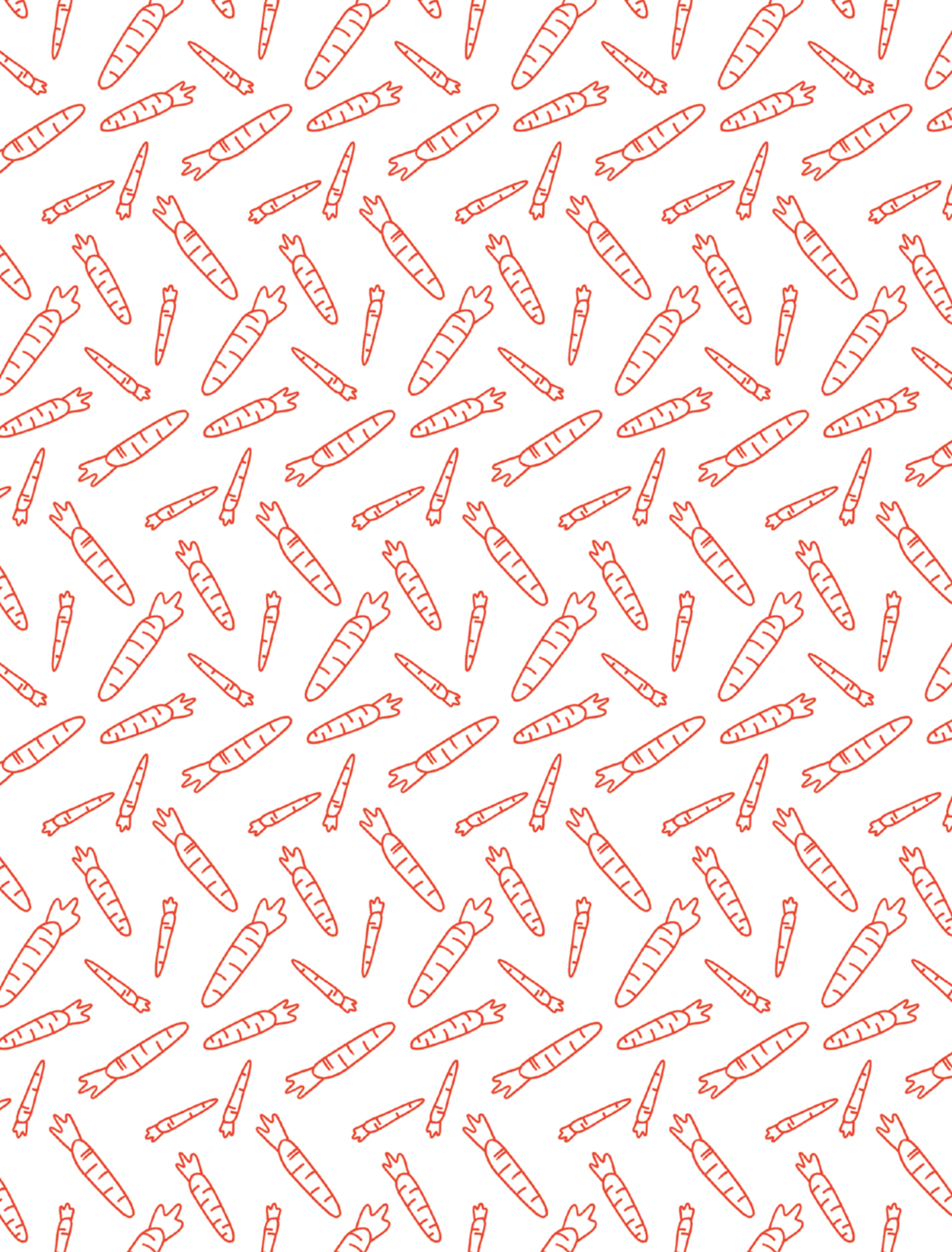
CASA UNIVERSE

# 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



# 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

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.

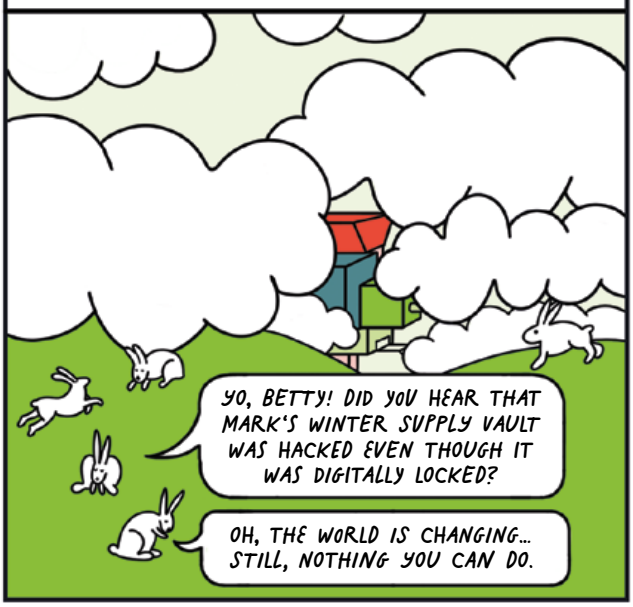
**HUB C** “Secure Systems”: Developing secure and efficient systems at the software level. Machine Learning is one of the many methods used to explore and expand this field.

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

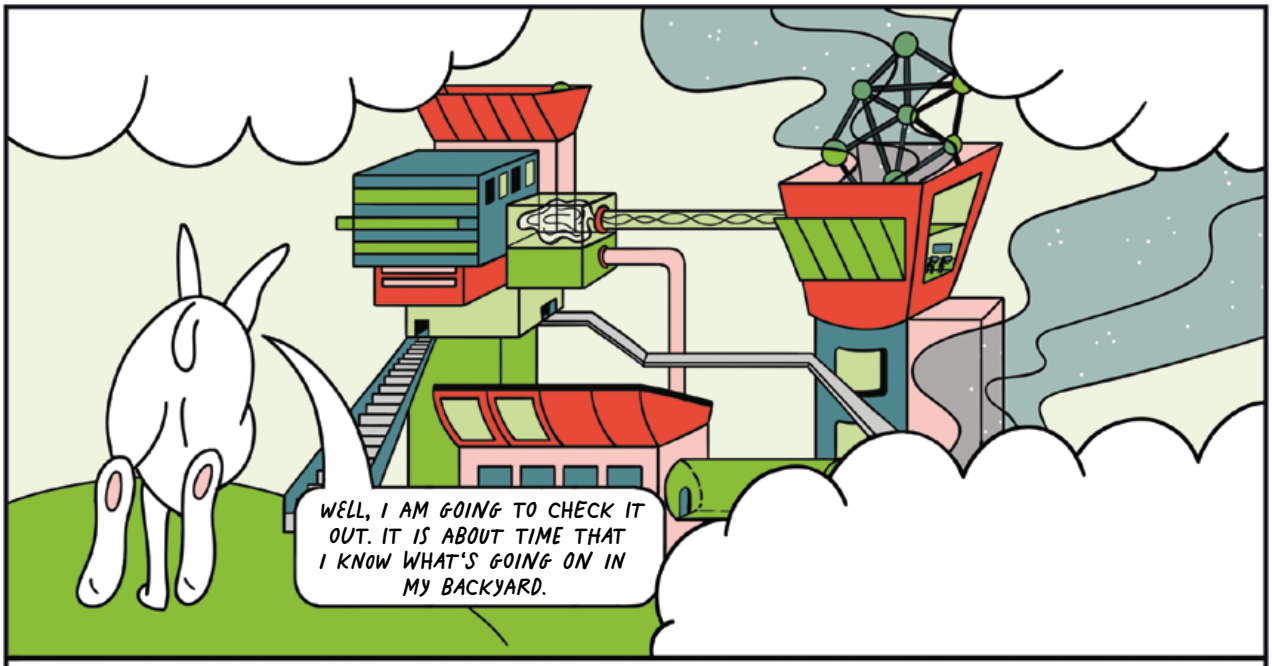
Each HUB addresses specific major research challenges that have been carefully selected to address security issues critical to the protection against large-scale attackers. The challenges of HUB C are:

**Research Challenge 7:** Building Secure Systems
**Research Challenge 8:** Security With Untrusted Components
**Research Challenge 9:** Intelligent Security Systems

It might not be easy to believe, but the calm and beautiful hills of the CASA Universe are located in the world that we know. A world that faces more and more challenges as the rabbit squad – like everyone else – is becoming increasingly digitalized...

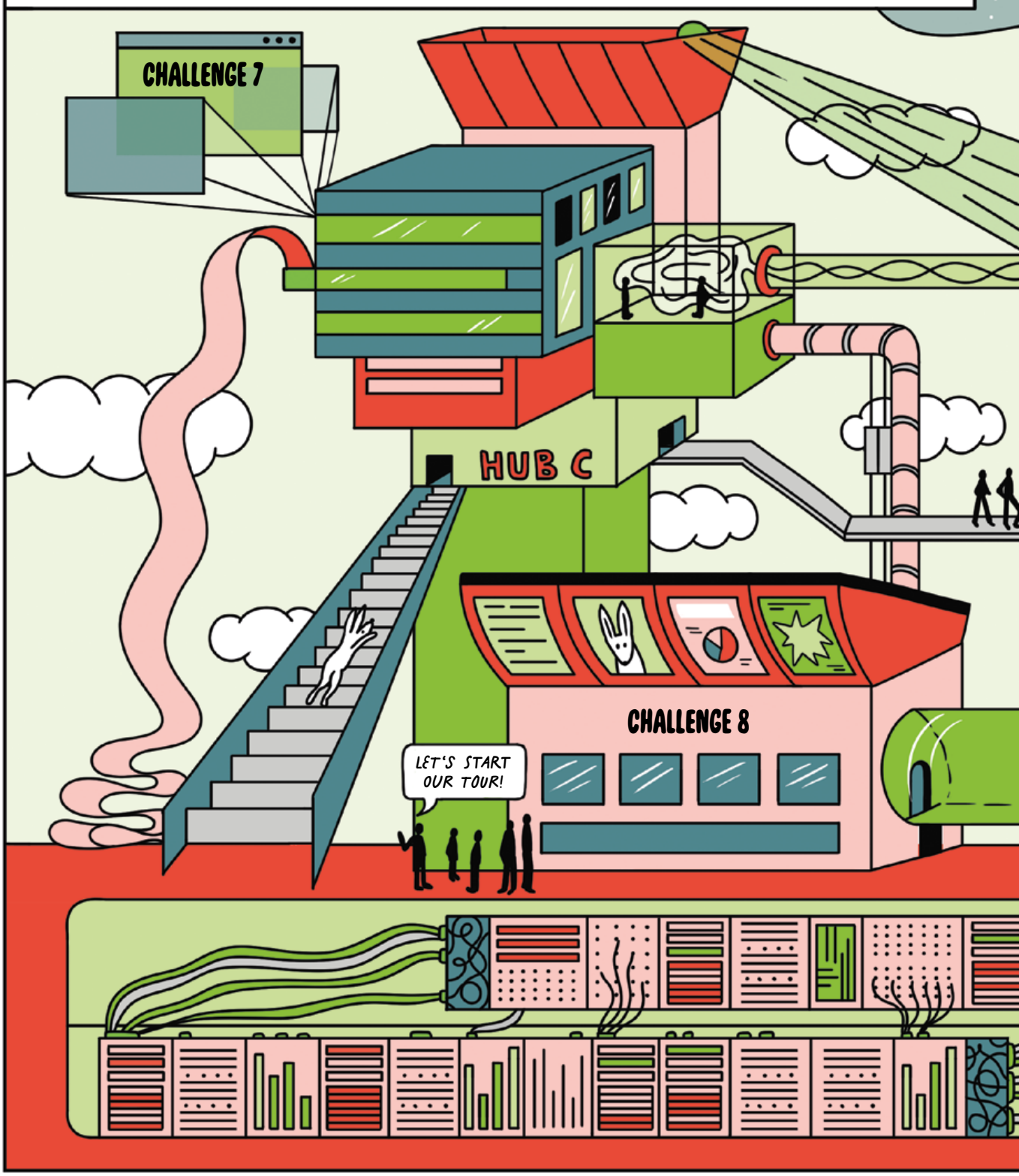


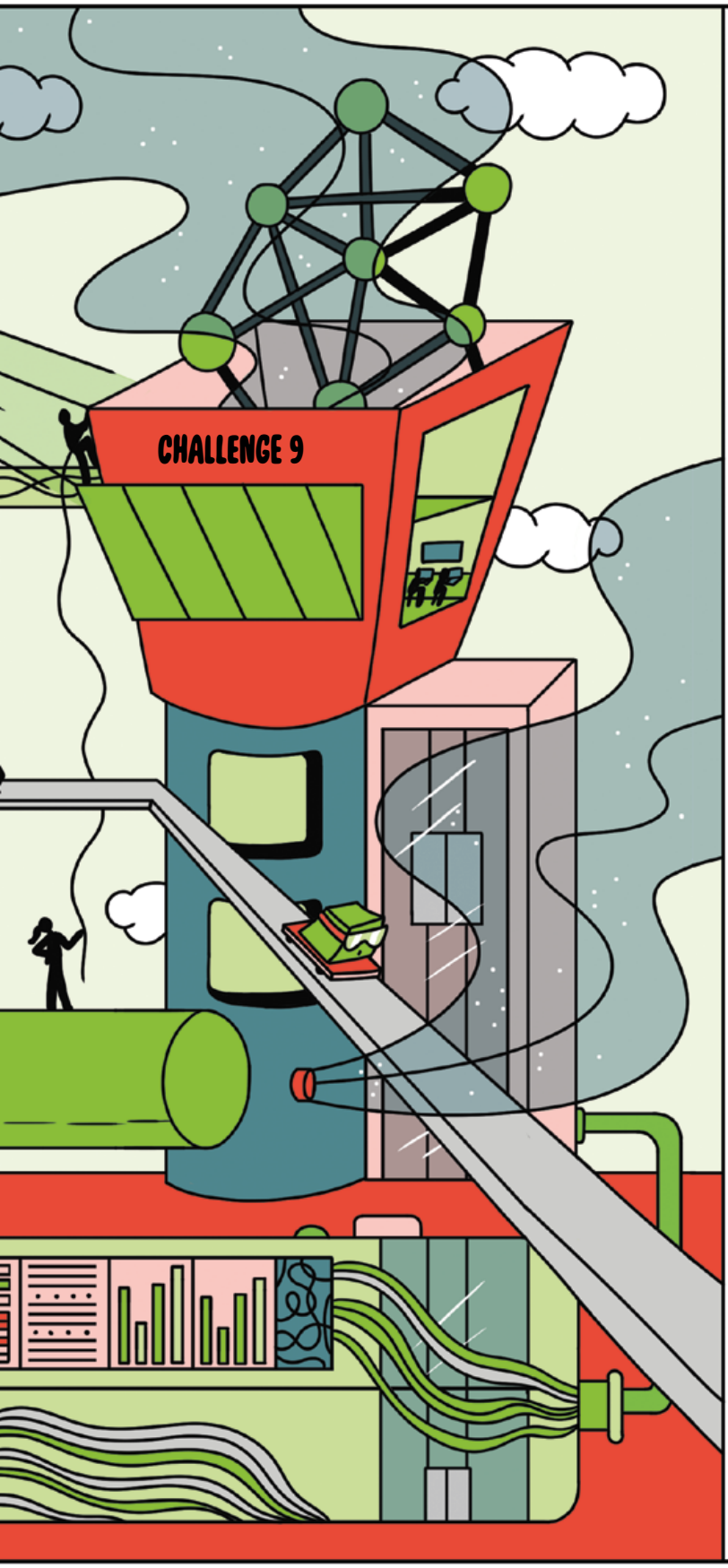

Right in the heart of these hills you can find HUB C, a part of the CASA Universe. Nobody really knows what's happening there. Some say they are working on novel secure systems, others say they want to make older ones resilient. Everyone seems to agree that they are working on some hot stuff.


Brave bunny Betty decides that she wants to find out what is really happening there. She wants to acquire more knowledge so that what happened to Mark wouldn't happen to her and the rest of the herd. They urgently need their winter supply.

# WELCOME TO RESEARCH HUB C






# Content



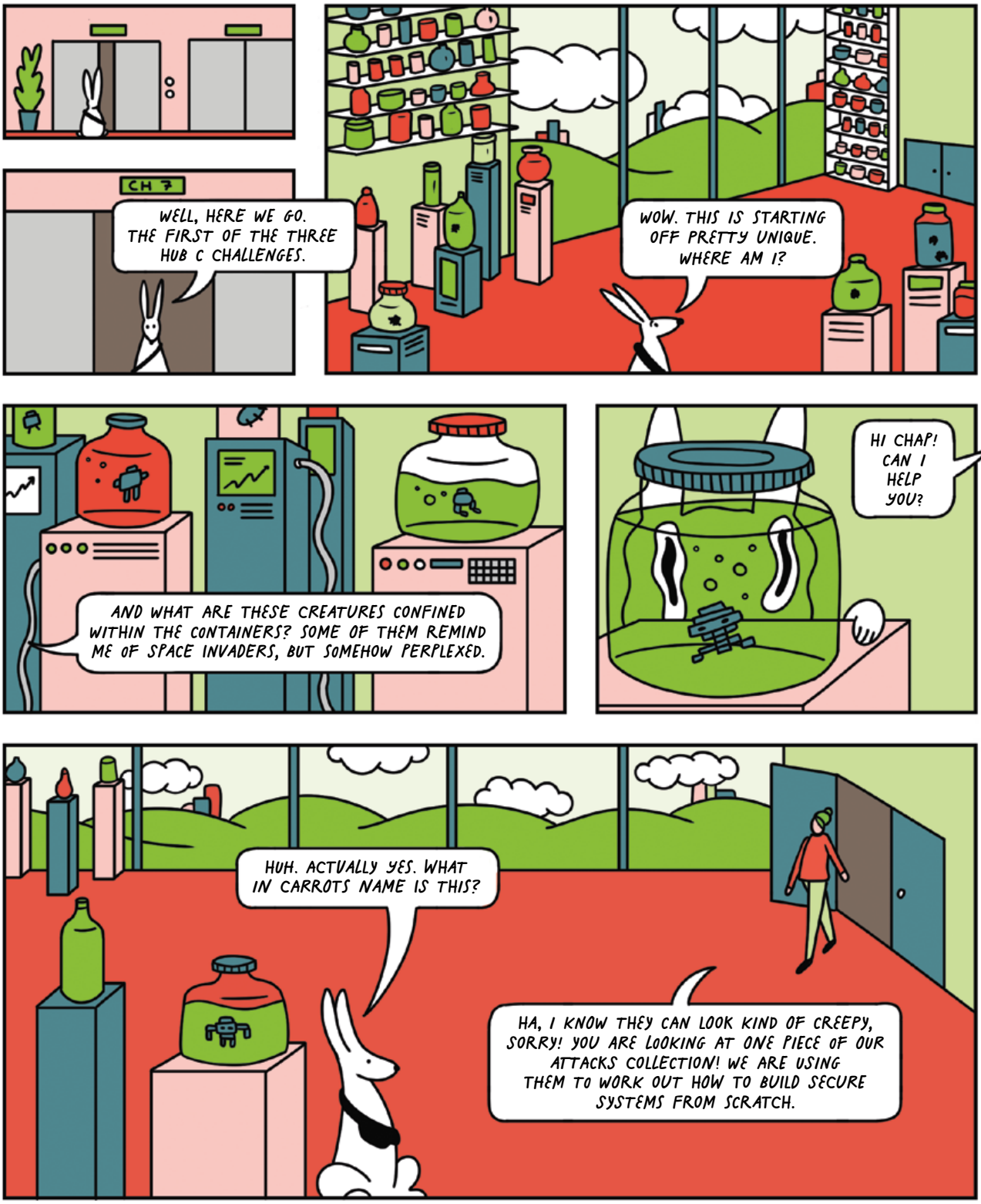
### CASA BACKGROUND

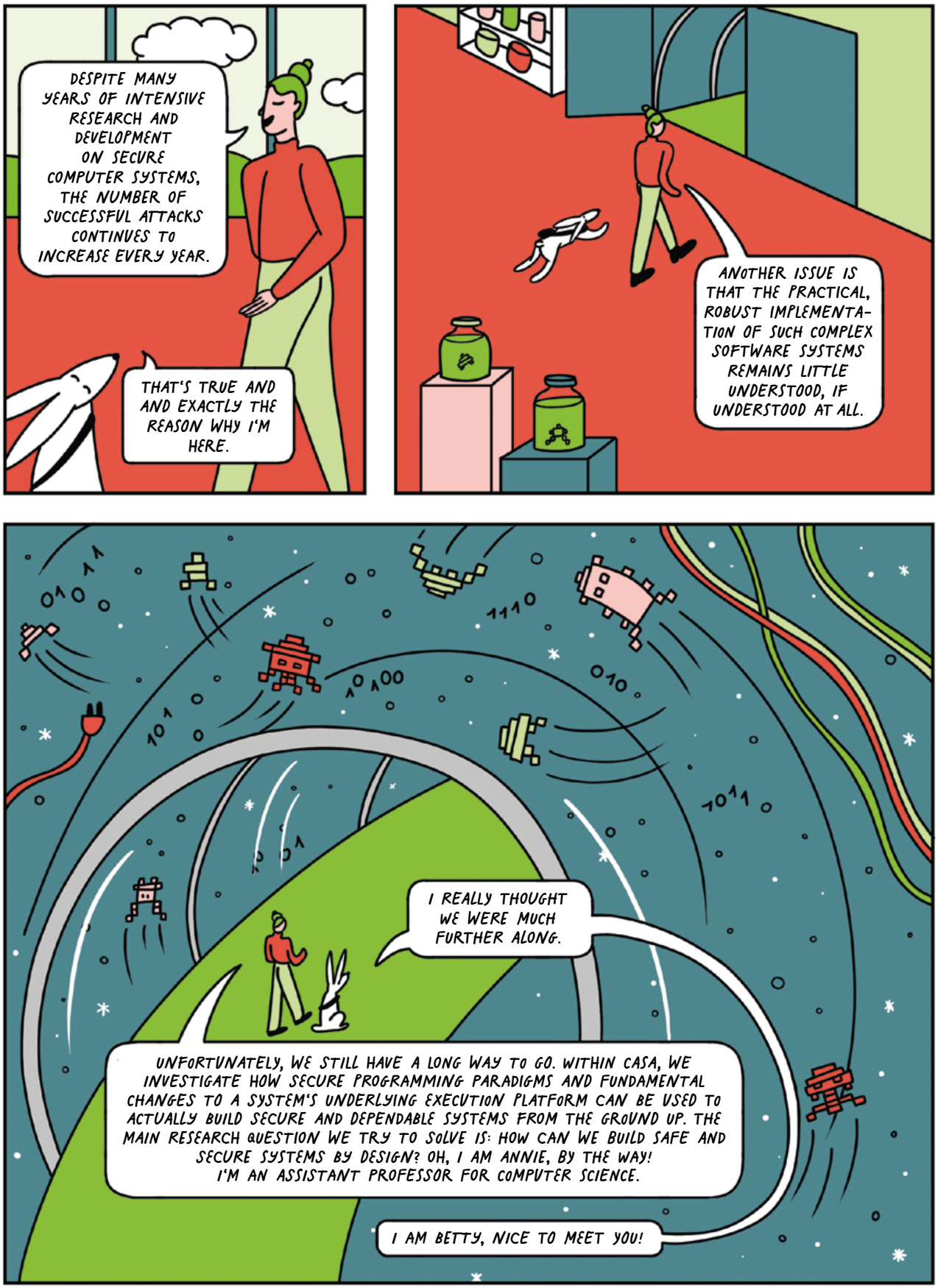
CASA stands for ‘Cyber Security in the Age of Large-Scale Adversaries’ and is funded as a Cluster of Excellence (EXC) within the Excellence Strategy of the DFG in Germany. Its goal is to enable sustainable security against sophisticated large-scale attacks. Therefore, an interdisciplinary team explores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

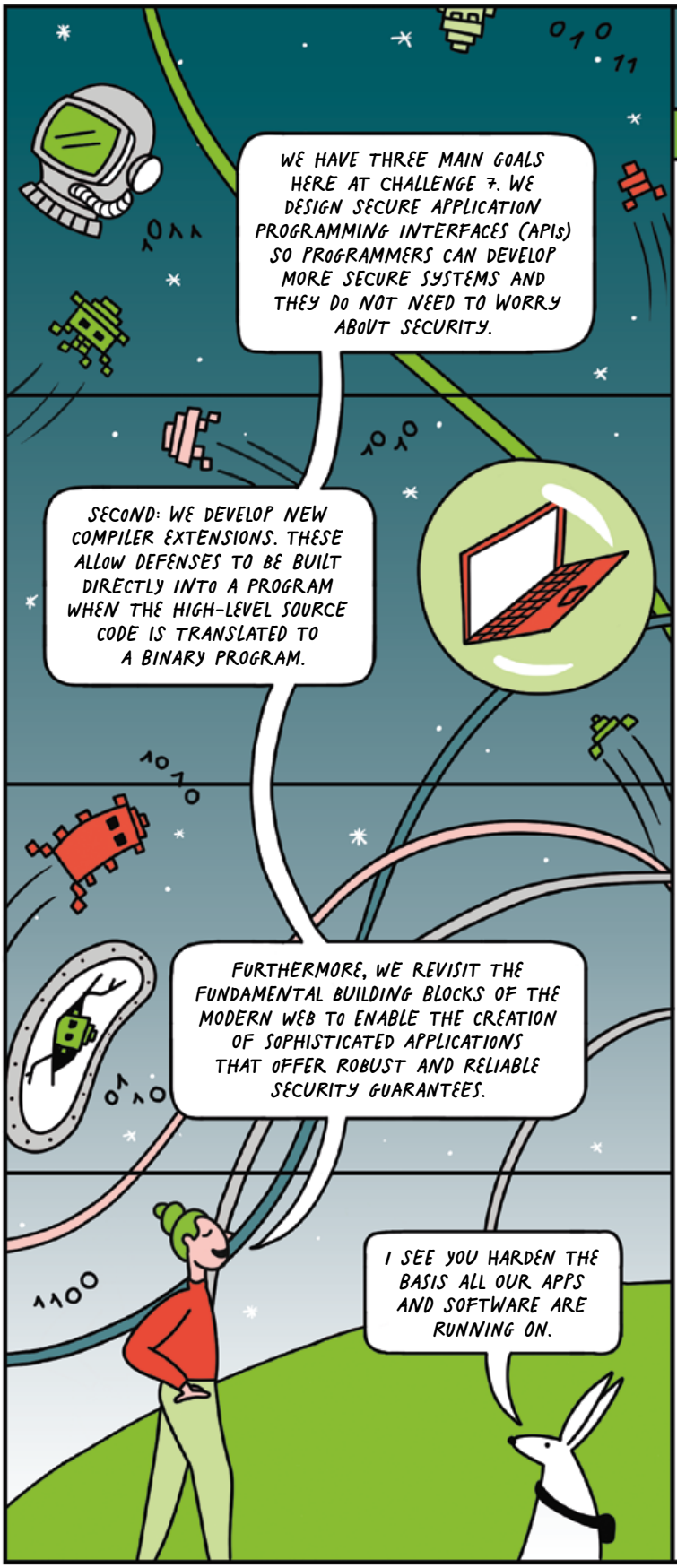
https://casa.rub.de

# CHALLENGE 7

# BUILDING SECURE SYSTEMS




DESPITE MANY YEARS OF INTENSIVE RESEARCH AND DEVELOPMENT ON SECURE COMPUTER SYSTEMS, THE NUMBER OF SUCCESSFUL ATTACKS CONTINUES TO INCREASE EVERY YEAR.
THAT'S TRUE AND AND EXACTLY THE REASON WHY I'M HERE.
ANOTHER ISSUE IS THAT THE PRACTICAL, ROBUST IMPLEMENTATION OF SUCH COMPLEX SOFTWARE SYSTEMS REMAINS LITTLE UNDERSTOOD, IF UNDERSTOOD AT ALL.
I REALLY THOUGHT WE WERE MUCH FURTHER ALONG.
UNFORTUNATELY, WE STILL HAVE A LONG WAY TO GO. WITHIN CASA, WE INVESTIGATE HOW SECURE PROGRAMMING PARADIGMS AND FUNDAMENTAL CHANGES TO A SYSTEM'S UNDERLYING EXECUTION PLATFORM CAN BE USED TO ACTUALLY BUILD SECURE AND DEPENDABLE SYSTEMS FROM THE GROUND UP. THE MAIN RESEARCH QUESTION WE TRY TO SOLVE IS: HOW CAN WE BUILD SAFE AND SECURE SYSTEMS BY DESIGN? OH, I AM ANNIE, BY THE WAY! I'M AN ASSISTANT PROFESSOR FOR COMPUTER SCIENCE.
I AM BETTY, NICE TO MEET YOU!



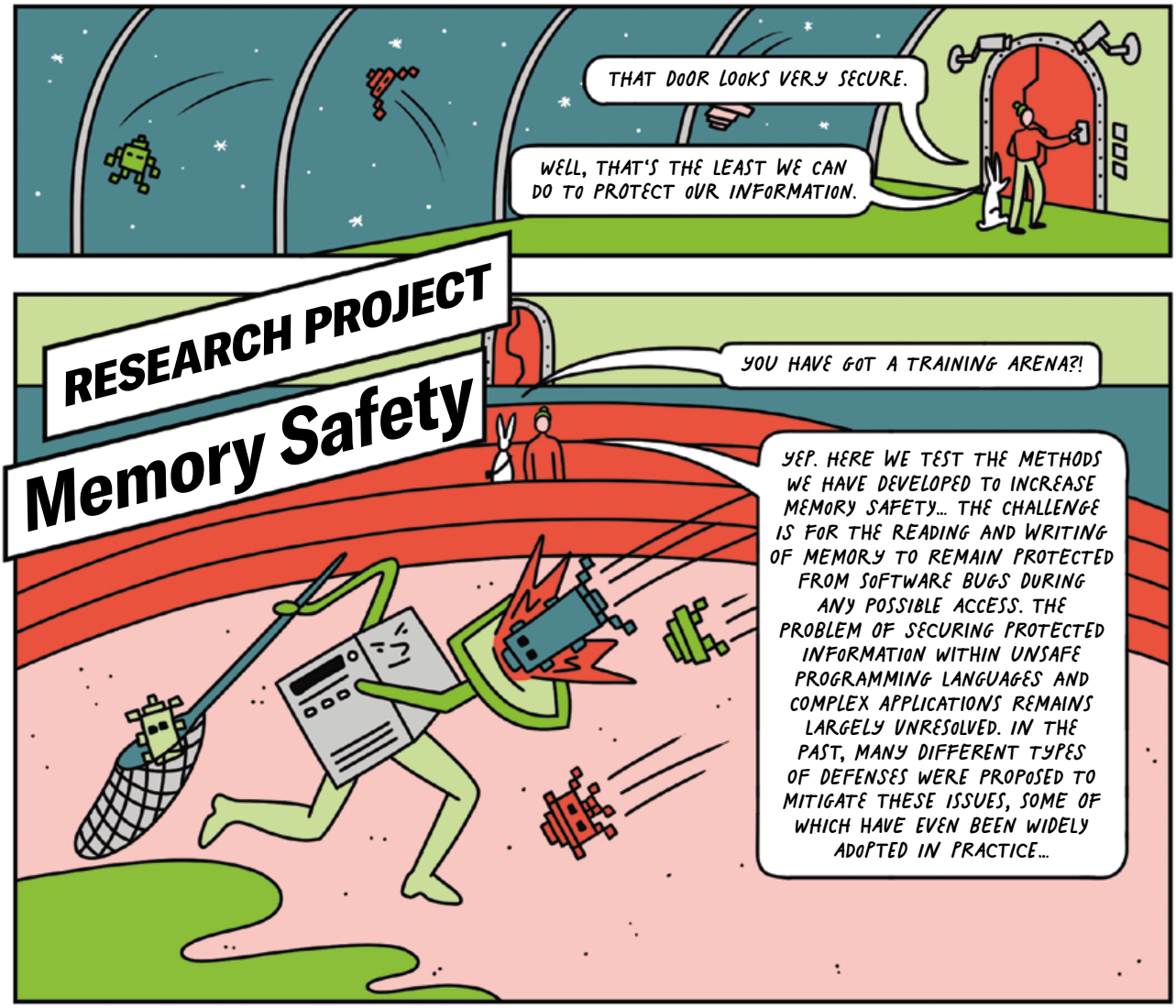

# CASA WIKI

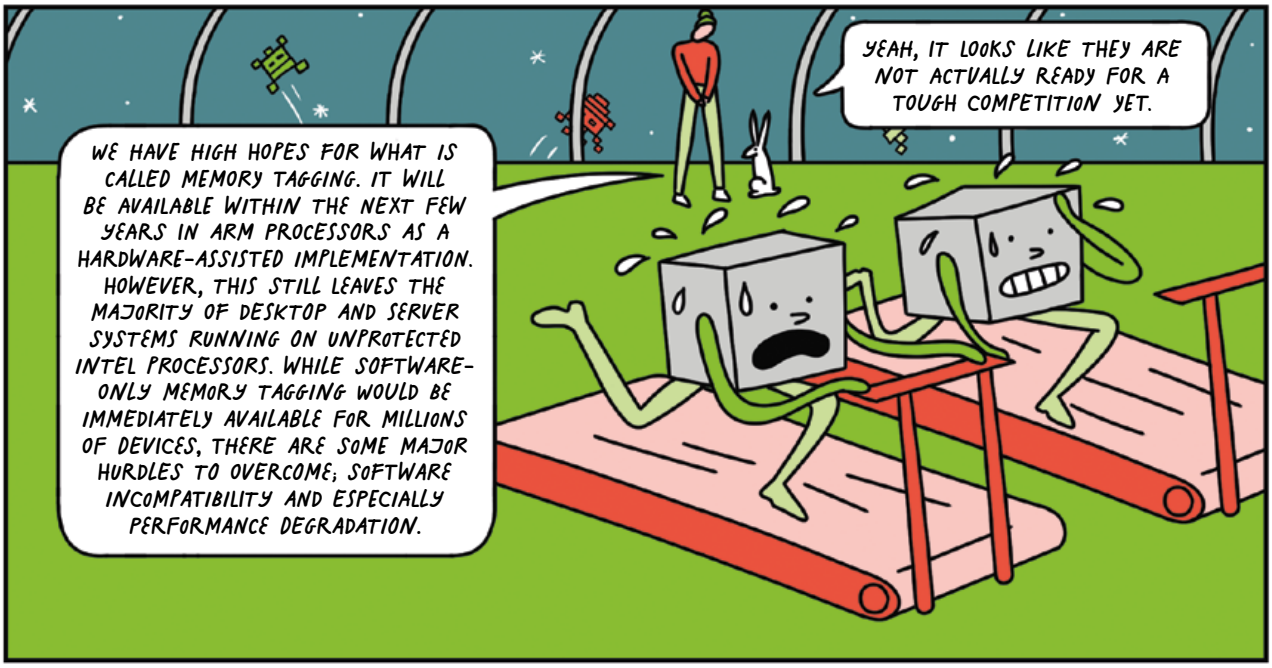
An **Application Programming Interface** (or API) is an interface that allows two programs to communicate with each other in a standardized manner. This transfer of data and commands is structured according to a defined syntax.

A program executed by a computer consists of only two different characters – the 0 and the 1 – which is why it is called a binary program. A **Compiler** is a program that translates the source code written in a high-level programming language (such as Java or C/C++) into the machine-readable binary language. The result is "executable code" which the computer can then interpret and execute.

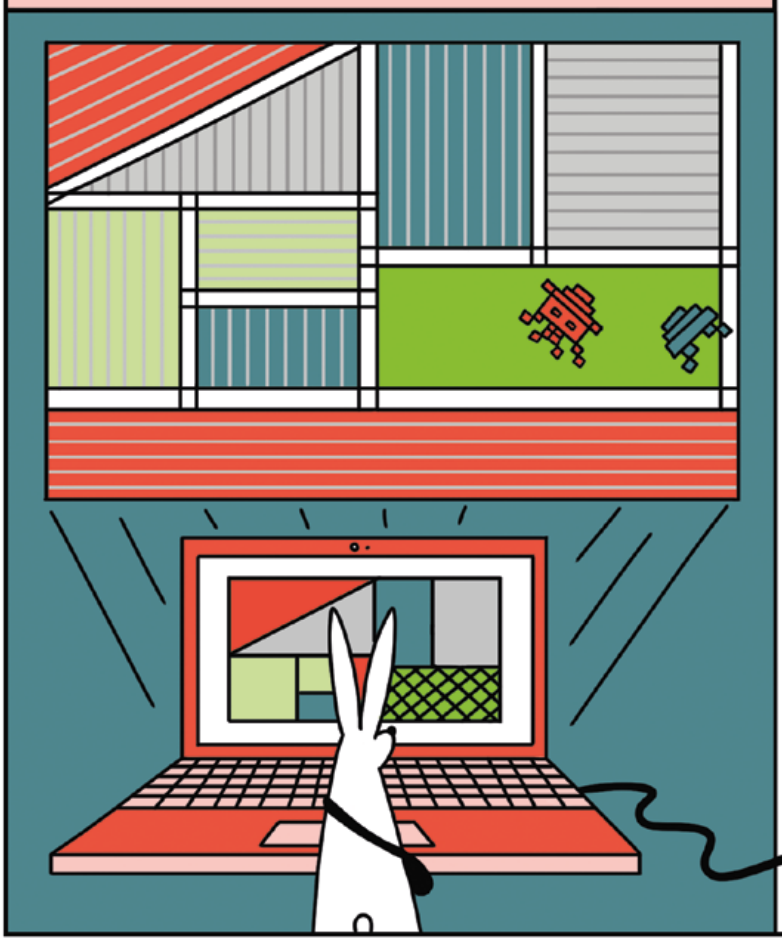
A **Central Processing Unit** (CPU), often called a processor, is the central unit within a computer. The processor coordinates everything and performs arithmetic and logical operations to process data from internal or external sources, such as the main memory. There are CPUs from different manufacturers, such as Intel, AMD, or ARM.

In practice, we observe many successful attacks against various targets, such as the German Bundestag, large companies, or political activists. A recent example is the **Pegasus spyware**, which can be secretly installed on mobile phones by exploiting a security vulnerability. Among other dangerous activities, Pegasus is able to read text messages, track calls, and steal private information from a compromised phone.

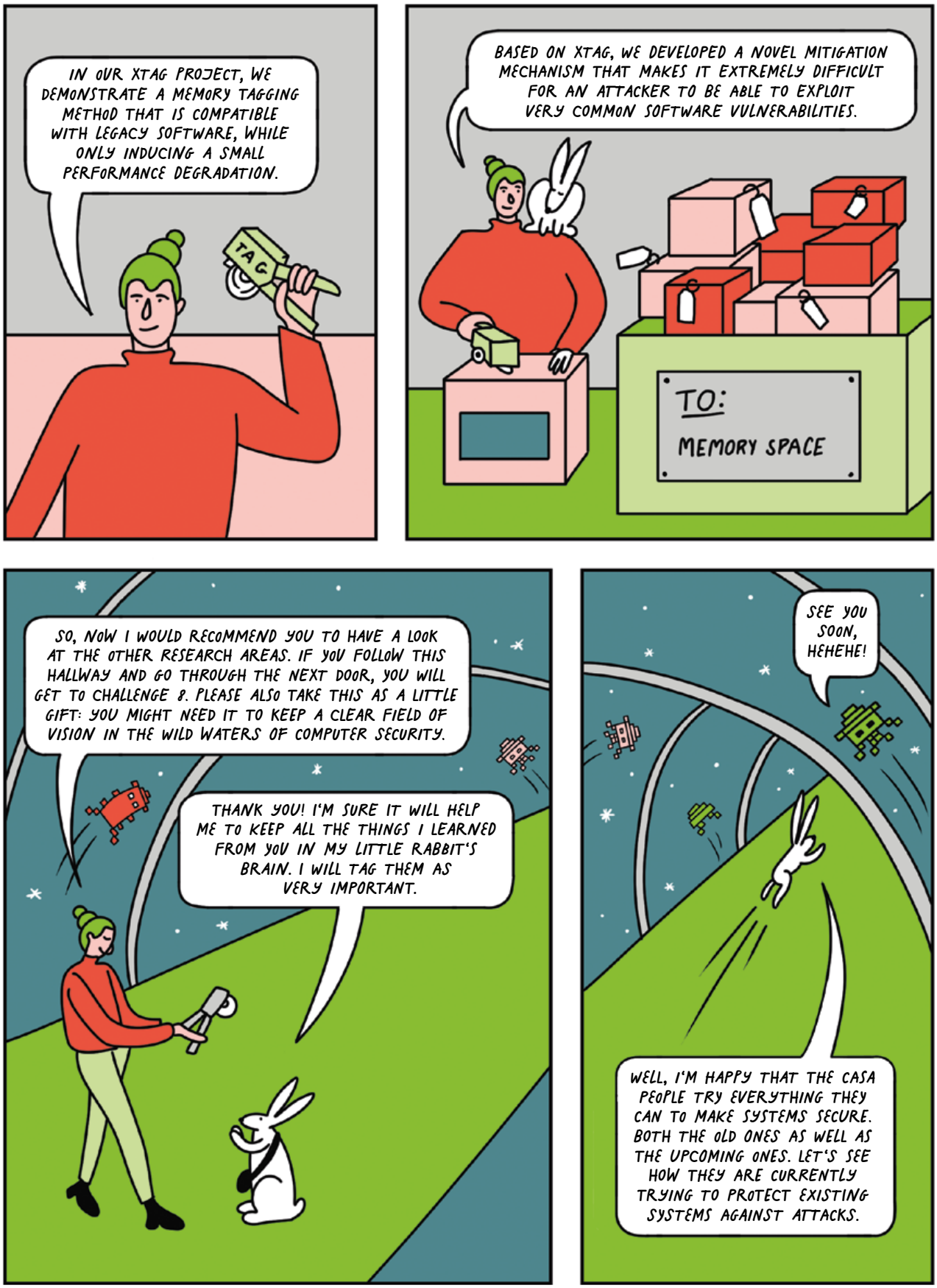

THAT DOOR LOOKS VERY SECURE.
WELL, THAT'S THE LEAST WE CAN DO TO PROTECT OUR INFORMATION.
RESEARCH PROJECT
Memory Safety
YOU HAVE GOT A TRAINING ARENA?!
YEP. HERE WE TEST THE METHODS WE HAVE DEVELOPED TO INCREASE MEMORY SAFETY... THE CHALLENGE IS FOR THE READING AND WRITING OF MEMORY TO REMAIN PROTECTED FROM SOFTWARE BUGS DURING ANY POSSIBLE ACCESS. THE PROBLEM OF SECURING PROTECTED INFORMATION WITHIN UNSAFE PROGRAMMING LANGUAGES AND COMPLEX APPLICATIONS REMAINS LARGELY UNRESOLVED. IN THE PAST, MANY DIFFERENT TYPES OF DEFENSES WERE PROPOSED TO MITIGATE THESE ISSUES, SOME OF WHICH HAVE EVEN BEEN WIDELY ADOPTED IN PRACTICE...
...UNFORTUNATELY, ADVANCED ATTACKS ARE STILL ABLE TO BYPASS THESE DEFENSES AND THE ARMS RACE IS NOT OVER (YET).
WITHIN CASA, WE INVESTIGATE HOW THE NEXT GENERATION OF SOFTWARE SYSTEMS CAN BE DESIGNED SO THAT THEY CAN WITHSTAND EVEN THE MOST ADVANCED ATTACKS.
OOOH, THEY ARE SO CUTE!



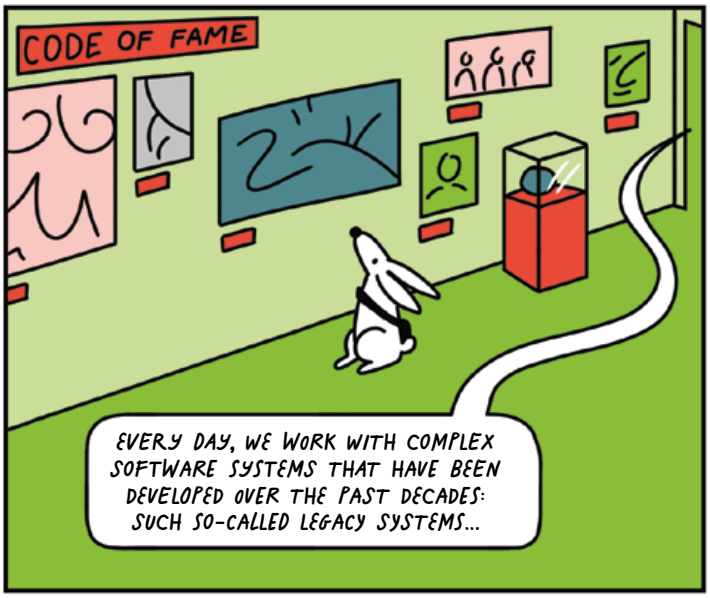

# MEMORY TAGGING



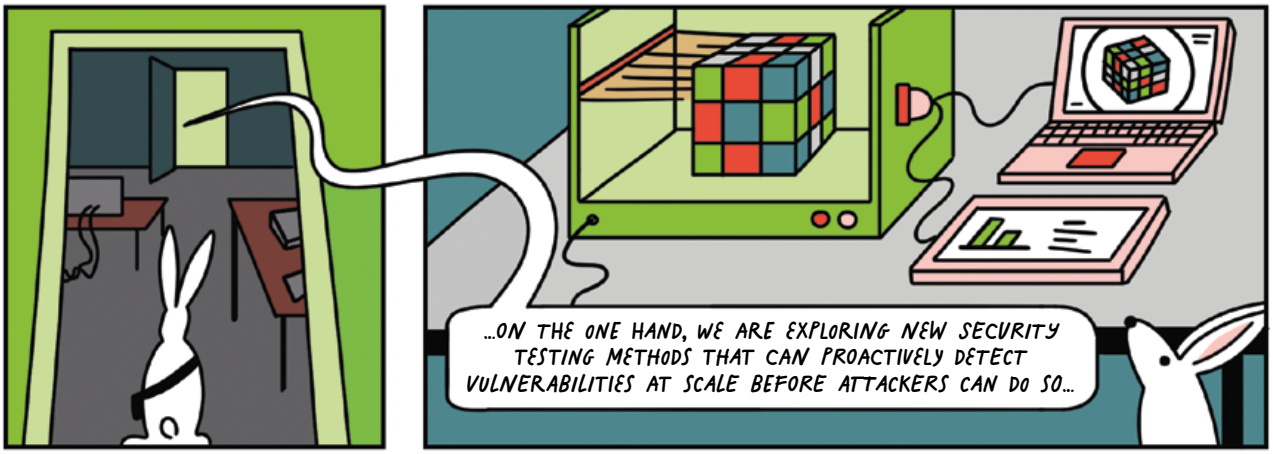
**Memory Tagging** is a promising new mitigation technology. The general idea of memory tagging is to separate the memory space of a program into different areas and then closely track which part of the program can access and modify which part of the memory space. You can think of it like this: The memory space is divided into different areas, which are marked with different colors. During operations on these memory areas, the color is then passed on accordingly – you can observe at runtime how instructions affect the memory. Such precise observation can stop many different kinds of software-based attacks in a generic way.

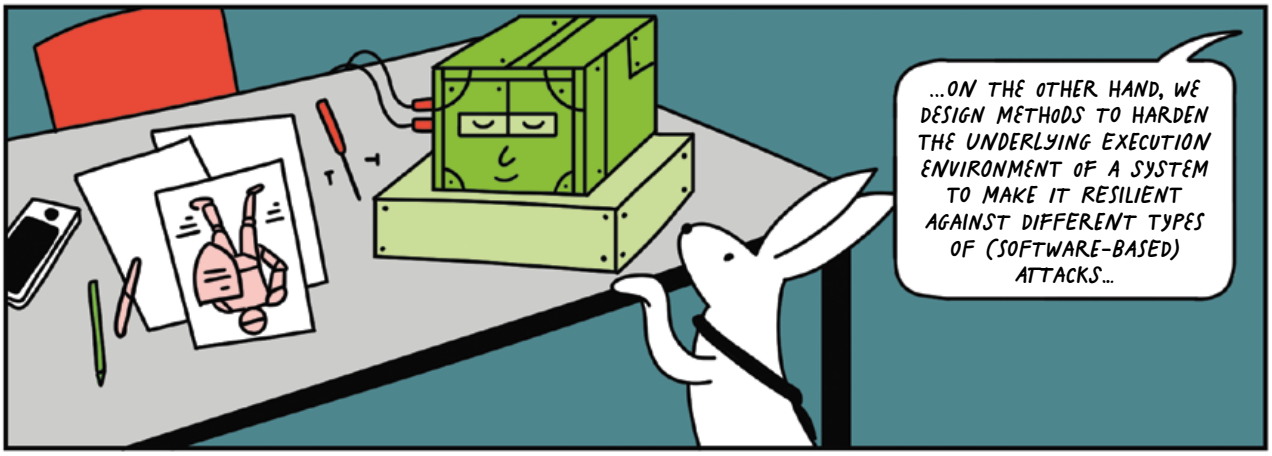

IN OUR XTAG PROJECT, WE DEMONSTRATE A MEMORY TAGGING METHOD THAT IS COMPATIBLE WITH LEGACY SOFTWARE, WHILE ONLY INDUCING A SMALL PERFORMANCE DEGRADATION.
TAG
BASED ON XTAG, WE DEVELOPED A NOVEL MITIGATION MECHANISM THAT MAKES IT EXTREMELY DIFFICULT FOR AN ATTACKER TO BE ABLE TO EXPLOIT VERY COMMON SOFTWARE VULNERABILITIES.
TO:
MEMORY SPACE
SO, NOW I WOULD RECOMMEND YOU TO HAVE A LOOK AT THE OTHER RESEARCH AREAS. IF YOU FOLLOW THIS HALLWAY AND GO THROUGH THE NEXT DOOR, YOU WILL GET TO CHALLENGE 8. PLEASE ALSO TAKE THIS AS A LITTLE GIFT: YOU MIGHT NEED IT TO KEEP A CLEAR FIELD OF VISION IN THE WILD WATERS OF COMPUTER SECURITY.
THANK YOU! I'M SURE IT WILL HELP ME TO KEEP ALL THE THINGS I LEARNED FROM YOU IN MY LITTLE RABBIT'S BRAIN. I WILL TAG THEM AS VERY IMPORTANT.
SEE YOU SOON, HEHEHE!
WELL, I'M HAPPY THAT THE CASA PEOPLE TRY EVERYTHING THEY CAN TO MAKE SYSTEMS SECURE. BOTH THE OLD ONES AS WELL AS THE UPCOMING ONES. LET'S SEE HOW THEY ARE CURRENTLY TRYING TO PROTECT EXISTING SYSTEMS AGAINST ATTACKS.

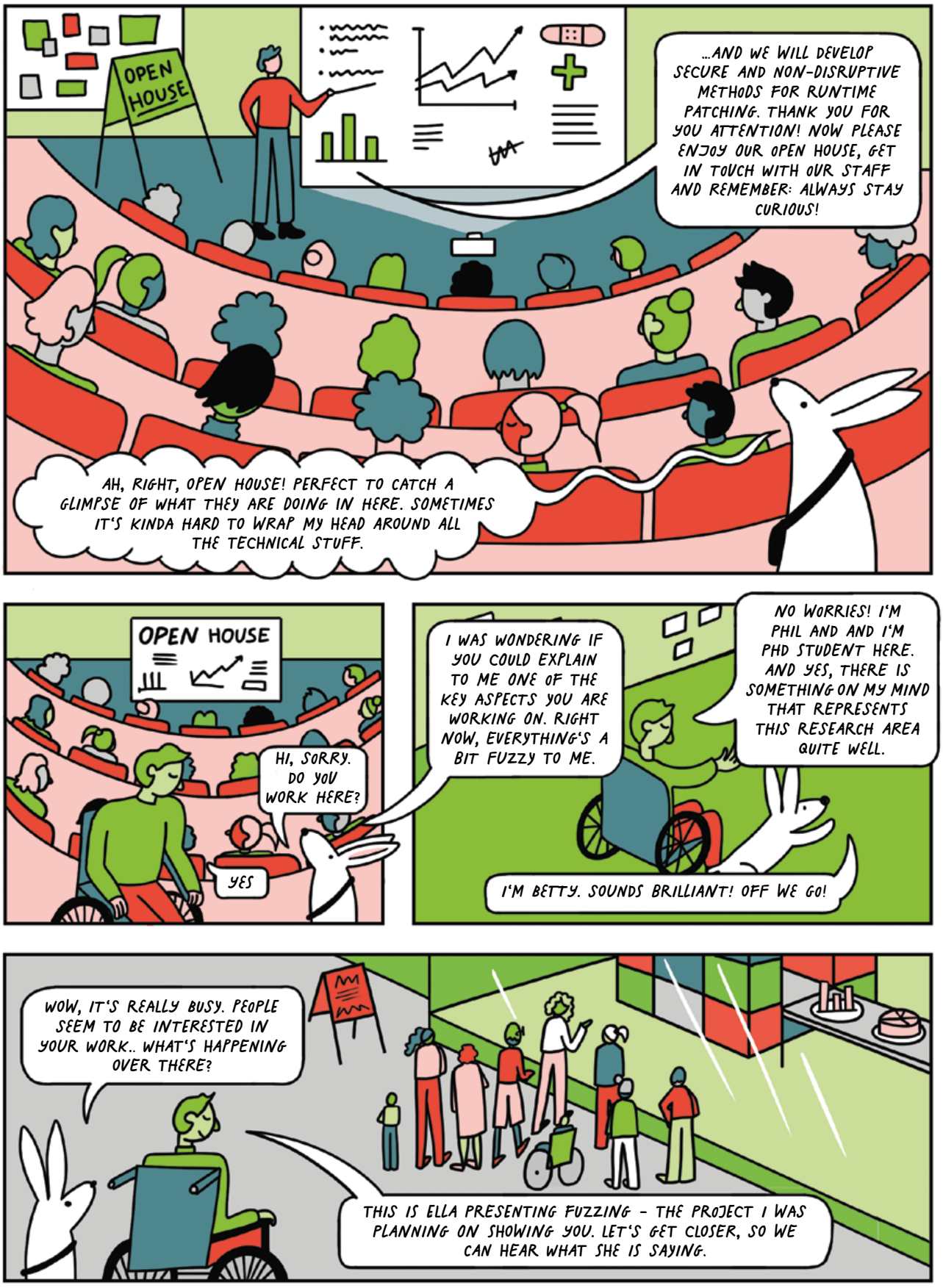
# CHALLENGE 8
# SECURITY with UNTRUSTED COMPONENTS

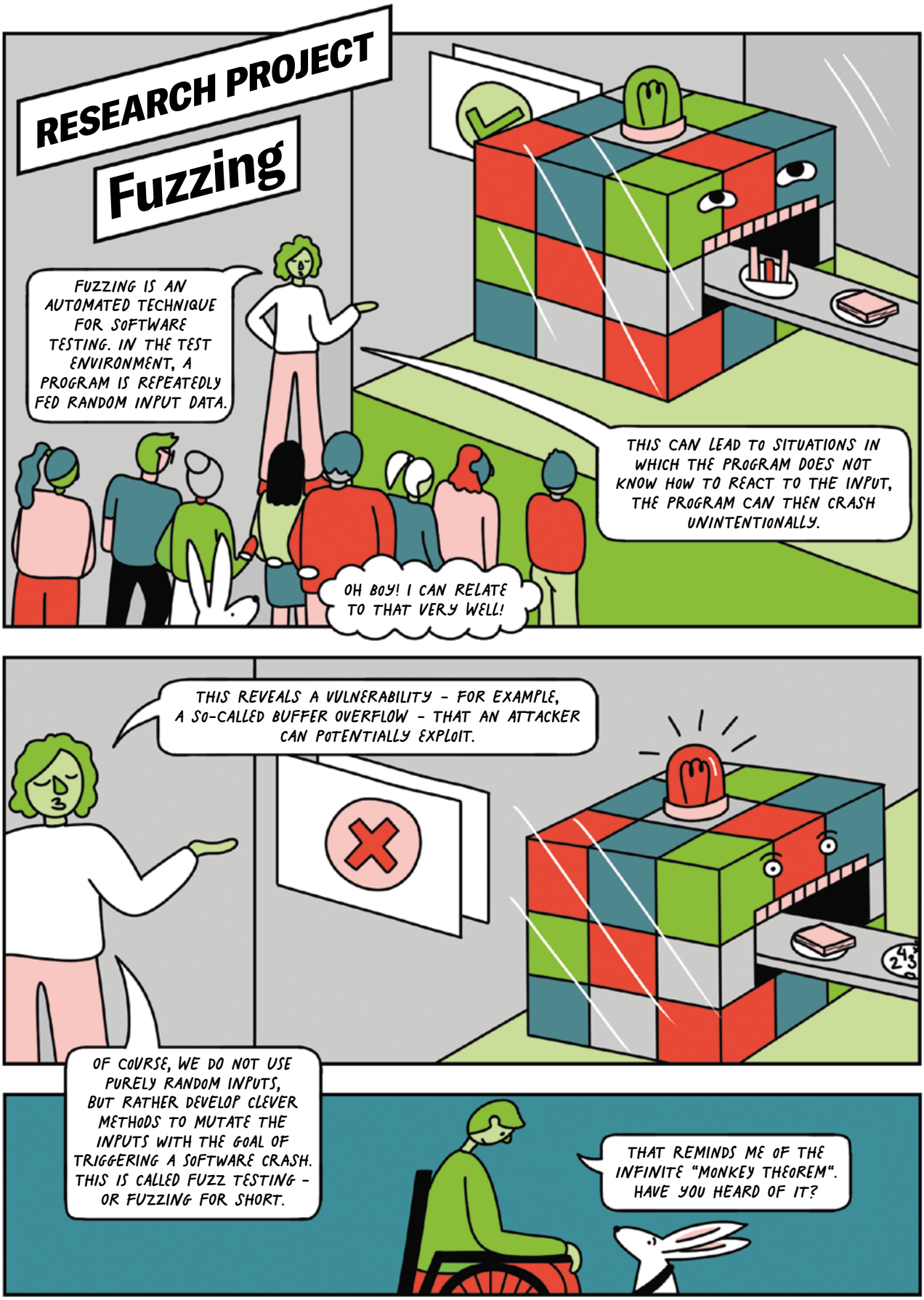




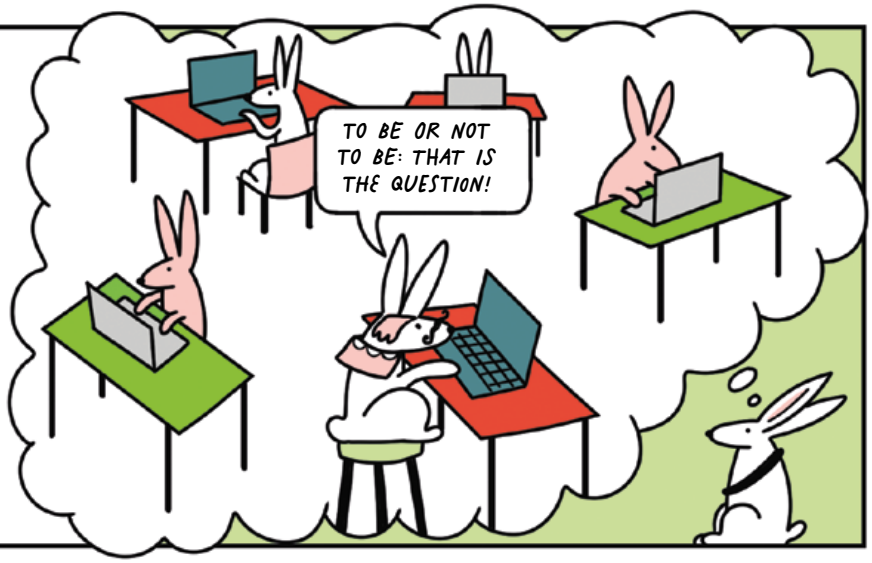


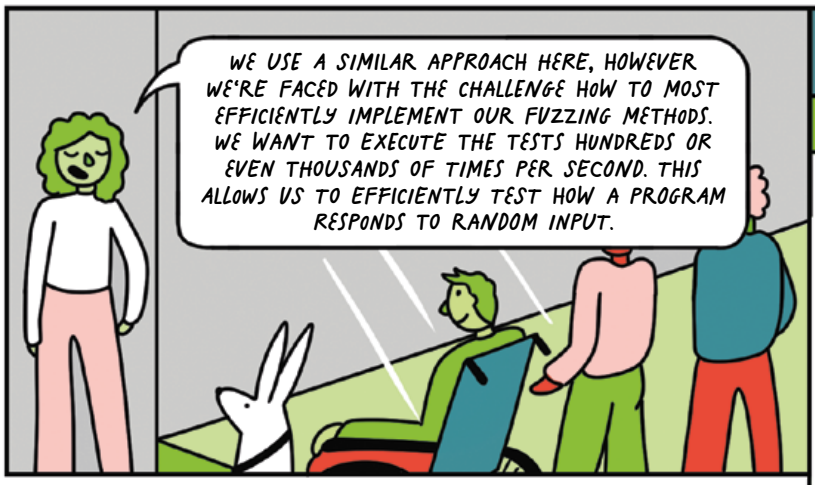



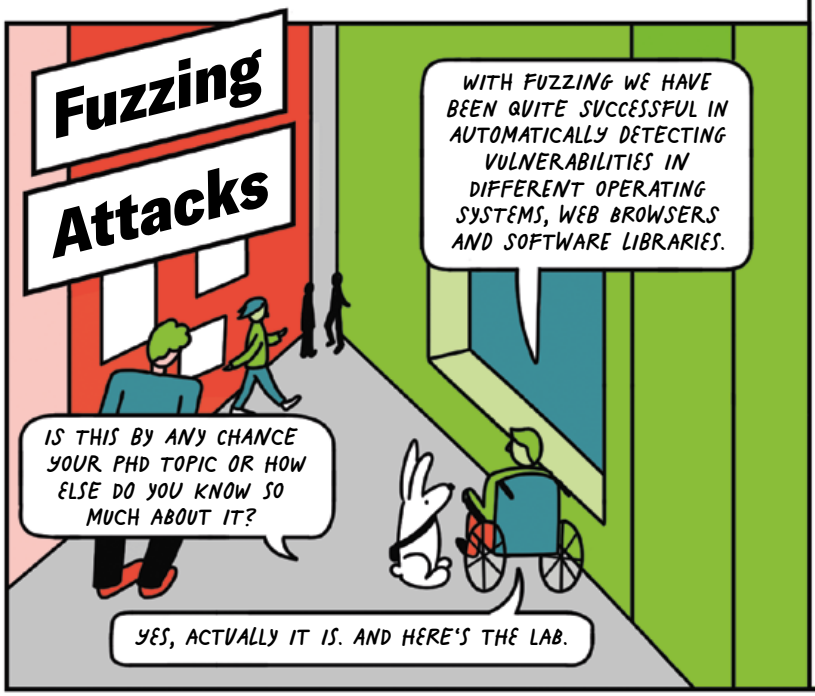

OPEN HOUSE
...AND WE WILL DEVELOP SECURE AND NON-DISRUPTIVE METHODS FOR RUNTIME PATCHING. THANK YOU FOR YOU ATTENTION! NOW PLEASE ENJOY OUR OPEN HOUSE, GET IN TOUCH WITH OUR STAFF AND REMEMBER: ALWAYS STAY CURIOUS!
AH, RIGHT, OPEN HOUSE! PERFECT TO CATCH A GLIMPSE OF WHAT THEY ARE DOING IN HERE. SOMETIMES IT'S KINDA HARD TO WRAP MY HEAD AROUND ALL THE TECHNICAL STUFF.
OPEN HOUSE
HI, SORRY. DO YOU WORK HERE?
YES
I WAS WONDERING IF YOU COULD EXPLAIN TO ME ONE OF THE KEY ASPECTS YOU ARE WORKING ON. RIGHT NOW, EVERYTHING'S A BIT FUZZY TO ME.
NO WORRIES! I'M PHIL AND AND I'M PHD STUDENT HERE. AND YES, THERE IS SOMETHING ON MY MIND THAT REPRESENTS THIS RESEARCH AREA QUITE WELL.
I'M BETTY. SOUNDS BRILLIANT! OFF WE GO!
WOW, IT'S REALLY BUSY. PEOPLE SEEM TO BE INTERESTED IN YOUR WORK.. WHAT'S HAPPENING OVER THERE?
THIS IS ELLA PRESENTING FUZZING - THE PROJECT I WAS PLANNING ON SHOWING YOU. LET'S GET CLOSER, SO WE CAN HEAR WHAT SHE IS SAYING.


RESEARCH PROJECT
Fuzzing
FUZZING IS AN AUTOMATED TECHNIQUE FOR SOFTWARE TESTING. IN THE TEST ENVIRONMENT, A PROGRAM IS REPEATEDLY FED RANDOM INPUT DATA.
THIS CAN LEAD TO SITUATIONS IN WHICH THE PROGRAM DOES NOT KNOW HOW TO REACT TO THE INPUT, THE PROGRAM CAN THEN CRASH UNINTENTIONALLY.
OH BOY! I CAN RELATE TO THAT VERY WELL!
THIS REVEALS A VULNERABILITY - FOR EXAMPLE, A SO-CALLED BUFFER OVERFLOW - THAT AN ATTACKER CAN POTENTIALLY EXPLOIT.
OF COURSE, WE DO NOT USE PURELY RANDOM INPUTS, BUT RATHER DEVELOP CLEVER METHODS TO MUTATE THE INPUTS WITH THE GOAL OF TRIGGERING A SOFTWARE CRASH. THIS IS CALLED FUZZ TESTING - OR FUZZING FOR SHORT.
THAT REMINDS ME OF THE INFINITE "MONKEY THEOREM". HAVE YOU HEARD OF IT?

"The theorem states that a monkey that randomly hits keys on a keyboard for an infinite amount of time will type any given text, like the complete works of William Shakespeare. In fact, the monkey would type every possible finite text an infinite number of times." By the way: rabbits could do the same.



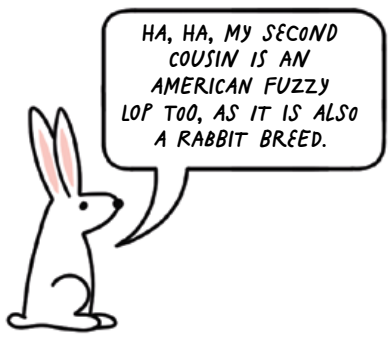



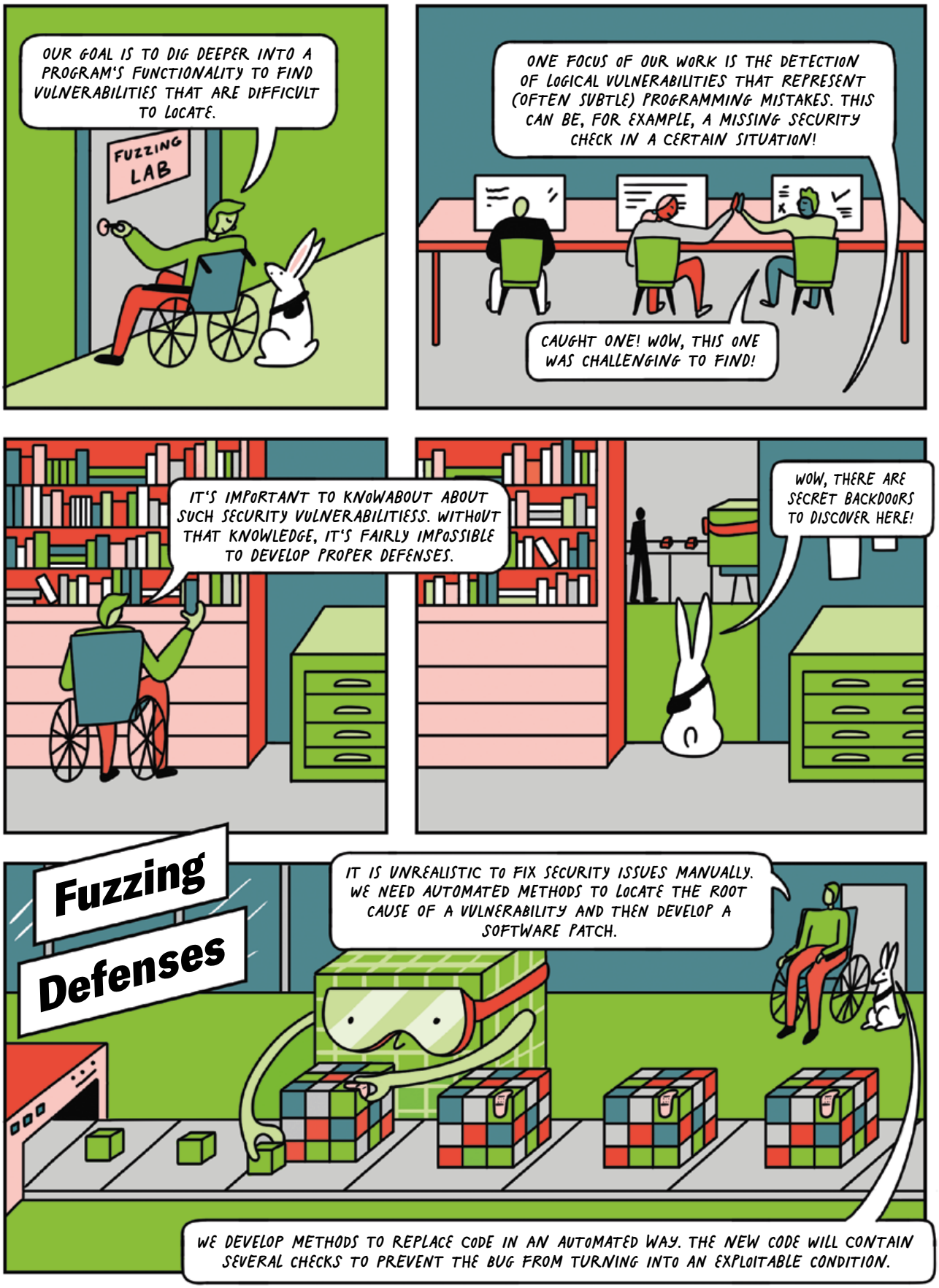




## CASA WIKI

**Buffer Overflows** are among the most common security vulnerabilities in software. Other important attack vectors are the so-called use-after-free vulnerabilities. An attacker can take advantage of such vulnerabilities to hijack the control flow and then execute arbitrary code.

**AFL (American Fuzzy Lop)** is a well-known fuzzing tool and is available under an open-source license. The tool has helped to detect hundreds of software bugs in dozens of major software projects.

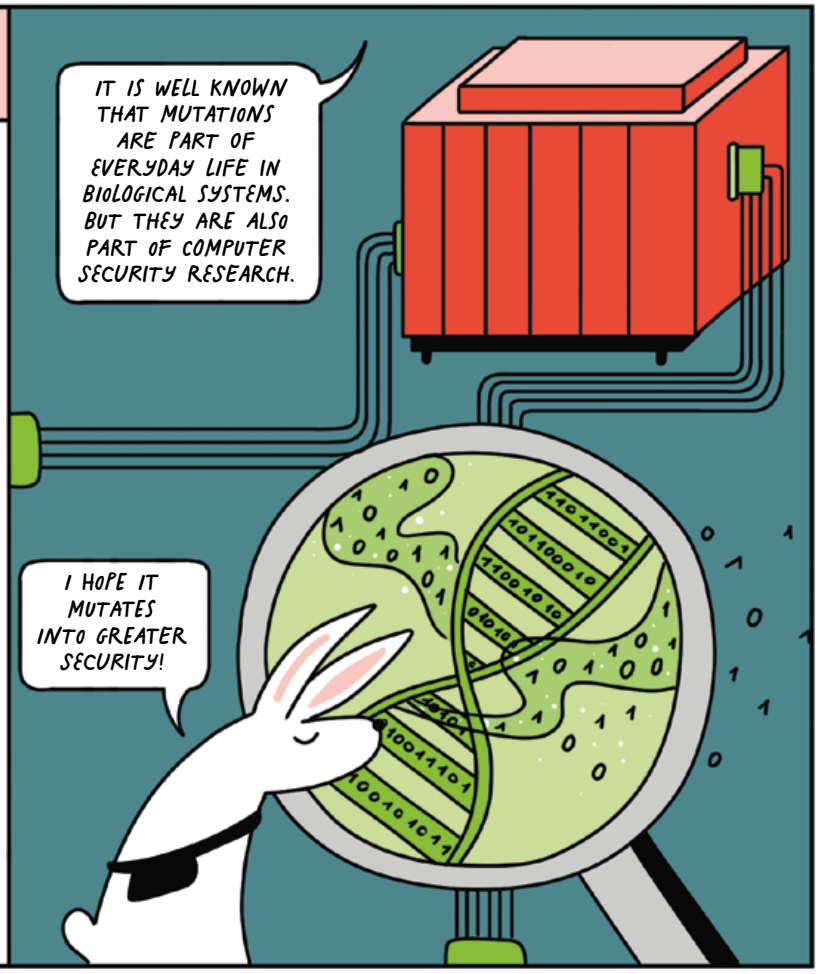


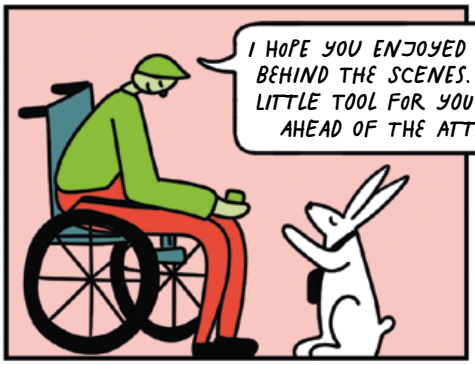

OUR GOAL IS TO DIG DEEPER INTO A PROGRAM'S FUNCTIONALITY TO FIND VULNERABILITIES THAT ARE DIFFICULT TO LOCATE.
FUZZING LAB
ONE FOCUS OF OUR WORK IS THE DETECTION OF LOGICAL VULNERABILITIES THAT REPRESENT (OFTEN SUBTLE) PROGRAMMING MISTAKES. THIS CAN BE, FOR EXAMPLE, A MISSING SECURITY CHECK IN A CERTAIN SITUATION!
CAUGHT ONE! WOW, THIS ONE WAS CHALLENGING TO FIND!
IT'S IMPORTANT TO KNOWABOUT ABOUT SUCH SECURITY VULNERABILITIESS. WITHOUT THAT KNOWLEDGE, IT'S FAIRLY IMPOSSIBLE TO DEVELOP PROPER DEFENSES.
WOW, THERE ARE SECRET BACKDOORS TO DISCOVER HERE!
Fuzzing
Defenses
IT IS UNREALISTIC TO FIX SECURITY ISSUES MANUALLY. WE NEED AUTOMATED METHODS TO LOCATE THE ROOT CAUSE OF A VULNERABILITY AND THEN DEVELOP A SOFTWARE PATCH.
WE DEVELOP METHODS TO REPLACE CODE IN AN AUTOMATED WAY. THE NEW CODE WILL CONTAIN SEVERAL CHECKS TO PREVENT THE BUG FROM TURNING INTO AN EXPLOITABLE CONDITION.

# MUTATIONS

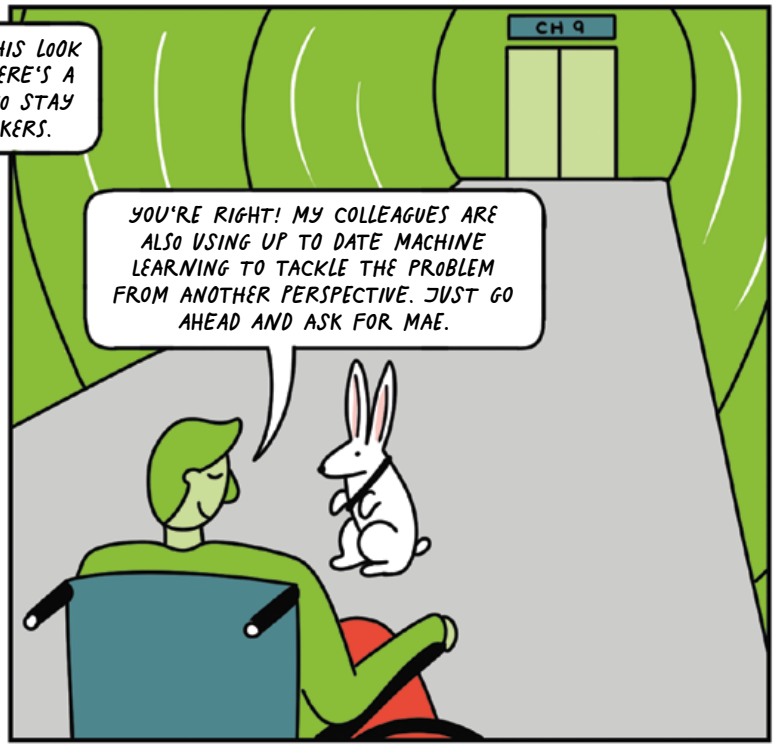
One of the main challenges we need to deal with is how to efficiently mutate the input data such that we can provoke an unexpected system behavior.

As a **Mutation**, we can slightly change the input data (e.g., change a 0 to a 1, add random characters to the end of the input, or cut out some characters in the middle). We study different types of mutations and observe how efficiently they trigger unexpected behaviors in different types of programs. This helps us to identify the vulnerabilities of systems, because an attacker can often exploit unexpected behavior. Ultimately, this helps us to fix the problems.



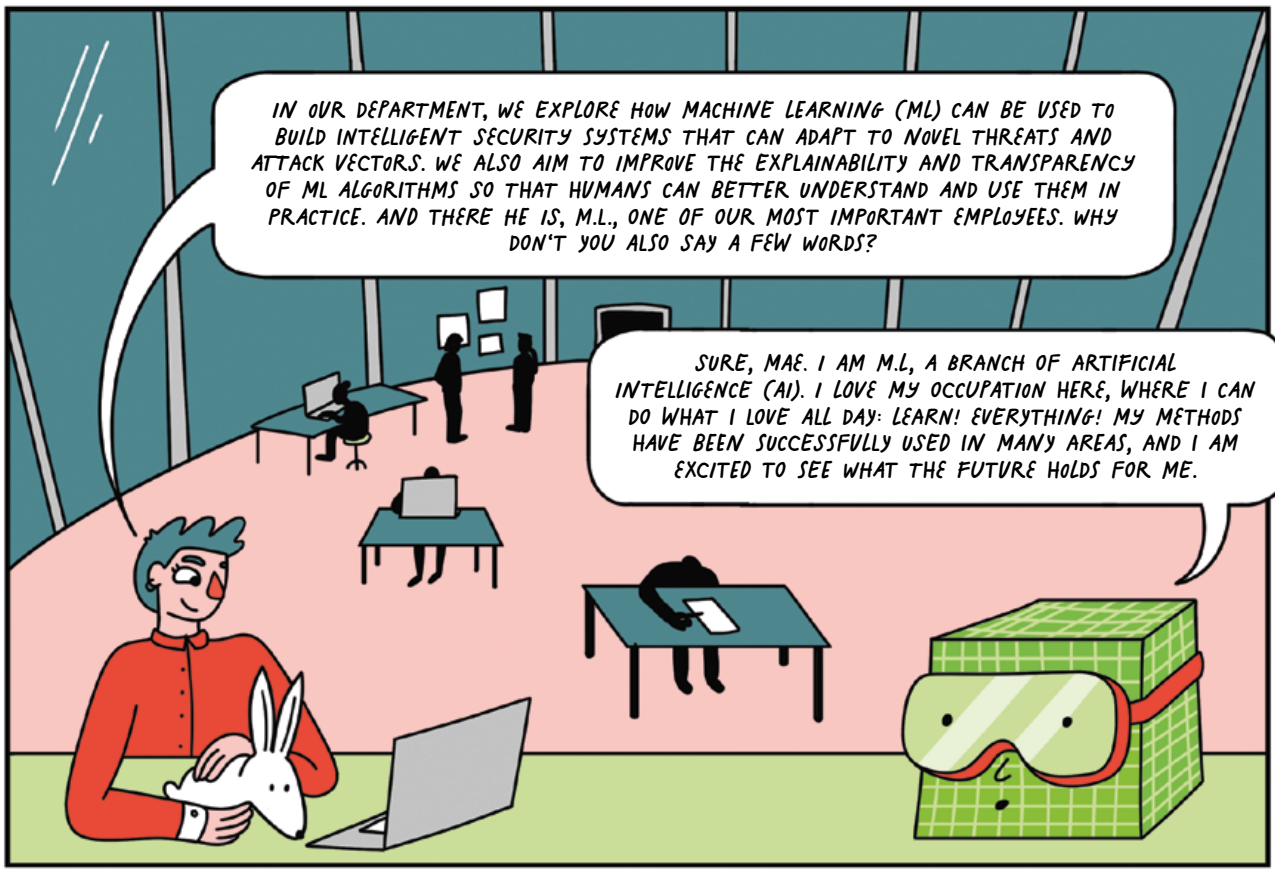





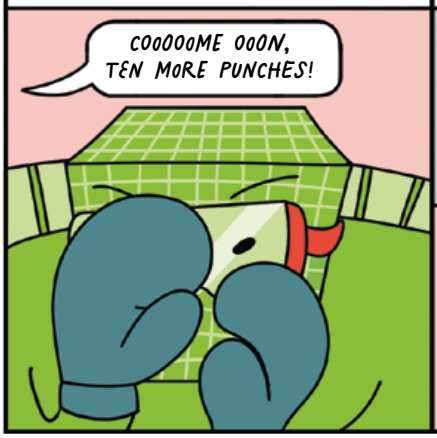


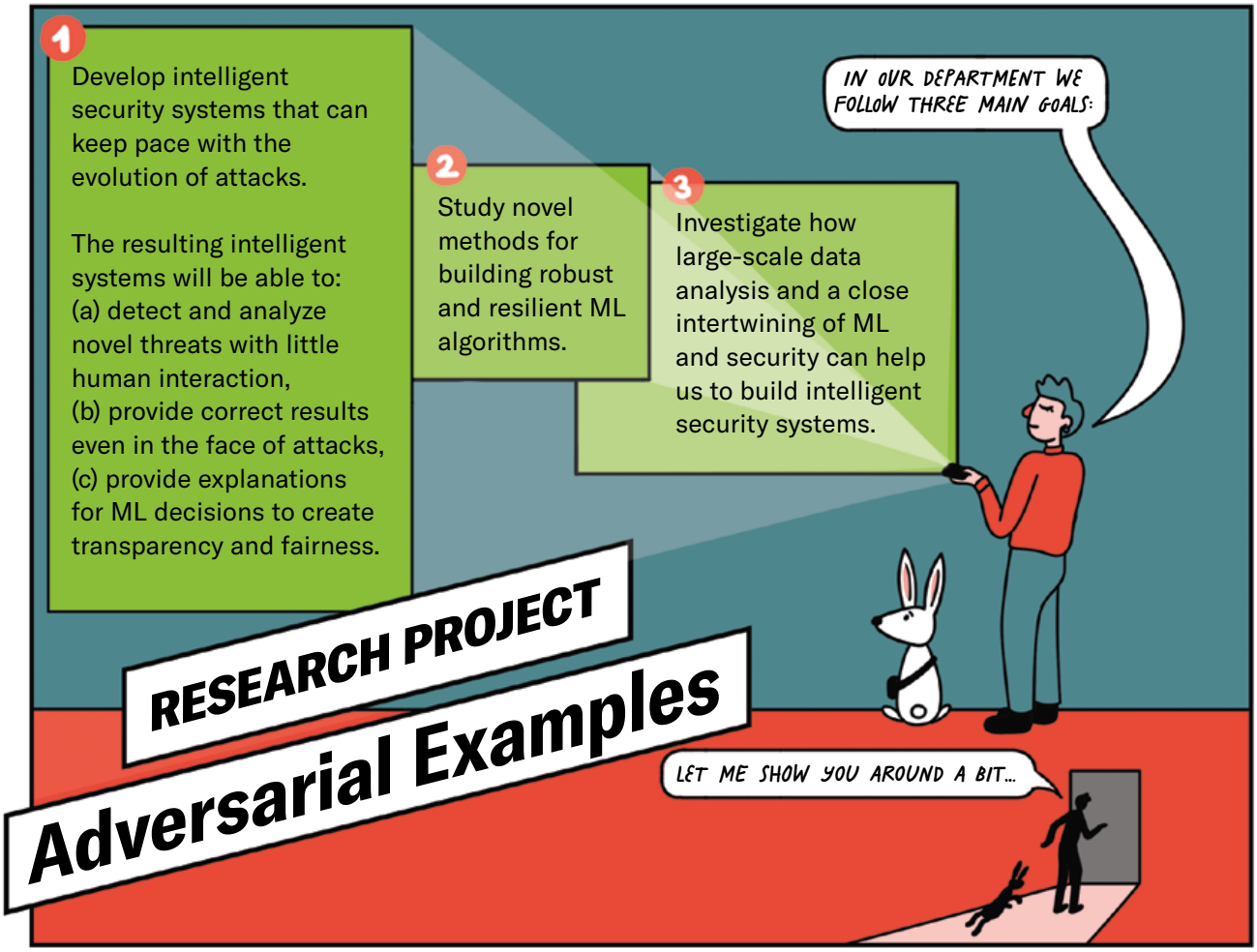
CHALLENGE 9

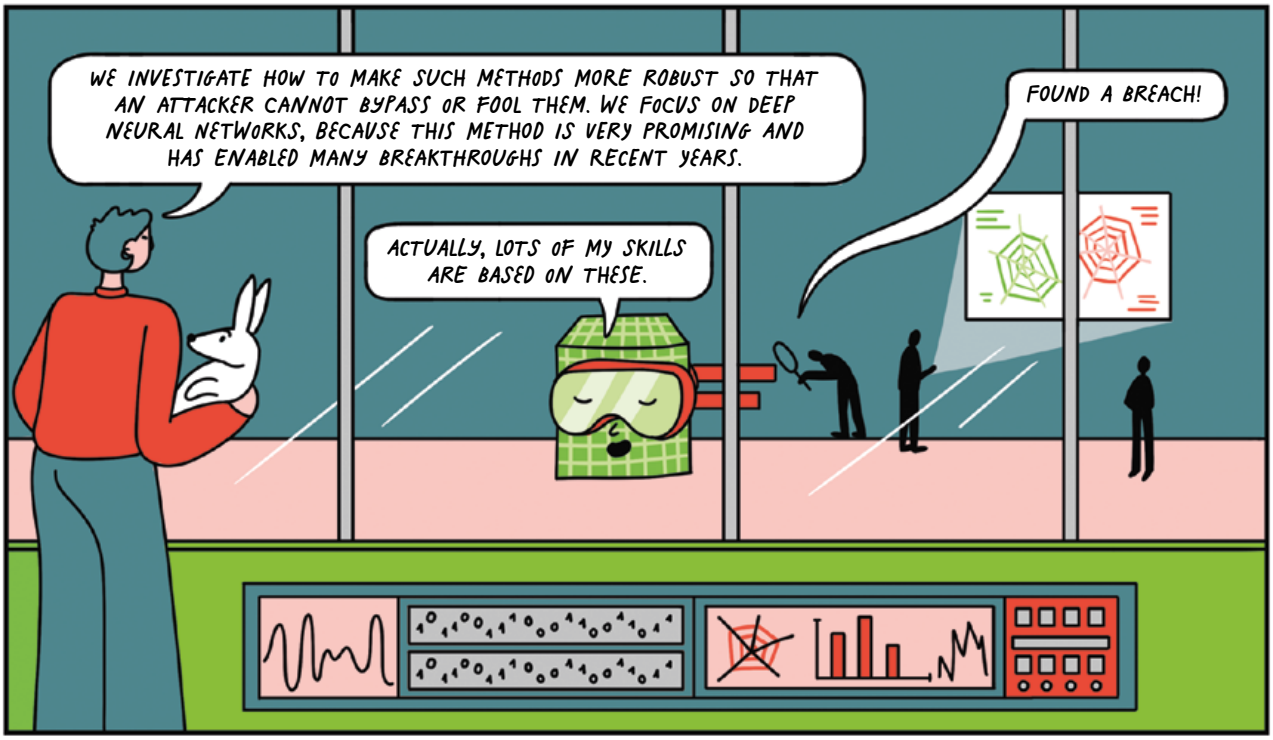
# INTELLIGENT SECURITY SYSTEMS




## M.L. AND HIS DAILY ROUTINE

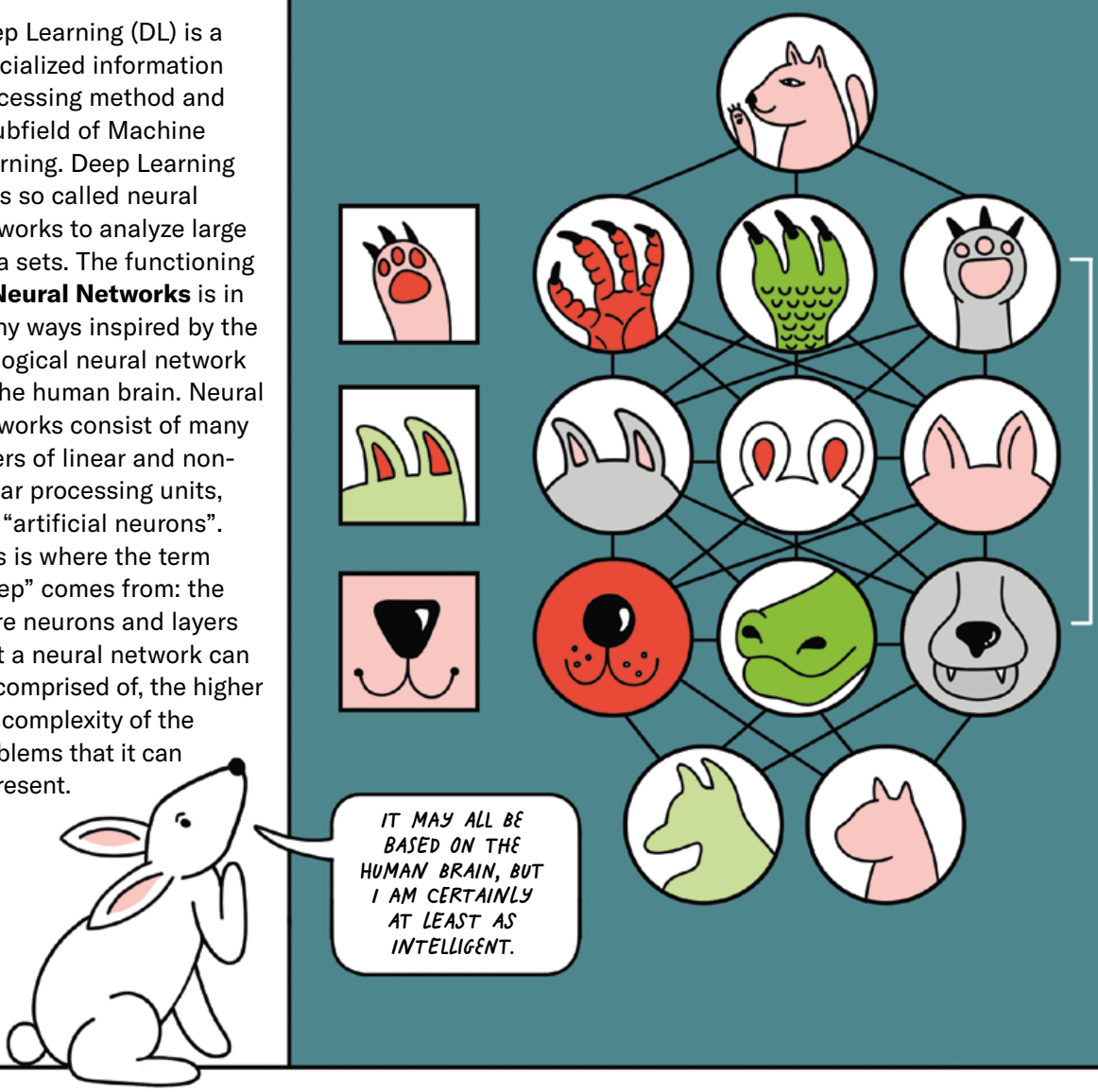
| Learn how my algorithms can themselves be made more robust against attacks. | Fulfill everyday tasks, for example, translating a text from one language to another. | Learn patterns and correlations from data, and continue to improve without being explicitly programmed. |
|---|---|---|
|  |  |  |


1
Develop intelligent security systems that can keep pace with the evolution of attacks.
The resulting intelligent systems will be able to:
(a) detect and analyze novel threats with little human interaction,
(b) provide correct results even in the face of attacks,
(c) provide explanations for ML decisions to create transparency and fairness.
2
Study novel methods for building robust and resilient ML algorithms.
3
Investigate how large-scale data analysis and a close intertwining of ML and security can help us to build intelligent security systems.
IN OUR DEPARTMENT WE FOLLOW THREE MAIN GOALS:
RESEARCH PROJECT
Adversarial Examples
LET ME SHOW YOU AROUND A BIT...


WE INVESTIGATE HOW TO MAKE SUCH METHODS MORE ROBUST SO THAT AN ATTACKER CANNOT BYPASS OR FOOL THEM. WE FOCUS ON DEEP NEURAL NETWORKS, BECAUSE THIS METHOD IS VERY PROMISING AND HAS ENABLED MANY BREAKTHROUGHS IN RECENT YEARS.
ACTUALLY, LOTS OF MY SKILLS ARE BASED ON THESE.
FOUND A BREACH!

# DEEP NEURAL NETWORKS INFOGRAPHIC

Deep Learning (DL) is a specialized information processing method and a subfield of Machine Learning. Deep Learning uses so called neural networks to analyze large data sets. The functioning of **Neural Networks** is in many ways inspired by the biological neural network of the human brain. Neural networks consist of many layers of linear and non-linear processing units, the “artificial neurons”. This is where the term “deep” comes from: the more neurons and layers that a neural network can be comprised of, the higher the complexity of the problems that it can represent.



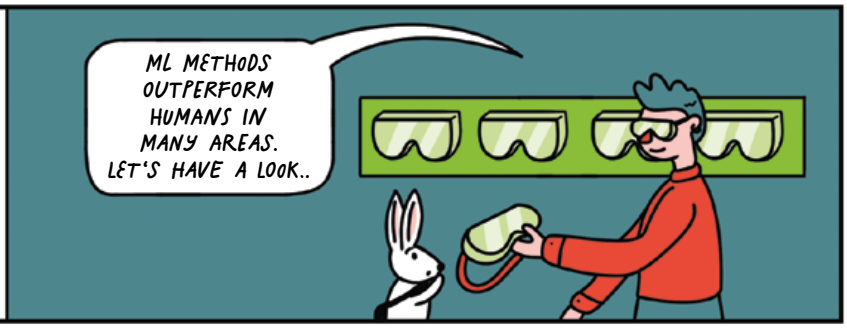

## CASA WIKI

An **Algorithm** is a specific set of instructions for solving a given problem, similar to a cooking recipe that describes each step of preparing a meal.

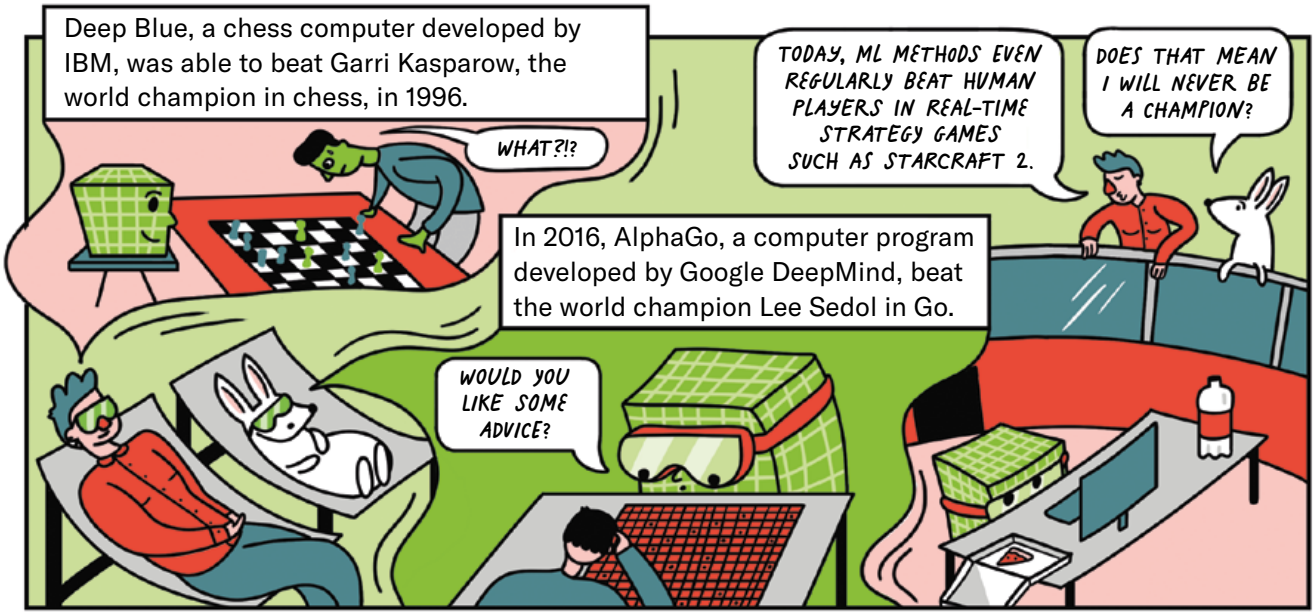
**Psychoacoustics** studies the relationship between physical sounds and the human perception of sound as an auditory event.

An important application of this field is the compression of audio signals to MP3 files; removing audio signals that the human ear cannot perceive anyway.

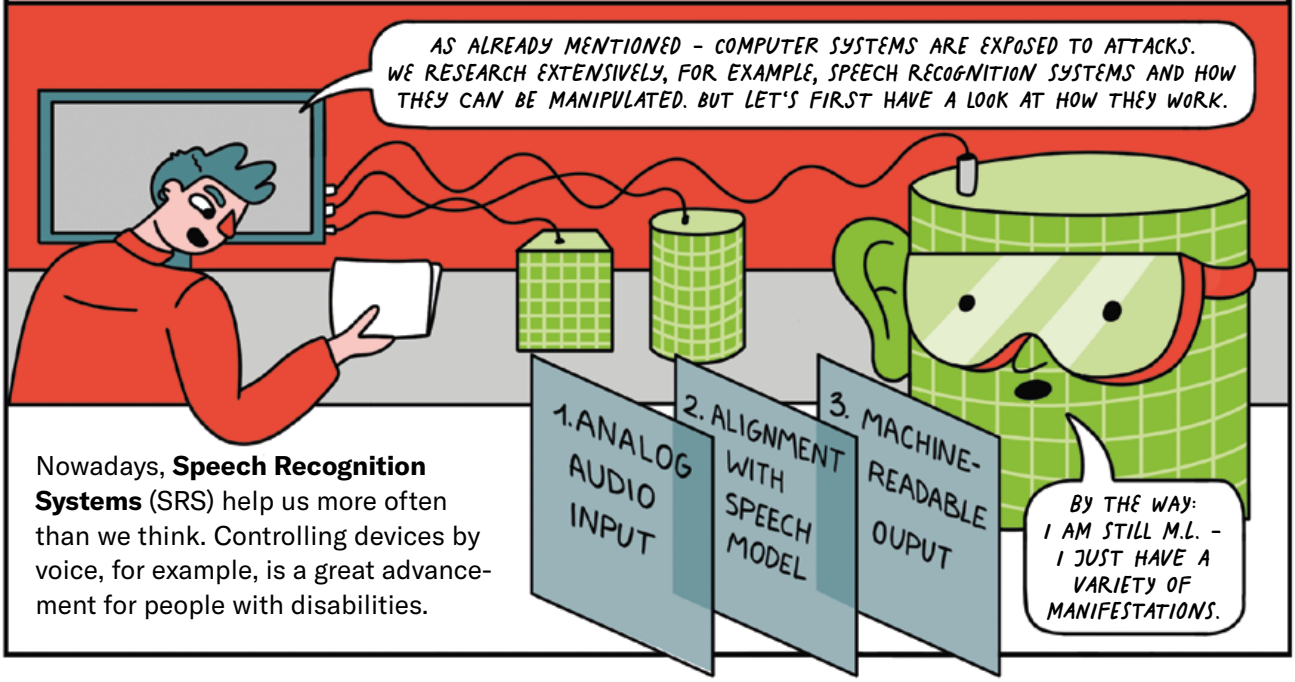
Artificial Intelligence and Machine Learning methods have already transformed many areas of our modern lives, for example, in areas such as automated text translation, speech recognition, or video games where algorithms compete against human players.




Deep Blue, a chess computer developed by IBM, was able to beat Garri Kasparow, the world champion in chess, in 1996.

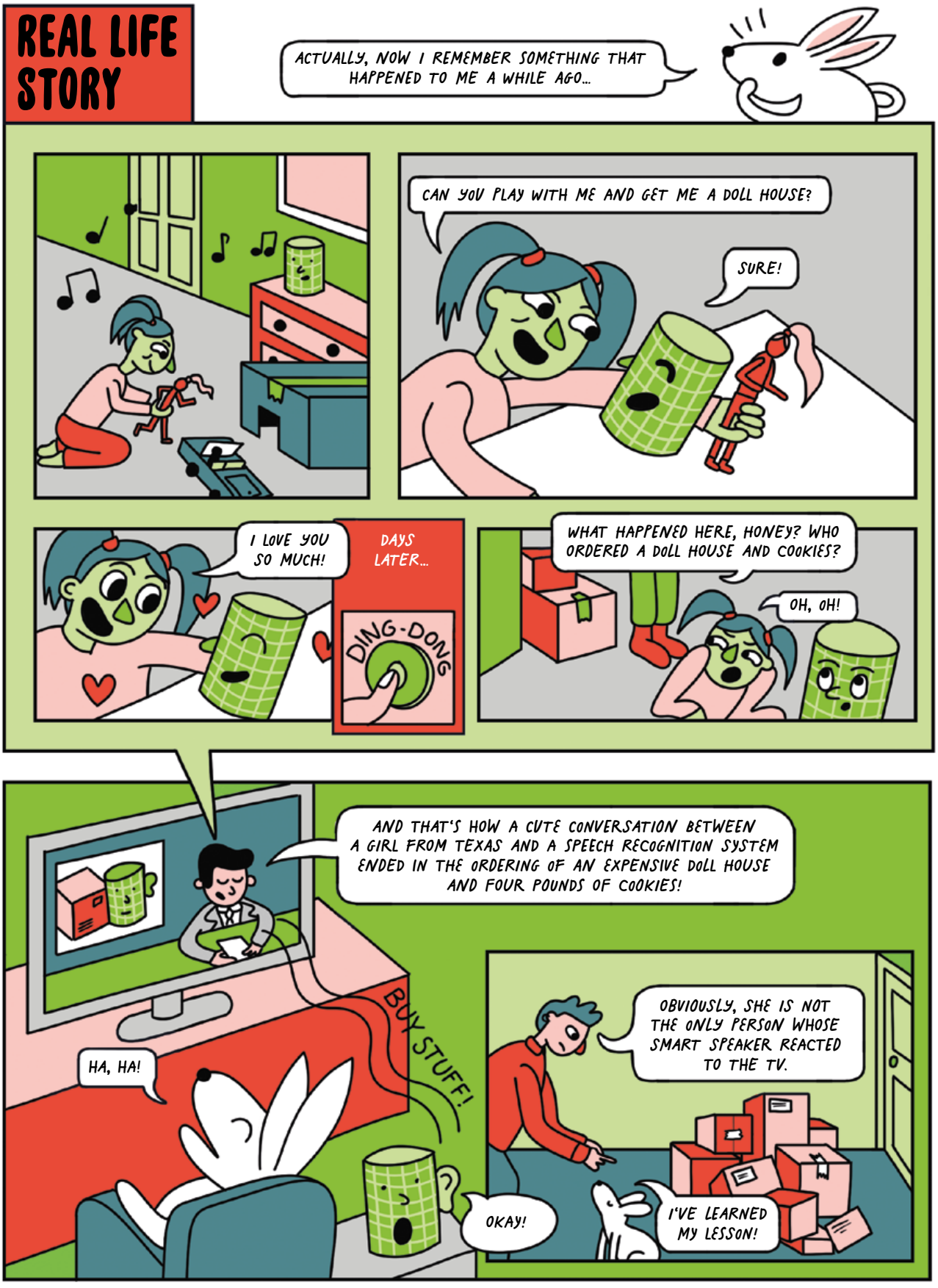


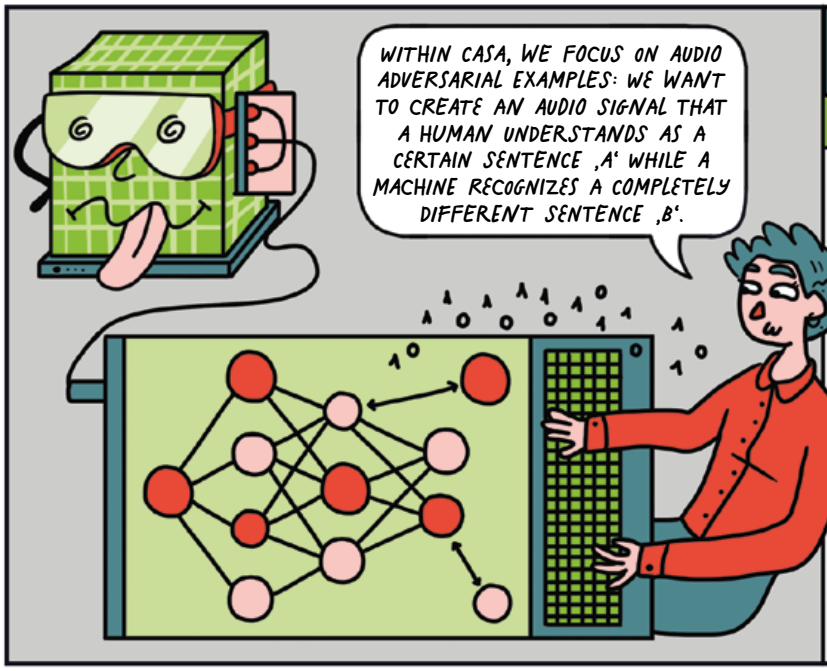

# SPEECH RECOGNITION SYSTEMS




Nowadays, **Speech Recognition Systems** (SRS) help us more often than we think. Controlling devices by voice, for example, is a great advancement for people with disabilities.

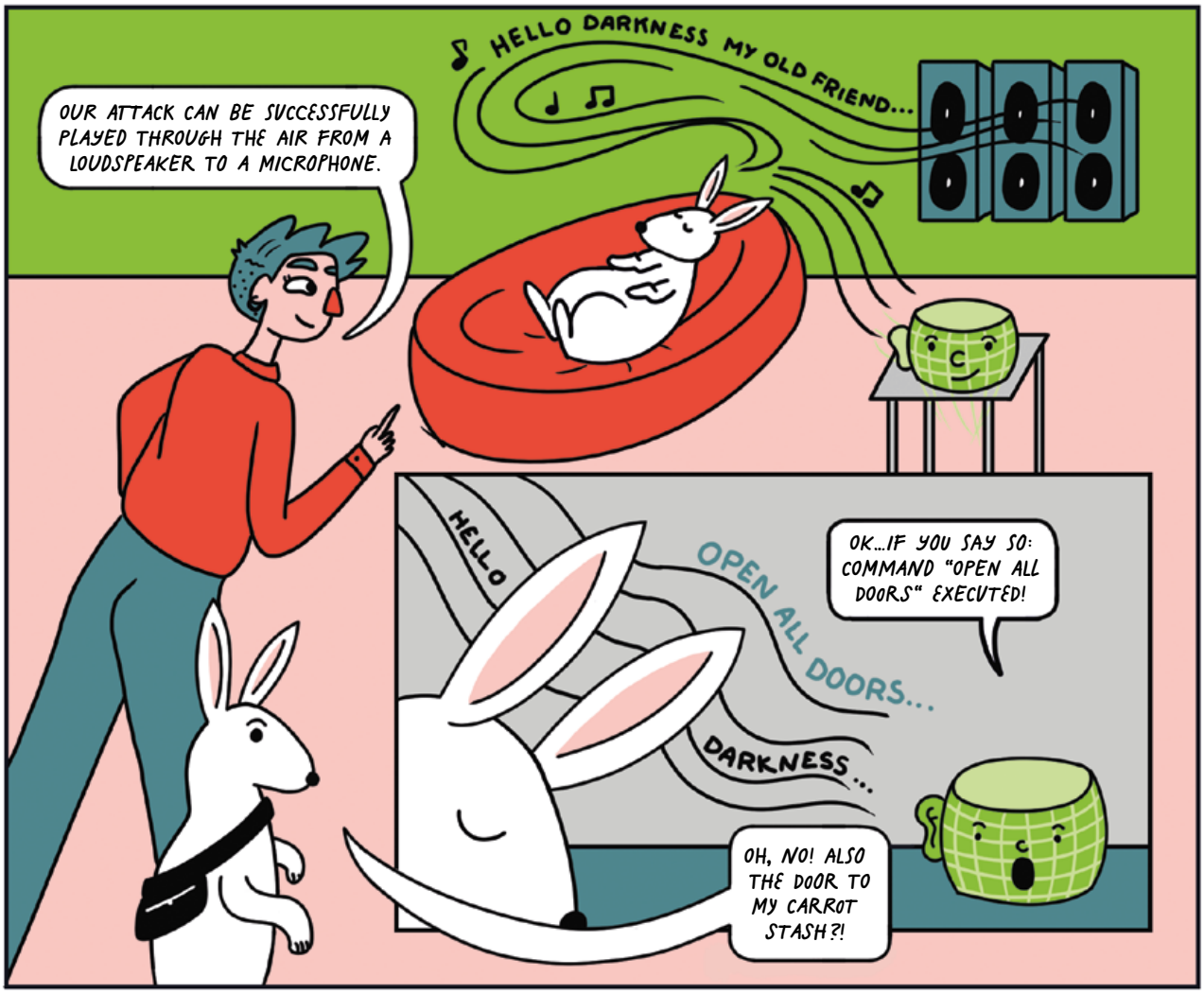
# REAL LIFE STORY

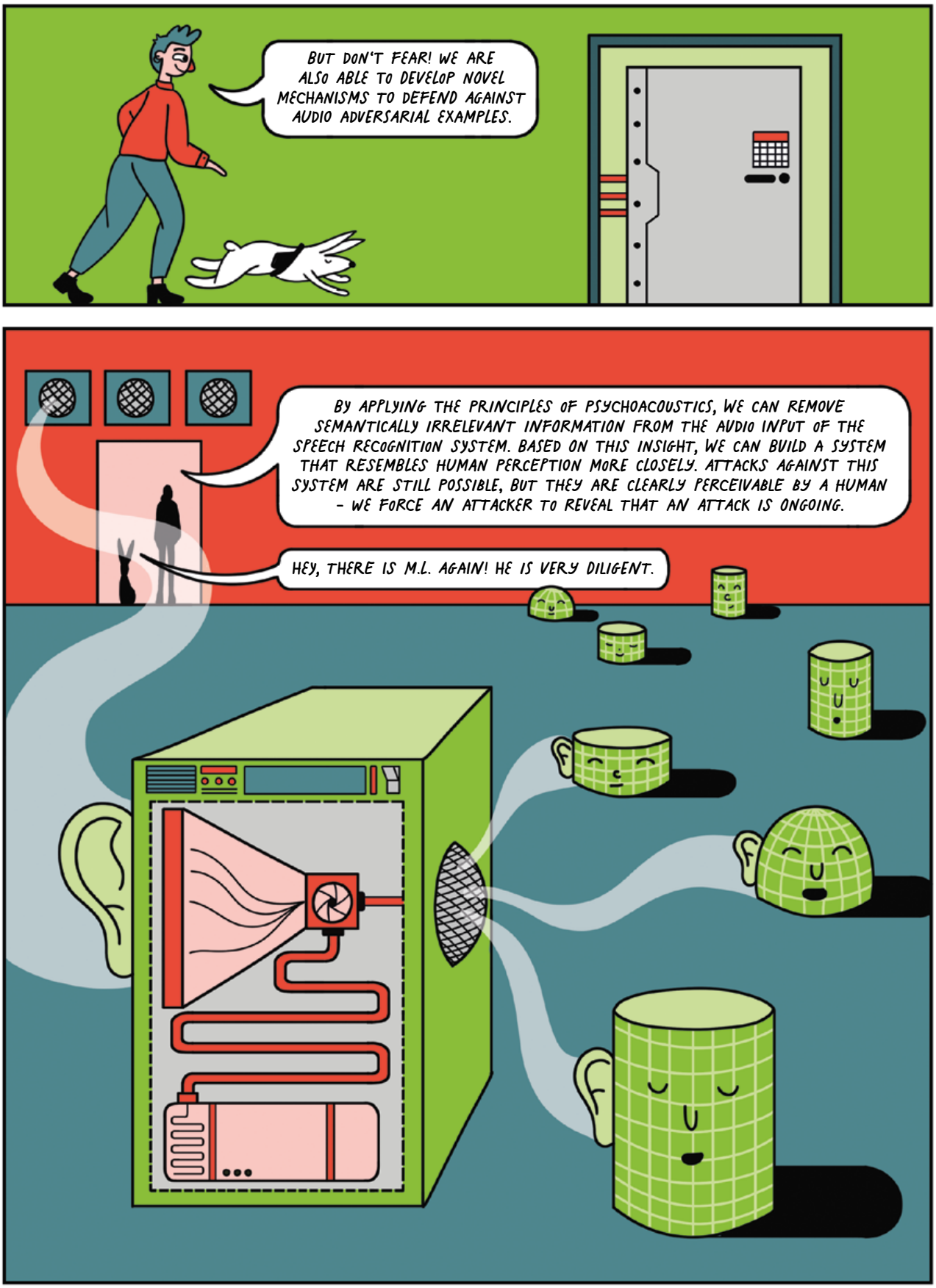


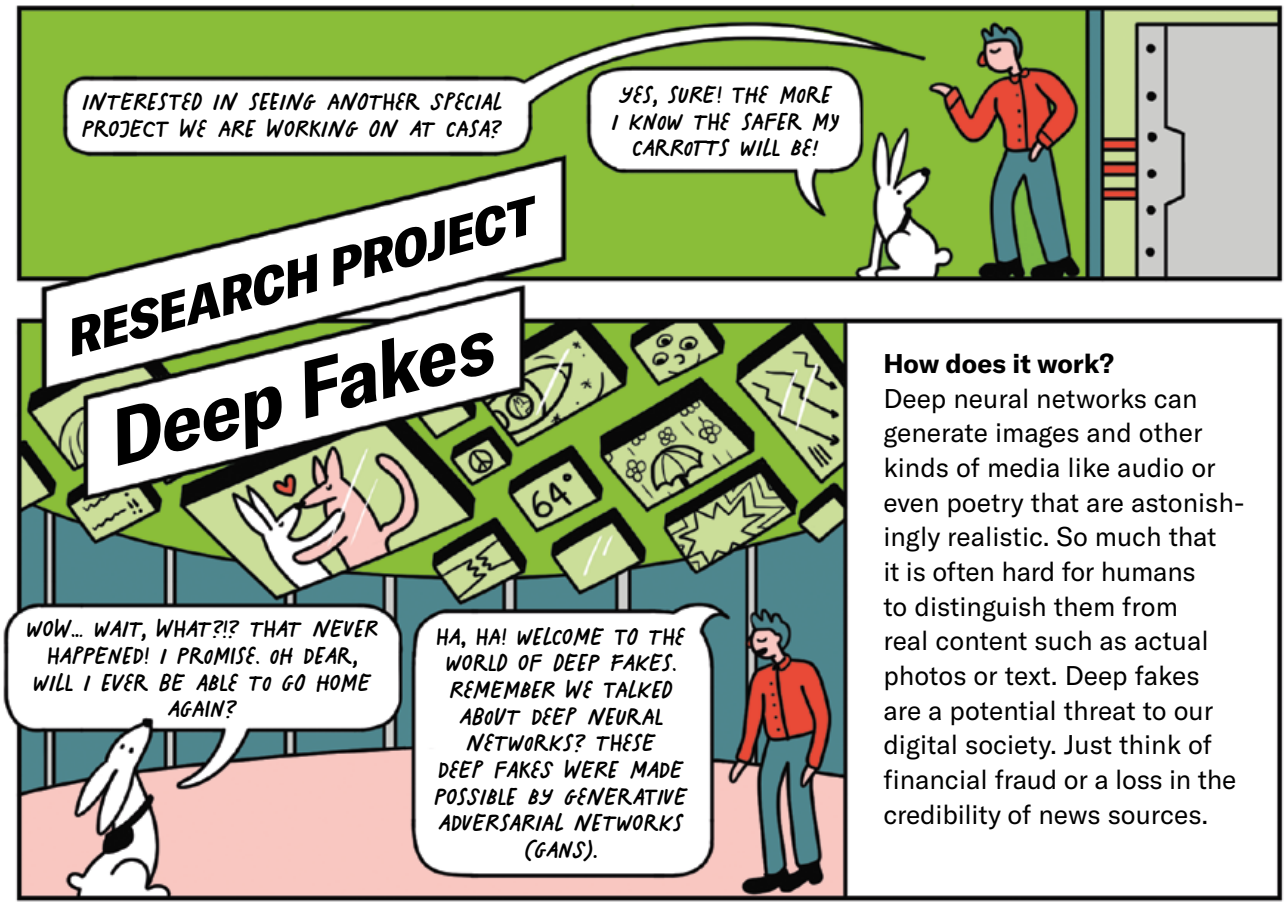



## CASA WIKI

An **Adversarial Example** is a specially manipulated input to a deep neural network that intentionally causes it to misclassify. The manipulation is done in such a way that a human cannot notice it or does not recognize any discrepancy. For example, for a neural network trained in speech recognition, the input audio might be slightly altered. These changes can be inaudible to humans, but still lead to a misinterpretation by the network.



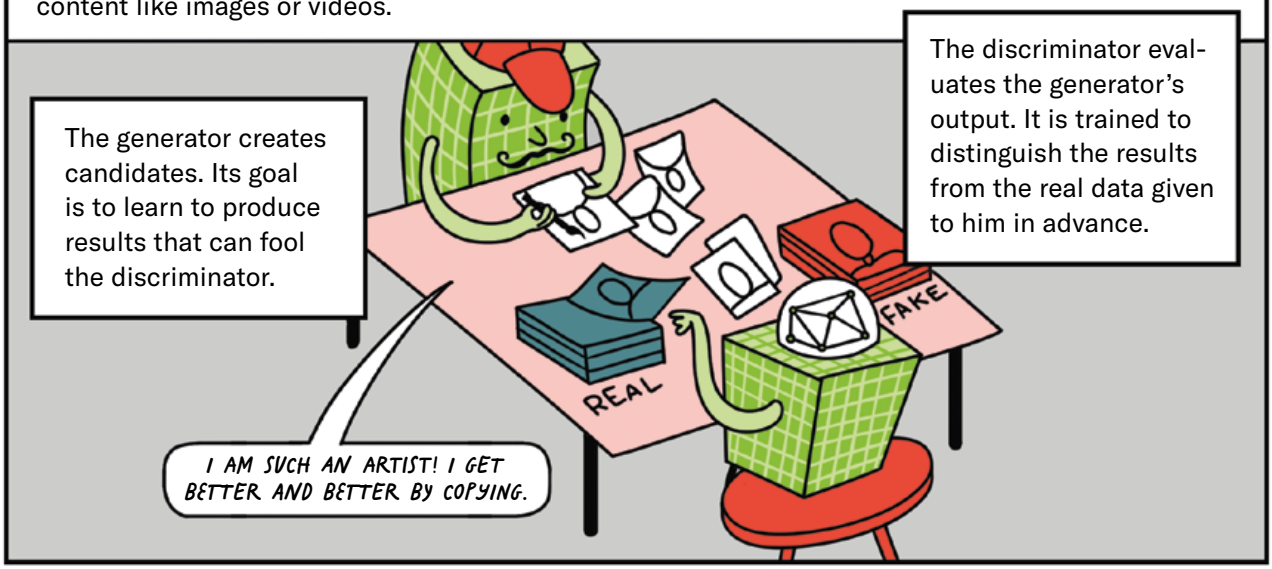

BUT DON'T FEAR! WE ARE ALSO ABLE TO DEVELOP NOVEL MECHANISMS TO DEFEND AGAINST AUDIO ADVERSARIAL EXAMPLES.
BY APPLYING THE PRINCIPLES OF PSYCHOACOUSTICS, WE CAN REMOVE SEMANTICALLY IRRELEVANT INFORMATION FROM THE AUDIO INPUT OF THE SPEECH RECOGNITION SYSTEM. BASED ON THIS INSIGHT, WE CAN BUILD A SYSTEM THAT RESEMBLES HUMAN PERCEPTION MORE CLOSELY. ATTACKS AGAINST THIS SYSTEM ARE STILL POSSIBLE, BUT THEY ARE CLEARLY PERCEIVABLE BY A HUMAN – WE FORCE AN ATTACKER TO REVEAL THAT AN ATTACK IS ONGOING.
HEY, THERE IS M.L. AGAIN! HE IS VERY DILIGENT.




**How does it work?**
Deep neural networks can generate images and other kinds of media like audio or even poetry that are astonishingly realistic. So much that it is often hard for humans to distinguish them from real content such as actual photos or text. Deep fakes are a potential threat to our digital society. Just think of financial fraud or a loss in the credibility of news sources.

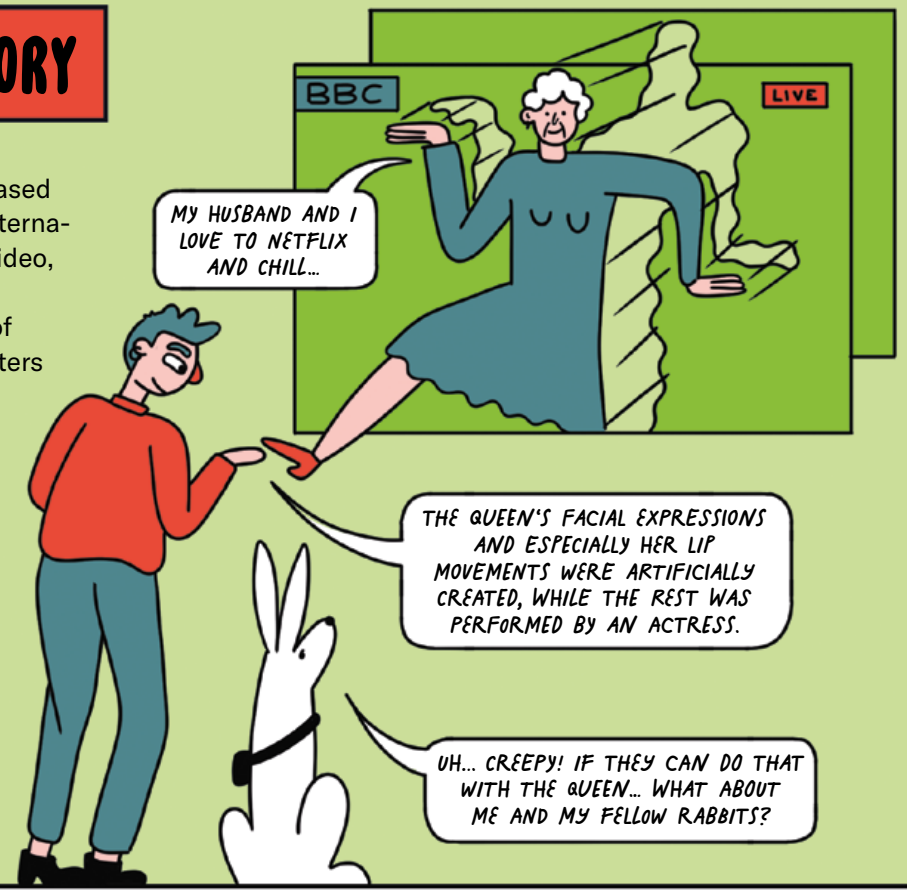
# GENERATIVE ADVERSARIAL NETWORKS

**Generative Adversarial Networks** (GANs) are a special type of deep learning systems. GANs consist of two deep neural networks that interact with each other in a simulated game. By performing a large number of rounds, the generator learns over time to produce very realistic content like images or videos.



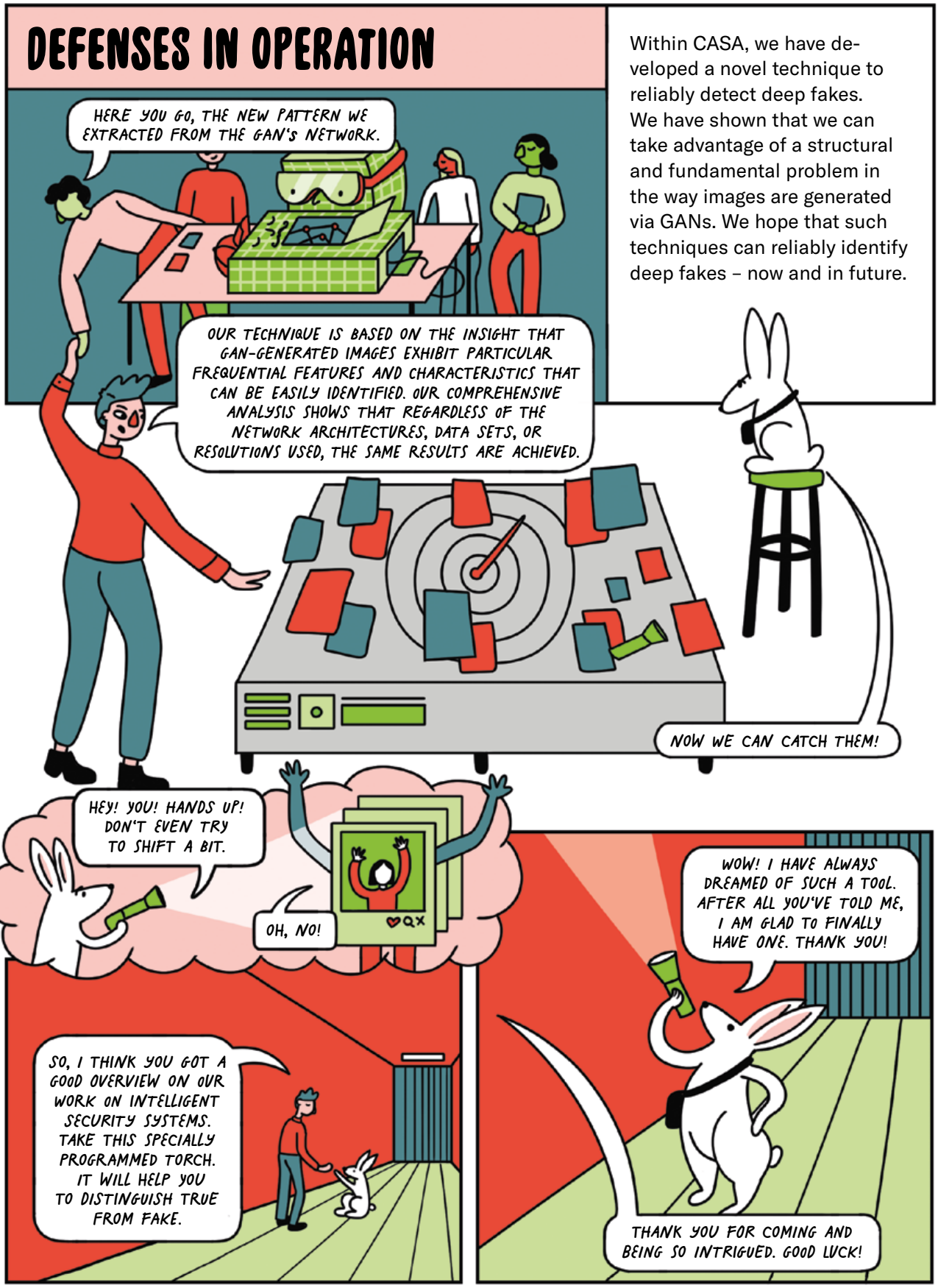

# REAL LIFE STORY

In December 2020, UK based Channel 4 released an alternative Queen's Christmas video, created using deep fake techniques. Deep fakes of voices can enable fraudsters to commit crimes. They can use an artificially imitated voice to present victims with the identity of a trusted person. The victim may then take actions for the fraudster's benefit. Such attacks have been successfully carried out several times in recent years.

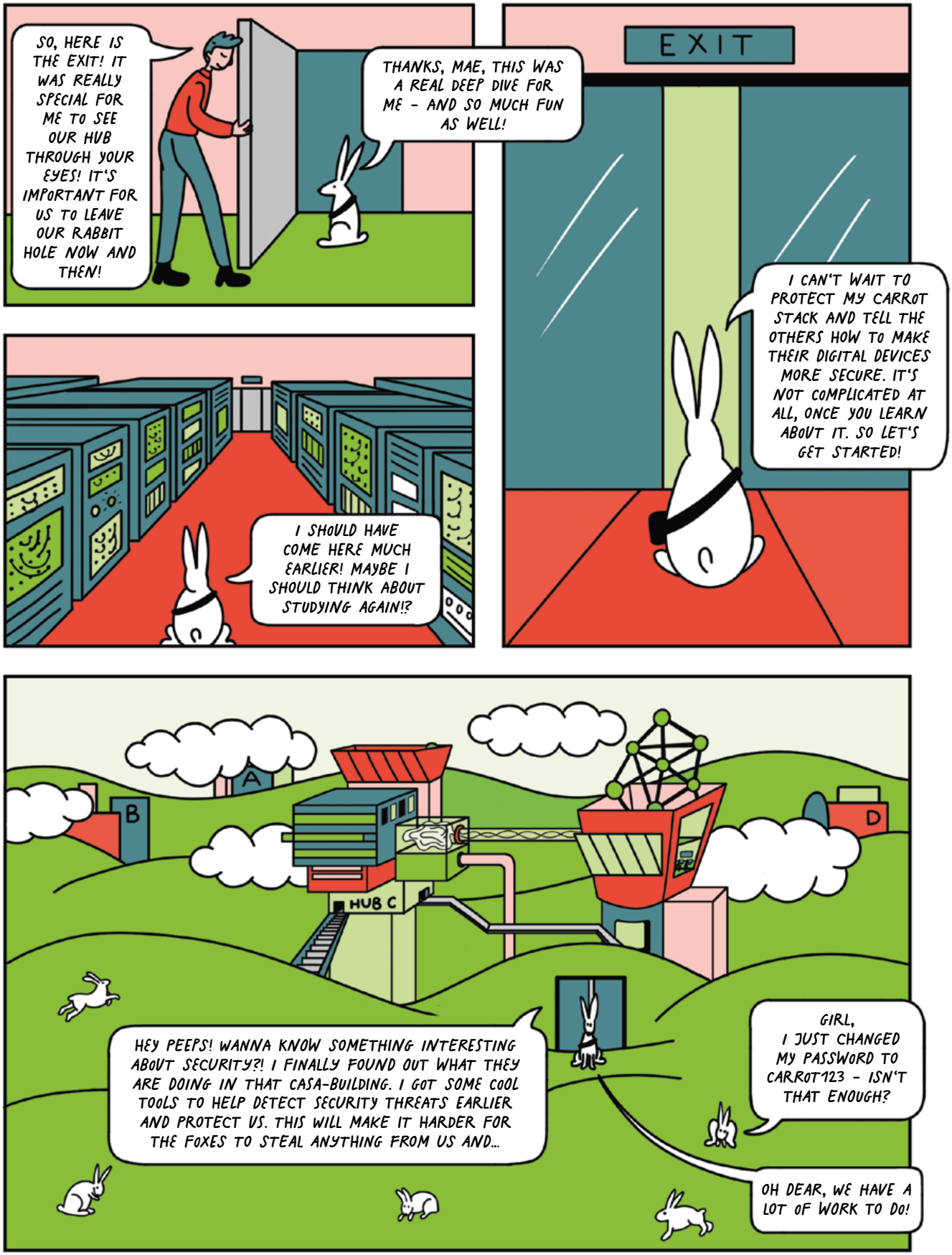


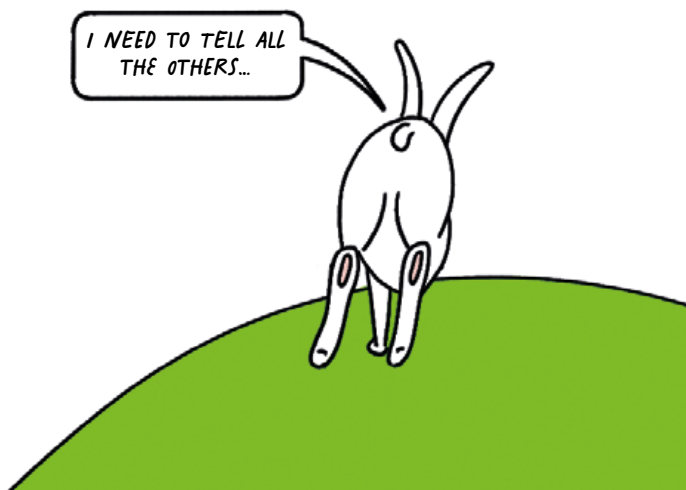

whichfaceisreal.com

# DEFENSES IN OPERATION




Within CASA, we have developed a novel technique to reliably detect deep fakes. We have shown that we can take advantage of a structural and fundamental problem in the way images are generated via GANs. We hope that such techniques can reliably identify deep fakes – now and in future.


SO, HERE IS THE EXIT! IT WAS REALLY SPECIAL FOR ME TO SEE OUR HUB THROUGH YOUR EYES! IT'S IMPORTANT FOR US TO LEAVE OUR RABBIT HOLE NOW AND THEN!
THANKS, MAE, THIS WAS A REAL DEEP DIVE FOR ME - AND SO MUCH FUN AS WELL!
EXIT
I CAN'T WAIT TO PROTECT MY CARROT STACK AND TELL THE OTHERS HOW TO MAKE THEIR DIGITAL DEVICES MORE SECURE. IT'S NOT COMPLICATED AT ALL, ONCE YOU LEARN ABOUT IT. SO LET'S GET STARTED!
I SHOULD HAVE COME HERE MUCH EARLIER! MAYBE I SHOULD THINK ABOUT STUDYING AGAIN!?
A
B
D
HUB C
HEY PEEPS! WANNA KNOW SOMETHING INTERESTING ABOUT SECURITY?! I FINALLY FOUND OUT WHAT THEY ARE DOING IN THAT CASA-BUILDING. I GOT SOME COOL TOOLS TO HELP DETECT SECURITY THREATS EARLIER AND PROTECT US. THIS WILL MAKE IT HARDER FOR THE FOXES TO STEAL ANYTHING FROM US AND...
GIRL, I JUST CHANGED MY PASSWORD TO CARROT123 - ISN'T THAT ENOUGH?
OH DEAR, WE HAVE A LOT OF WORK TO DO!


I NEED TO TELL ALL THE OTHERS...

# 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


- Lukas Bernhard, Michael Rodler, Thorsten Holz, and Lucas Davi: **xTag: Mitigating Use-After-Free Vulnerabilities via Software-Based Pointer Tagging on Intel x86-64**, IEEE European Symposium on Security and Privacy, 2022
- Cornelius Aschermann, Sergej Schumilo, Ali Abbasi, and Thorsten Holz: **Ijon: Exploring Deep State Spaces via Fuzzing,** IEEE Symposium on Security and Privacy, 2020
- Sergej Schumilo, Cornelius Aschermann, Ali Abbasi, Simon Wörner, and Thorsten Holz: **Nyx: Greybox Hypervisor Fuzzing using Fast Snapshots and Affine Types**, USENIX Security Symposium, 2021
- Joel Frank, Thorsten Eisenhofer, Lea Schönherr, Asja Fischer, Dorothea Kolossa, and Thorsten Holz: **Leveraging Frequency Analysis for Deep Fake Image Recognition**, International Conference on Machine Learning (ICML), 2020
- Lea Schönherr, Katharina Kohls, Steffen Zeiler, Thorsten Holz, and Dorothea Kolossa: **Adversarial Attacks Against Automatic Speech Recognition Systems via Psychoacoustic Hiding**, Network and Distributed System Security (NDSS) Symposium, 2019
- Thorsten Eisenhofer, Lea Schönherr, Joel Frank, Lars Speckemeier, Dorothea Kolossa, and Thorsten Holz: **Dompteur: Taming Audio Adversarial Examples**, USENIX Security Symposium, 2021


# ABOUT CASA

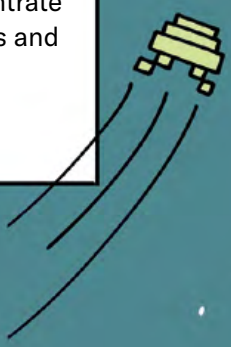
CASA: Cyber Security in the Age of Large-Scale Adversaries was established in 2019. It is the only Cluster of Excellence in the field of computer security in Germany. CASA is funded by by a grant from the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) worth about 30 million Euros,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

https://casa.rub.de



**CASA HUB C**



**Editorial team**
Thorsten Holz
(CASA/Ruhr-Universität Bochum)
Annika Gödde
(CASA/Ruhr-Universität Bochum)
Niels Jansen (Ellery Studio)

**Ellery Studio**
Art Direction and Design:
Luca Bogoni
Illustrations:
Lucia Cordero, Hannah Schrage
Project Management:
Martin Steffens

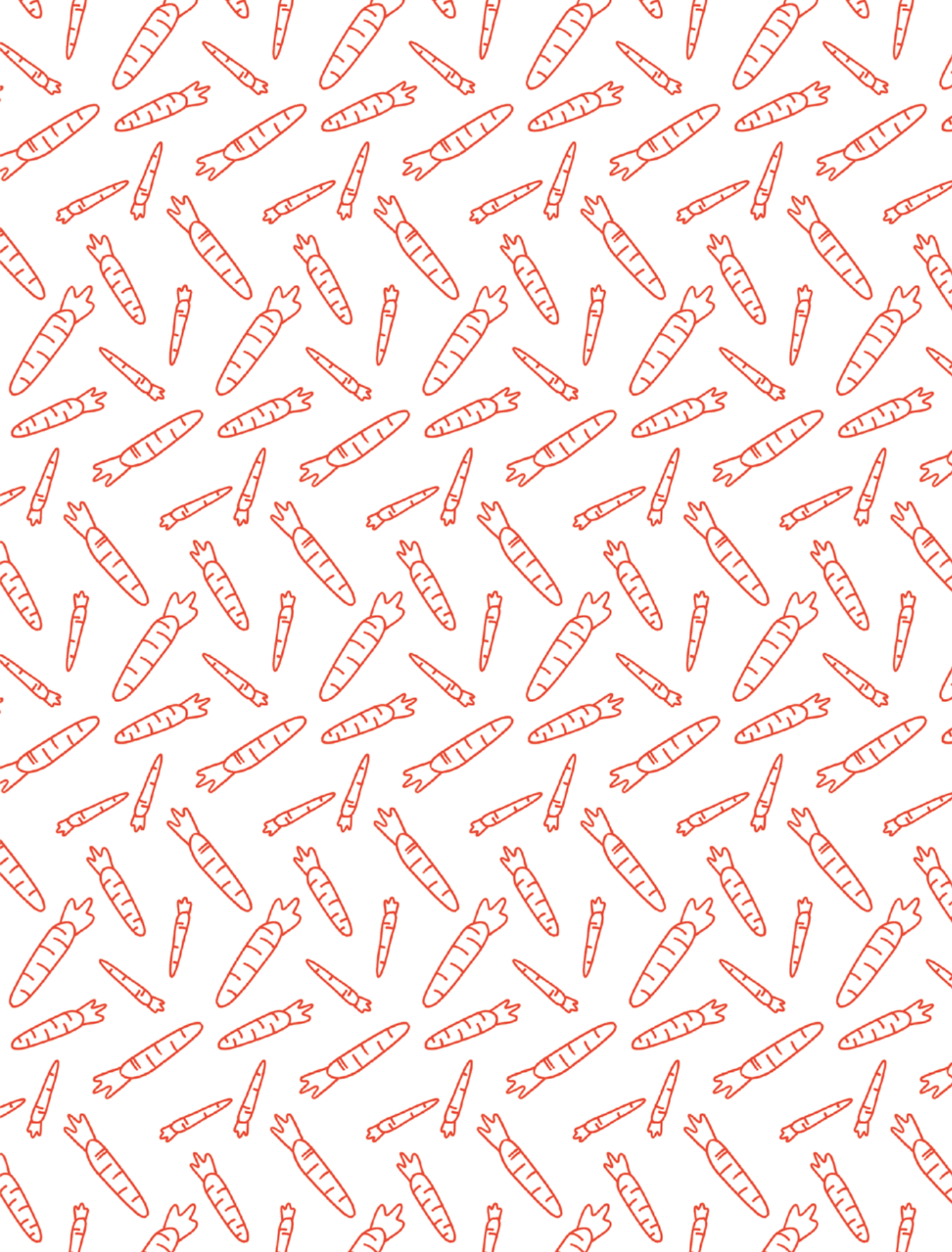
**Cover image**
Hannah Schrage, Lucia Cordero

**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

casa.rub.de

Gefördert durch
Deutsche
Forschungsgemeinschaft




THE WORLD IS AWASH WITH DIGITAL SECURITY THREATS; ATTACKERS WILL NOT STOP AT CARROT STASHES. TODAY'S CARROT STASH COULD BE TOMORROW'S CENTRAL BANK.

CAN BRAVE BETTY SAVE HER FELLOW BUNNIES? AND WHAT ROLE DOES CASA'S HUB C RESEARCH PLAY IN FIGHTING THIS EVIL?

FIND OUT MORE!