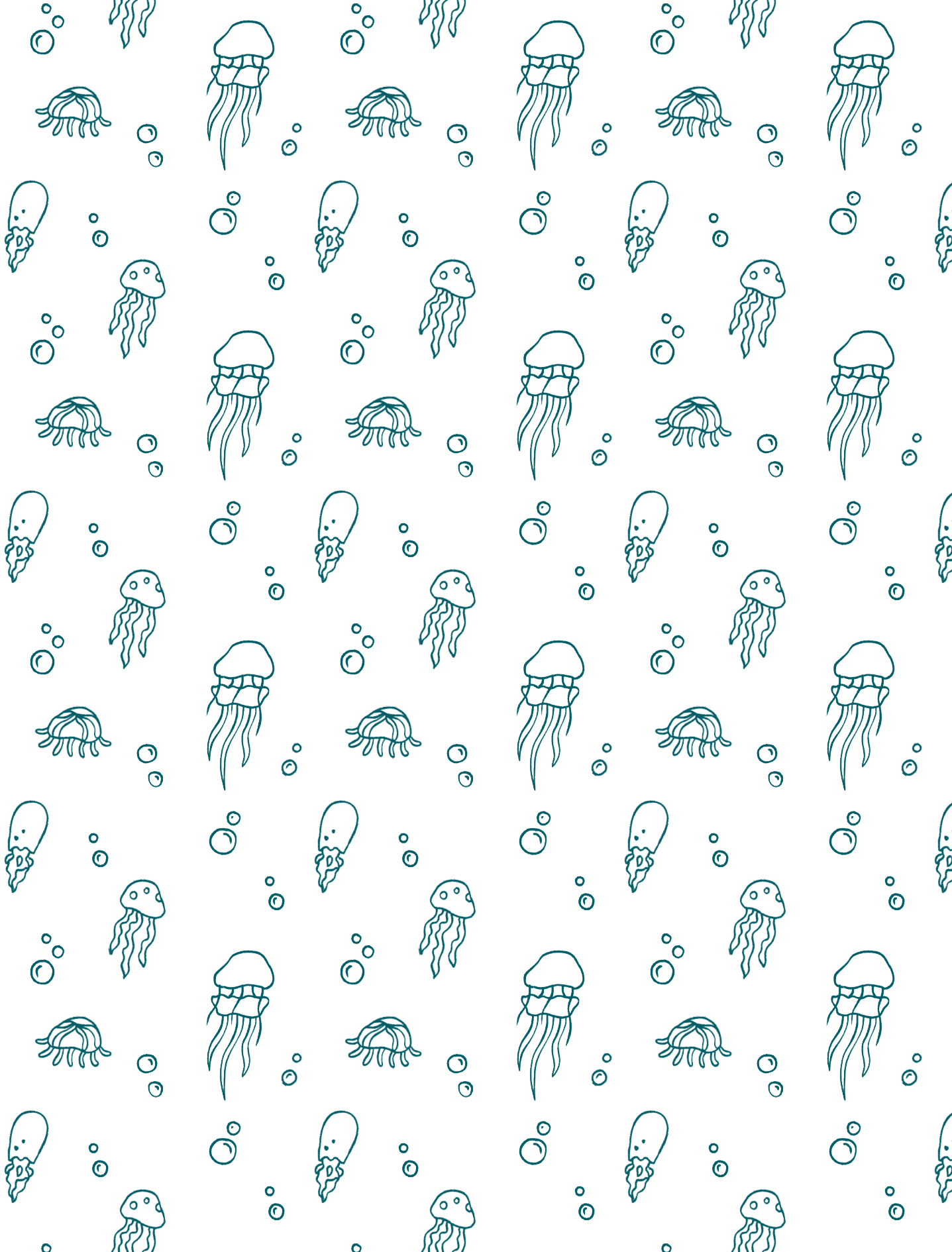
- The Secrets of HUB A
  and the Traces of the Cookies
- What's the Fuzz About HUB C
  and the Missing Carrots?
- HUB D and the Rumble
  in the Jungle of Usability

CASA
Cyber Security in the Age
of Large-Scale Adversaries

Gefördert durch
DFG Deutsche
Forschungsgemeinschaft

RUHR
UNIVERSITÄT
BOCHUM
RUB

ellery
studio




HUB A
HUB B
HUB C
HUB D
FROM HARDWARE TROJANS TO SIDE-CHANNEL ATTACKS, IT HAS BECOME CLEAR THAT HARDWARE CAN ALSO BE THE TARGET OF ATTACKS. AS SYSTEMS FALL INTO THE HANDS OF VARIOUS AND POTENTIALLY MALICIOUS USERS, NUMEROUS OPPORTUNITIES ARISE TO BREACH SUCH SEEMINGLY AND ALLEGEDLY SECURE SYSTEMS.
FOLLOW FEARLESS BEAVER PAUL ON HIS DIVE INTO THE RESEARCH FINDINGS OF CASA'S HUB B. WILL HE SOLVE THE MYSTERY OF HIS FAMILY'S UNSTABLE DAM? HAVE THEY BECOME THE TARGET OF A LARGE-SCALE ADVERSARY?
FIND OUT MORE!