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

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.
Content

CHALLENGE 7
Building Secure Systems
How can we build safe and secure systems by design? From scratch and more trustworthy than ever before.

CHALLENGE 8
Security With Untrusted Components
How can we make and keep systems reliable and robust even when using older hard- and software?

CHALLENGE 9
Intelligent Security Systems
Security is a process, not a state. How can we stay ahead of potential attacks and be resilient even when unforeseen things happen?

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.

https://casa.rub.de
Well, here we go. The first of the three Hub C Challenges.

WOW. THIS IS STARTING OFF PRETTY UNIQUE. WHERE AM I?

AND WHAT ARE THESE CREATURES CONFINED WITHIN THE CONTAINERS? SOME OF THEM REMIND ME OF SPACE INVADERS, BUT SOMEHOW PERPLEXED.

HA, I KNOW THEY CAN LOOK KIND OF CREEPY, SORRY! YOU ARE LOOKING AT ONE PIECE OF OUR ATTACKS COLLECTION! WE ARE USING THEM TO WORK OUT HOW TO BUILD SECURE SYSTEMS FROM SCRATCH.

HI CHAP! CAN I HELP YOU?

HUH. ACTUALLY YES. WHAT IN CARROTS NAME IS THIS?
THAT'S TRUE AND AND EXACTLY THE REASON WHY I'M HERE.

I REALlY THOUGHT wE WERE muCH FuRTHER ALONG…

I AM bEtty, NICE To mEET You!

DESpiTE MANy yEARS oF INTENSIvE RESEARCH AND DEVELOPMENT ON SECURE COMPUTER SYSTEMS, THE NUMBER OF SUCCESSFUL ATTACKS CONTINUES TO INCREASE EVERY YEAR.

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!
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 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 vendors, 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.

YOU HAVE GOT A TRAINING ARENA?!

RESEARCH PROJECT

Memory Safety

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!
WE HAVE HIGH HOPES FOR WHAT IS CALLED MEMORY TAGGING. IT WILL BE AVAILABLE WITHIN THE NEXT FEW YEARS IN ARM PROCESSORS AS A HARDWARE-ASSISTED IMPLEMENTATION. HOWEVER, THIS STILL LEAVES THE MAJORITY OF DESKTOP AND SERVER SYSTEMS RUNNING ON UNPROTECTED INTEL PROCESSORS. WHILE SOFTWARE-ONLY MEMORY TAGGING WOULD BE IMMEDIATELY AVAILABLE FOR MILLIONS OF DEVICES, THERE ARE SOME MAJOR HURDLES TO OVERCOME; SOFTWARE INCOMPATIBILITY AND ESPECIALLY PERFORMANCE DEGRADATION.

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.

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.

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.

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.

See you soon, hehehe!
Every day, we work with complex software systems that have been developed over the past decades: such so-called legacy systems...

...on the other hand, we design methods to harden the underlying execution environment of a system to make it resilient against different types of (software-based) attacks...

...on the one hand, we are exploring new security testing methods that can proactively detect vulnerabilities at scale before attackers can do so...

...were often designed without considering security aspects and are vulnerable to attacks...
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.

WOW, IT’S REALLY BUSY. PEOPLE SEEM TO BE INTERESTED IN YOUR WORK... WHAT’S HAPPENING OVER THERE?

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.

I’M BETTY. SOUNDS BRILLIANT! OFF WE GO!

NO WORRIES! I’M PHIL AND I’M PHD STUDENT HERE. AND YES, THERE IS SOMETHING ON MY MIND THAT REPRESENTS THIS RESEARCH AREA QUITE WELL.

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.

AND WE WILL DEVELOP SECURE AND NON-DISRUPTIVE METHODS FOR RUNTIME PATCHING. THANK YOU FOR YOUR ATTENTION! NOW PLEASE ENJOY OUR OPEN HOUSE, GET IN TOUCH WITH OUR STAFF AND REMEMBER: ALWAYS STAY CURIOUS!
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!

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?

This reveals a vulnerability - for example, a so-called buffer overflow - that an attacker can potentially exploit.
WE USE A SIMILAR APPROACH HERE, HOWEVER WE'RE FACED WITH THE CHALLENGE HOW TO MOST EFFICIENTLY IMPLEMENT OUR FUZZING METHODS. WE WANT TO EXECUTE THE TESTS HUNDREDS OR EVEN THOUSANDS OF TIMES PER SECOND. THIS ALLOWS US TO EFFICIENTLY TEST HOW A PROGRAM RESPONDS TO RANDOM INPUT.

TO BE OR NOT TO BE: THAT IS THE QUESTION!

Fuzzing Attacks

With fuzzing we have been quite successful in automatically detecting vulnerabilities in different operating systems, web browsers and software libraries.

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.

HA, HA, MY SECOND COUSIN IS AN AMERICAN FUZZY LOP TOO, AS IT IS ALSO A RABBIT BREED.

YES, ACTUALLY IT IS. AND HERE'S THE LAB.

“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.
Our goal is to dig deeper into a program’s functionality to find vulnerabilities that are difficult to locate.

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 know about such security vulnerabilities. Without that knowledge, it’s fairly impossible to develop proper defenses.

Wow, there are secret backdoors to discover here!

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.

Fuzzing Defenses

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.
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.

**IT IS WELL KNOWN THAT MUTATIONS ARE PART OF EVERYDAY LIFE IN BIOLOGICAL SYSTEMS. BUT THEY ARE ALSO PART OF COMPUTER SECURITY RESEARCH.**

**I HOPE IT MUTATES INTO GREATER SECURITY!**

I HOPE YOU ENJOYED THIS LOOK BEHIND THE SCENES. HERE'S A LITTLE TOOL FOR YOU TO STAY AHEAD OF THE ATTACKERS.

THAT'S KIND! IT'S SCARY TO HEAR ABOUT ALL OF THESE PROBLEMS. BUT IT'S GOOD TO SEE THAT WE ARE NOT HELPLESS.

YOU'RE RIGHT! MY COLLEAGUES ARE ALSO USING UP TO DATE MACHINE LEARNING TO TACKLE THE PROBLEM FROM ANOTHER PERSPECTIVE. JUST GO AHEAD AND ASK FOR MAE.
IN OUR DEPARTMENT, WE EXPLORE HOW MACHINE LEARNING, OR ML FOR SHORT, CAN BE USED TO BUILD INTELLIGENT SECURITY SYSTEMS THAT CAN ADAPT TO NOVEL THREATS AND ATTACK VECTORS. WE ALSO AIM TO IMPROVE THE EXPLAINABILITY AND TRANSPARENCY OF ML ALGORITHMS SO THAT HUMANS CAN BETTER UNDERSTAND AND USE THEM IN PRACTICE. AND THERE HE IS, M.L., ONE OF OUR MOST IMPORTANT EMPLOYEES: WHY DON’T YOU ALSO SAY A FEW WORDS?

SURE, MAE. I AM M.L, A BRANCH OF ARTIFICIAL INTELLIGENCE. I LOVE MY OCCUPATION HERE, WHERE I CAN DO WHAT I LOVE ALL DAY: LEARN! EVERYTHING! MY METHODS HAVE BEEN SUCCESSFULLY USED IN MANY AREAS, AND I AM EXCITED TO SEE WHAT THE FUTURE HOLDS FOR ME.

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.

COOOOOME OON, TEN MORE PUNCHES!

Puh, that’s a tough one. She said “Hello”.

HALLO!
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.

Study novel methods for building robust and resilient ML algorithms.

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:

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.
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 nonlinear 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.

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. In 2016, AlphaGo, a computer program developed by Google DeepMind, beat the world champion Lee Sedol in Go.

Today, ML methods even regularly beat human players in real-time strategy games such as StarCraft 2.

Does that mean I will never be a champion?

Would you like some advice?

By the way: I am still M.L. – I just have a variety of manifestations.

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

---

**SPEECH RECOGNITION SYSTEMS**

As already mentioned – computer systems are exposed to attacks. We research extensively, for example, speech recognition systems and how they can be manipulated. But let’s first have a look at how they work.
Actually, now I remember something that happened to me a while ago...

Can you play with me and get me a doll house?

Sure!

I love you so much!

Days later...

What happened here, honey? Who ordered a doll house and cookies?

Oh, oh!

And that’s how a cute conversation between a girl from Texas and a speech recognition system ended in the ordering of an expensive doll house and four pounds of cookies!

Ha, ha!

HA, HA!

Obviously, she is not the only person whose smart speaker reacted to the TV.

Okay!

Okay!

I’ve learned my lesson!
Within Casa, we focus on audio adversarial examples: we want to create an audio signal that a human understands as a certain sentence 'A' while a machine recognizes a completely different sentence 'B'.

Our attack can be successfully played through the air from a loudspeaker to a microphone.

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.

OK...if you say so: command "open all doors" executed!

Oh, no! Also the door to my carrot stash?!
But don’t fear! We are also able to develop novel mechanisms to defend against audio adversarial examples.

Hey, there is M.L. again! He is very diligent.

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.
INTERESTED IN SEEING ANOTHER SPECIAL PROJECT WE ARE WORKING ON AT CASA?

YES, SURE! THE MORE I KNOW THE SAFER MY CARROTS WILL BE!

**Deepfakes**

WOW... WAIT, WHAT?!? THAT NEVER HAPPENED! I PROMISE. OH DEAR, WILL I EVER BE ABLE TO GO HOME AGAIN?

HA, HA! WELCOME TO THE WORLD OF DEEPFAKES. REMEMBER WE TALKED ABOUT DEEP NEURAL NETWORKS? THESE DEEPFAKES WERE MADE POSSIBLE BY GENERATIVE ADVERSARIAL NETWORKS.

The generator creates candidates. Its goal is to learn to produce results that can fool the discriminator.

**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. Deepfakes 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** (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.

The discriminator evaluates the generator's output. It is trained to distinguish the results from the real data given to him in advance.

I AM SUCH AN ARTIST! I GET BETTER AND BETTER BY COPYING.
SOON you will not be able to reliably distinguish between fake and real content!

THE Queen’s Facial Expressions and especially her lip movements were artificially created, while the rest was performed by an actress.

That’s why, as part of our research, we investigate how deepfakes can be detected, and how Machine Learning can help us to do so.

I really almost can’t tell a difference.

My husband and I love to Netflix and chill...

UH... CREEPY! IF THEY CAN DO THAT WITH THE QUEEN... WHAT ABOUT ME AND MY FELLOW RABBITS?

In December 2020, UK based Channel 4 released an alternative Queen’s Christmas video, created using deepfake techniques. Deepfakes 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.

DO YOU THINK YOU CAN TELL FAKE IMAGES FROM REAL ONES? TEST YOURSELF AND LEARN MORE ABOUT HOW TO SPOT THE TINY DIFFERENCES.

whichfaceisreal.com
Within CASA, we have developed a novel technique to reliably detect deepfakes. 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 deepfakes – 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!

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?

I’M JUST CHANGED MY PASSWORD TO CARROT123 – ISN’T THAT ENOUGH?

OH DEAR, WE HAVE A LOT OF WORK TO DO!

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?
I NEED TO TELL ALL THE OTHERS...
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

**TECHNICAL BACKGROUND**

**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


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.

https://casa.rub.de
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!