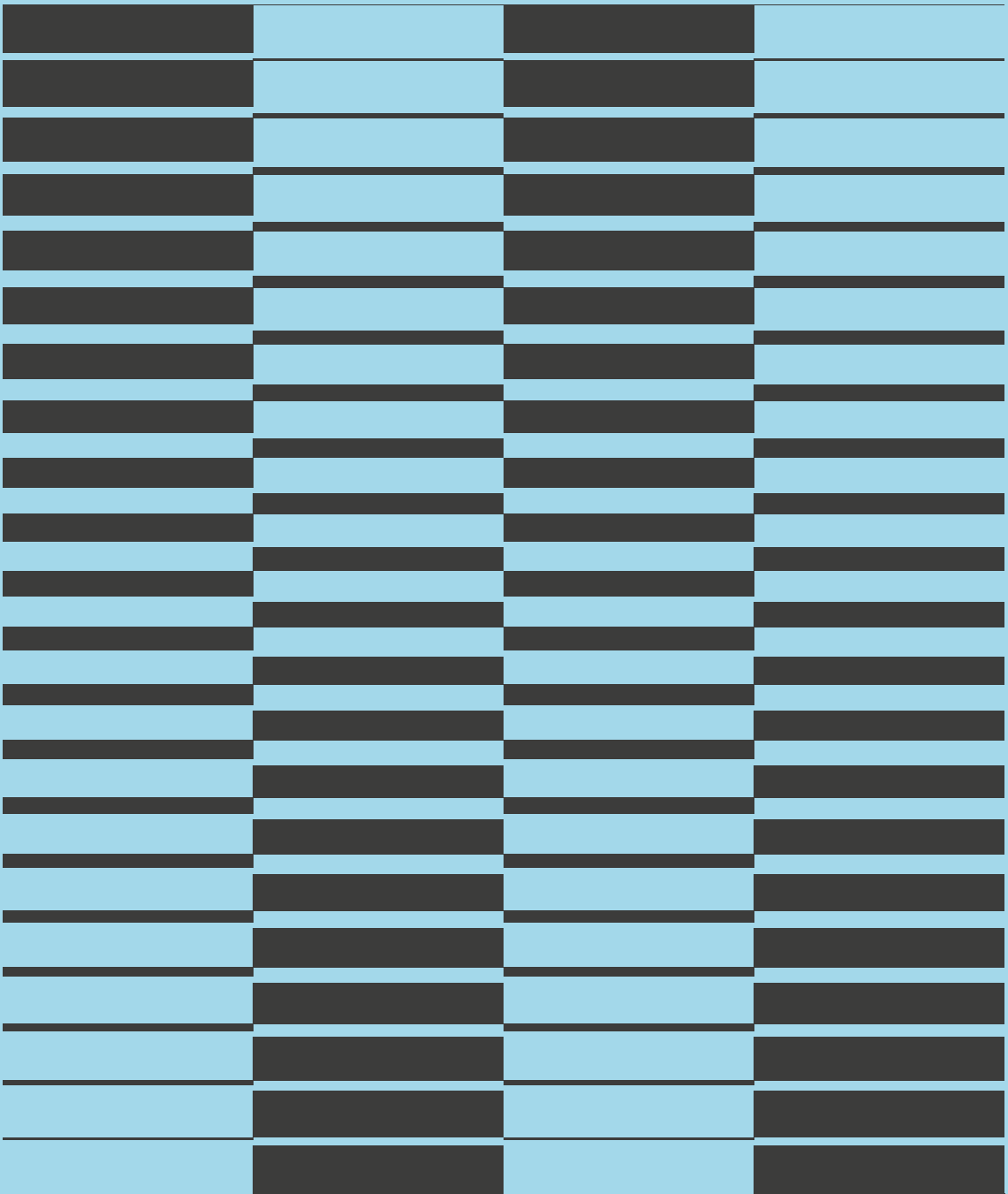
CISPA DISPLAY

EN

EDITION 2025



INTRODUCTION

Research thrives on curiosity, critical thinking and the pursuit of knowledge. Yet, to truly harness its potential, we must bridge the gap between research and society. In an era where information is available at unprecedented speed and scale, it is crucial to make scientific insights accessible and comprehensible. With this second edition of the CISPA Display, a scientific yearbook, we aim to offer you a glimpse into the topics that have inspired and challenged us and our researchers at CISPA throughout 2024. We aim to showcase the broad range of our research and highlight CISPA's societal contributions.

The Importance of Science for Society

In a democratic society, knowledge is not an end in itself. Instead, it serves as the foundation for making informed decisions, finding solutions to pressing challenges and shaping a future worth living. The scientific findings from CISPA on the security of IT systems and the design of trustworthy artificial intelligence, for example, can help protect personal information and critical infrastructure, and develop transparent and fair algorithms capable of making understandable decisions. But who benefits from our research if we fail to communicate it effectively?

Challenges in Science Communication

Presenting complex content in a way that is both understandable and relevant – without losing the precision it requires – is one of the greatest challenges in science communication. As communicators, we have to strike a balance between clarity and depth. In our communications department, we work closely with our researchers to distill the essence of their work and convey it without losing important nuances. At the same time, we often encounter the limits of what can be easily explained – not because the research is inaccessible, but because its depth demands patience and detailed exploration.

In today's media landscape, often dominated by quick headlines and easily digestible content, the subtleties of science can easily get lost. Effective, well-founded science communication requires time, resources, and, above all, an understanding that knowledge cannot always be reduced to simple answers. Our aspiration is not only to deliver results, but also to illustrate the road that our researchers have taken. Only in this way can we build trust in the scientific process.

With the CISPA Display, we aim to build the necessary bridge between science and society. This yearbook seeks to demonstrate how our research generates momentum

With the CISPA Display, we aim to build the necessary bridge between science and society. This yearbook seeks to demonstrate how our research generates momentum for societal questions.

for societal questions. It is about sparking curiosity, fostering reflection, and making the relevance of scientific knowledge visible in our everyday lives.

The limits and responsibilities of research

Science is a source of knowledge. It can create insights, provide guidance and create the basis on which informed decisions regarding current challenges can be made. Examples like climate change, the threat of targeted disinformation and the protection of our most sensitive data demonstrate that research findings often lead to viable solutions only through interdisciplinary collaboration. While research can and should offer impetus, implementation ultimately lies in the hands of society as a whole.

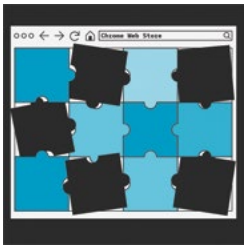
The Value of Science

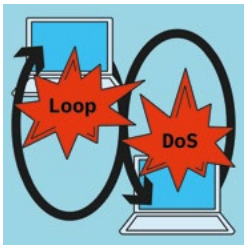
In conclusion, we want to thank our researchers. Collaborating with them is incredibly enriching for us as communicators. It is only through their dedication, thirst for knowledge and tireless work that a publication like the CISPA Display is possible.

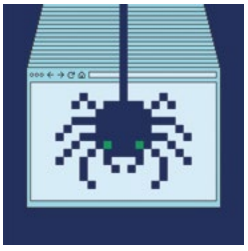
We hope that this yearbook provides not only insights but also the pleasure of exploring the diversity and depth of our research, helping to highlight the value of science for our society.

CONTENTS

CONTENTS







© Lea Mosbach

Online shops, social media accounts, online banking – internet users need passwords everywhere. These passwords should be as long and complex as possible in order to secure the accounts adequately. That is either a mammoth mental task or, even worse, means creating an endless pile of sticky notes with passwords. Password managers can help here. However, the added security they provide is often not fully realized in practice, as correctly setting up the tools is often cumbersome and time-consuming. This is shown in a qualitative study by CISPA researcher Sabrina Amft, who works in the team of CISPA-Faculty Professor Dr. Sascha Fahl in Hanover. She presented her paper paper "'Would You Give the Same Priority to the Bank and a Game? I Do Not!' Exploring Credential Management Strategies and Obstacles during Password Manager Setup" at the Symposium on Usable Privacy and Security 2023 (SOUPS).

How password managers need to improve

Sabrina Amft

Password managers are much more than just the digital equivalent of a password notebook. The programs not only store the login data for various internet services, but they also have two other useful functions: They can generate very strong and complex passwords for users and they are able to verify whether users are actually logging in on the intended website or on a fake site. “For the helpful functions of these programs to really work, users have to set them up correctly. And often, that’s a lot of work”, says Sabrina Amft. Whilst Amft’s study does not provide representative figures, she is interested in taking stock of how the tools are actually used and what obstacles are encountered when configuring them. In collaboration with research colleagues from CISPA, Leibniz University, George Washington University and Paderborn University, she surveyed 279 users of password managers and examined the functionality of 14 popular tools.

Managing passwords on an assembly line

“In our experience, users often modify one password and use it for many accounts. It is also not uncommon for this to be rather weak. Password managers allow them to create a unique, complex password for each account and manage it easily. However, they must first create a new password for their existing accounts and save it in the password manager. With an average of 100 internet accounts per person, this is no easy task”, Amft explains. Thus, it is not surprising that her study shows that users usually do not include all their internet accounts in the programs. “What is surprising, however, is that they don’t do this for conflicting reasons. For example, some stated that they do not add unimportant information to the password manager because security is less relevant. Others, for example, did not enter important data such as their online banking password because they don’t trust password managers enough.”

Justified concern or overcaution?

There have been attacks on major password managers such as LastPass or Norton in the recent past. “So, the users’ concerns are not entirely unfounded”, says Amft. According to the researcher, the consequences of such attacks can vary. “If the providers have proper encryption, hackers can steal the encrypted data set, but ultimately they have to put a lot of energy into trying to access the data.” A report in the IT trade magazine Heise from September 2023 shows that attackers are not shying away from this effort. Cybercriminals can now crack password

vaults and thus obtain access data to crypto wallets and empty them. In January 2023, Norton Life Lock warned its users that hackers had attempted to gain access to customer data by trying out popular passwords en masse – and were successful in some cases. All the more reason to protect the password managers themselves with a powerful password. Despite the two cases, it is clear to Amft that the decision against password managers is generally the worse choice: “Weak passwords used for more than one account are a much bigger security problem than password managers. Not least because incidents with password managers are communicated and compromised data is reported.”

Convenience over security

Amft’s survey of password manager users confirms what has been shown in many other studies: Convenience takes precedence over security for most users. Many of those surveyed stated that they used the tools primarily because they wanted to save themselves the trouble of entering and managing passwords. “Security is more of a secondary factor for them”, says Amft. It is therefore not surprising that almost none of the study participants chose the most secure way of entering all accounts and updating the associated passwords to a stronger alternative. The majority of users, on the other hand, stated that they only transfer accounts and their passwords to the password manager when they visit the relevant sites in their everyday lives. “In addition to the fact that entering all accounts directly is very time-consuming, the fact that many users do not have an overview of their online accounts plays a role here”, explains Amft. The majority of respondents stated that they had replaced at least some passwords with more secure alternatives.

Integrated password managers are used differently

Differences in usage behavior were particularly evident in the comparison between password managers that were purchased separately and those that were integrated into most browsers today. “People are often not even aware that they are using a password manager when they store their passwords in Google Chrome or Mozilla Firefox, for example.” Passwords are rarely entered manually into the integrated versions of the programs. Convenience and efficiency are even more important to their users. “It’s actually a good sign when security tools are designed in such a way that users hardly notice that they are using them. In the past, the integrated versions of password managers were unfortunately often not secure enough, but there has been progress in recent years.”

Recommendations for developers

"Some providers already took promising approaches. For example, some password managers scan websites visited by users and their email accounts in order to generate a list of suggestions for where a password has been created in the past. If such scans run locally, they can also be implemented in compliance with data protection regulations", explains Amft. Displaying popular pages could also be a solution if scanning is not possible. "We also need more automation overall. The process of adding and updating passwords must be as smooth as possible. Importing existing passwords must also be secure. Password managers should offer their own interfaces for this so that no local password lists have to be stored in plain text." According to Amft, developers could counter the mistrust of programs by introducing data protection labels that evaluate the encryption and other security mechanisms used and give users an easy way to assess the security of the programs.

Amft, Sabrina; Hölter-vennhoff, Sandra; Huaman, Nicolas; Acar, Yasemin; Fahl, Sascha (2023): "Would You Give the Same Priority to the Bank and a Game? I Do Not!" Exploring Credential Management Strategies and Obstacles during Password Manager Setup, In: SOUPS 2023, 6-8 Aug, 2023, Anaheim CA, USA, Conference: Symposium on Usable Privacy and Security

People use online security mechanisms for a variety of reasons. In some cases, different mechanisms are even combined. For example, when a VPN connection is used in addition to the Tor anonymization network. It is often unclear where the information comes from that a certain combination is useful and actually offers more security. Matthias Fassl, from the team of CISPA-Faculty Dr. Katharina Krombholz, has investigated how often users choose this combination and what they expect from it. He published his results in the paper "Investigating Security Folklore: A Case Study on the Tor over VPN Phenomenon" at the Conference on Computer-Supported Cooperative Work & Social Computing 2023 (CSCW) and received an Honorable Mention Award and a Methods Recognition.

The example of Tor and VPN: Cybersecurity between fact and folklore

Matthias Fassl

Tor and VPN are two IT applications that almost everyone has probably heard of. They are often topics of media discourse and, in the case of VPNs, have a broad user base. Tor is a network that enables anonymous communication. Its best-known tool is the Tor browser, which allows users to surf the internet anonymously, explains CISPA researcher Matthias Fassl. VPN is the abbreviation for Virtual Private Network. It is a virtual network that sets up encrypted data connections between two servers. It's a recent phenomenon that users combine the two applications, technically described as “Tor over VPN”. “We came across this idea in online forums and were wondering how many people actually use it”, says Fassl. “First of all, it is the combination of tools that is interesting. As the tools were not developed for this purpose, we don’t fully know what happens when they are used together. And for our research on Usable Security, it is exciting to learn about the users’ perception of the benefits of combining the tools”, continues Fassl. Usable security is a research area of cybersecurity that focuses less on the applications themselves, but on how people use them.

Three-step approach

In order to find out what the phenomenon of “Tor over VPN” is all about, Fassl and his colleagues followed a three-step approach. “We first investigated how many people use this combination”, Fassl explains. By taking measurements at the nodes of the Tor network, he and his team were able to find out that 6.23 percent of the connections to the Tor network originate from VPNs. “In a second step, we conducted a survey to find out what people expect from the combination and whether they intend to achieve certain security benefits”, Fassl continues. It turned out that there are two different types of users: those who always use a VPN, regardless of the context, and those who establish a VPN connection specifically for the Tor network. The second group was particularly dominant, expressing a variety of motivations such as the wish to bypass geo-blocking (blocking access to websites from certain geographical regions) or to hide IP addresses. “Finally, we searched online media, social media, etc. for articles and discussions on the topic to find out how the combination of the mechanisms is addressed there”, Fassl explains. Many recommendations descri-

be the combination of Tor and VPN but lack explaining the actual benefit. According to Fassl, the belief of many users that access via VPN would protect them from the dangers of the Tor network can be attributed to the role of the VPN providers. Those would exaggerate the threats within the Tor network, like dark net markets for illegal products, in order to promote their products. “It is evident that a VPN is not required for using the Tor browser securely and anonymously”, Fassl says. “Possible security benefits of ‘Tor over VPN’ remain unclear to this day.”

»We would, of course, prefer if people were using security mechanisms that met their needs and because they understand the effects. This is obviously not the case in reality.«

The notion of security folklore as an explanatory model

In order to explain why users combine Tor and VPN anyway, Fassl and his colleagues use the notion of security folklore. By this Fassl means "the transfer of practices and tips about security and privacy in social groups. This can be explicit, but it also often happens implicitly by stories or demonstrations, and it does not necessarily have to be in writing." If users read a post about the topic on social networks, or if they see someone using this combination in a movie, it can solidify their perception that the practice is useful. The tale of the combination of Tor and VPN offering more security would then be a so-called security folklore. This is reinforced by normative beliefs. People are more inclined to apply certain security mechanisms if they have observed them with others.

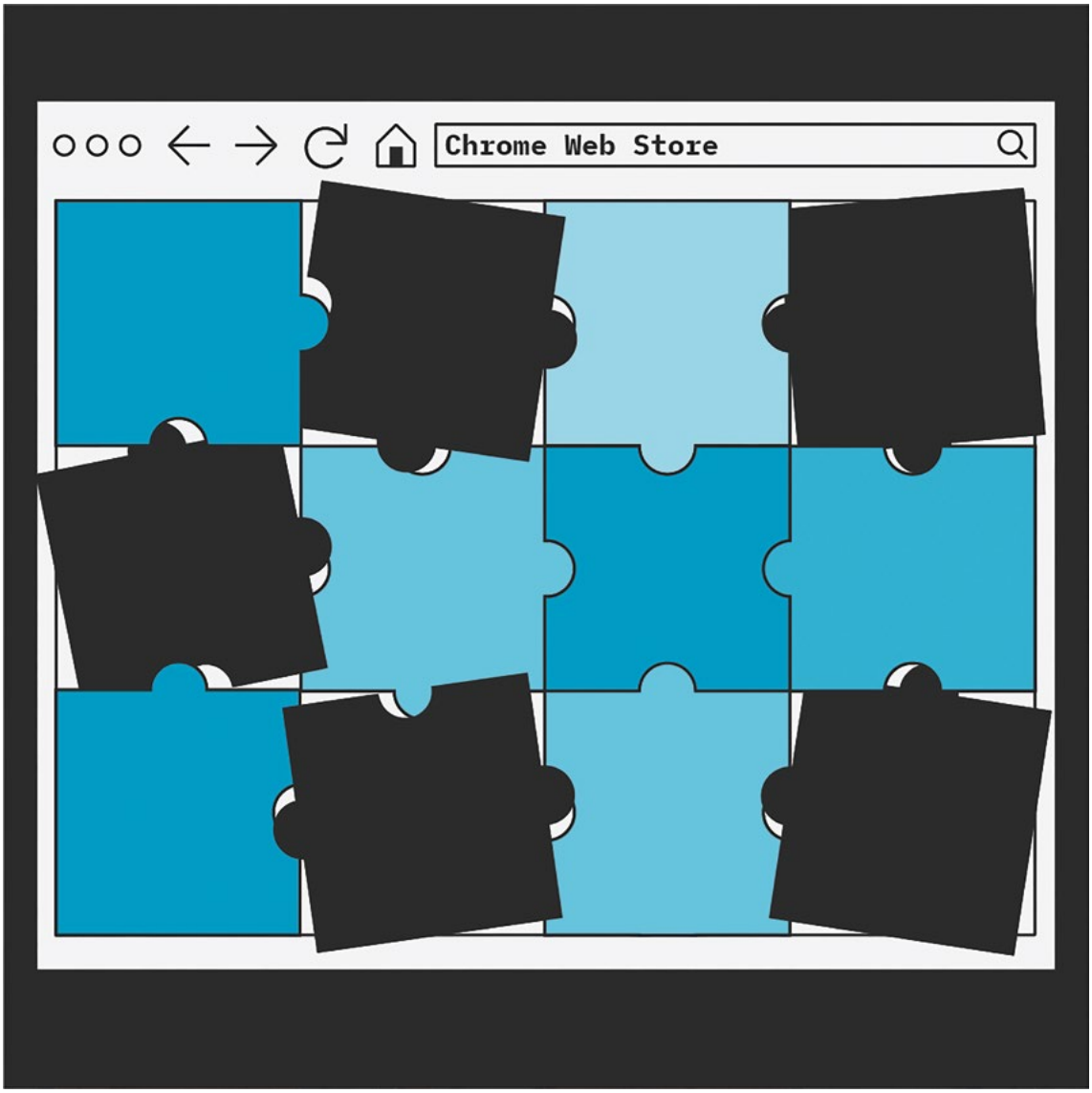
Takeaways for cybersecurity research

For cybersecurity research, the result is interesting because it shows that besides factual information by experts, the pop-cultural understanding of security mechanisms and the media discourse about them play an important role. But what are the consequences for research? "For us as researchers, this makes it a little more difficult", Fassl explains. "We would, of course, prefer if people were using security mechanisms that met their needs and because they understand the effects. This is obviously not the case in reality. People do things for all kinds of reasons, even if they don't understand them." However, working against this is a major challenge: "If, for example, we see that security mechanisms are shown on pop-cultural media like TV series, we can work towards better or more generally applicable methods being presented there." Fassl certainly sees a need for more research in this area: "I am fascinated by social dynamics and the influence of social norms. That's why I would like to take a more systematic look at how security mechanisms are addressed in Hollywood movies and Netflix series." We can look forward to seeing what he brings to light.

Fassl, Matthias; Ponticello, Alexander; Dabrowski, Adrian; Krombholz, Katharina (2023): Investigating Security Folklore: A Case Study on the Tor over VPN Phenomenon. In: CSCW 2023, 14-18 Oct, 2023, Minneapolis MN, USA, Conference: Conference on Computer-Supported Work and Social Computing

Researcher: Matthias Fassl
Author: Felix Koltermann

Publication date
29.01.2024



© Janine Wichmann-Paulus

Millions of users use browser extensions on a daily basis, for example, to block advertisements on websites. But is the use of extensions from third-party providers secure at all? CISPA-Faculty Dr. Aurore Fass together with her students Sheryl Hsu and Manda Tran, has investigated this question based on extensions for Google's web browser Chrome, thus providing the first large study on the Chrome Web Store. The related paper "What is in the Chrome Web Store?" was presented at the ACM ASIA Conference on Computer and Communications Security 2024.

Security vulnerabilities of browser extensions in the Chrome Web Store

Aurore Fass

To access the internet, users need a web browser like Chrome, Safari, Mozilla Firefox, or Microsoft Edge. If the browsers' default features are insufficient, third-party extensions can be used. "Browser extensions are very useful for extending browser functionality. If you add extensions such as an ad blocker, for example, you can block or restrict advertising on websites", explains CISPA-Faculty Dr. Aurore Fass. The extensions can be downloaded via the browser and installed with just a few clicks. Since all popular web browsers offer extensions, the CISPA-Faculty decided to investigate the Chrome Web Store. "We use Chrome because it is the most popular browser", she explains. "And Chrome has a WebExtensions API that works across all browsers. Therefore, from a developer's perspective, the extensions for Chrome and Firefox are very similar." Another important factor was that a tool named "Chrome-Stats" facilitates data access for Chrome. "Chrome-Stats collects longitudinal data for extensions in the Chrome Web Store. This was very important because as soon as an extension is removed from the store, we no longer have access to the metadata or the source code of these extensions", Fass continues.

The array of security-noteworthy extensions

For her investigations, the researcher distinguishes between benign and security-noteworthy extensions (SNEs), classifying the latter into three categories. "First, there are extensions that contain malware", Fass explains. "Those extensions are malicious in the sense that they were specifically developed by people who want to harm users. The second category is extensions that violate Google's data protection policy. And the third category are vulnerable extensions." Although the latter were created by developers with good intentions, they contain errors that can result in security vulnerabilities. The danger of SNEs is that they can be used by attackers to send malware, track users, spy on them or steal data. Fass and her colleagues analyzed extensions available in the Chrome Web Store between July 2020 and February 2023.

Lifetime and security risks of extensions

Fass' first important finding was that extensions have very short life cycles. "60 percent remain in the Chrome Web Store for less than a year", Fass explains. "This is crazy! You need regular analyses to know what is available in the store." The second finding relates to the presence of security-noteworthy extensions. "We have analyzed many security-noteworthy extensions in the Chrome Web Store that affect hundreds of millions of users", Fass continues. "Some of them remain in the store for ten years, thus compromising the security and privacy of users for a very long time." The third finding refers to the similarities between extensions. "Using clustering algorithms, we were able to identify extensions with a similar code base", Fass explains. "This helps us detect security-noteworthy extensions. Because if an extension is similar to a security-noteworthy extension, we can strongly assume that it is also security-noteworthy. This can help to identify previously unknown security-noteworthy extensions." The last finding is related to the lack of maintenance of the Chrome Web Store. "60 percent of the extensions have not been updated since their publication in the store. This means that they do not profit from Chrome's new APIs or features that improve security and privacy, like the new Manifest V3", Fass says.

»We have analyzed many security-noteworthy extensions in the Chrome Web Store that affect hundreds of millions of users.«

Findings about the source code of extensions

In a further step, Fass examined the source code of the extensions in the Chrome Web Score more closely. This was motivated by the assumption that searching for similar source code can help discover SNEs more easily and quickly. In fact, Fass discovered thousands of clusters with similar source code. This is not surprising, as developers often rely on pre-written code in their work, known as libraries, which are used to perform specific tasks and reduce the amount of programming effort needed. “30 percent of the browser extensions use a vulnerable library in their source code”, Fass explains. “Although we did not examine whether this can actually be exploited, we still think it is bad practice to use these vulnerable libraries. Because they are waiting for something bad to happen.” The problem is that the third-party code developers use is not maintained. “This results in using outdated, unmaintained code that could contain security vulnerabilities”, Fass says. In particular, developers often use code from a Tool called Extensionizr.

What can users, developers and Google do?

When asked what developers could do to make their extensions more secure, Fass replies: “Developers with good intentions should become aware of what can go wrong with extensions. It would be good if they thought about threat scenarios and what could be gateways for attackers.” Regular updates are also an important factor. For the users, things are trickier. “There are few means for them to find out whether an extension is dangerous or not”, Fass explains. “In theory, you can check the extensions’ permissions, but most have never dealt with this and do not understand the details.” This makes the monitoring by Google even more important. “Google has a monitoring system that checks extensions before they are published in the Chrome Web Store”, she continues. Fass even has an idea on how to improve the monitoring system: “In a previous paper, I show how vulnerable extensions could be detected automatically. This could be included in Google’s pipeline.”

Hsu, Sheryl; Tran, Manda; Fass, Aurore (2024): What is in the Chrome Web Store?. In: 18th ASIACCS 2023, 10-14 July 2023, Melbourne, Australia. Conference: ACM ASIA Conference on Computer and Communications Security

Clickbait PDFs are even worse than clickbait headlines: They are a new type of phishing attack, first studied by CISPA researcher and PhD candidate Giada Stivala and her colleagues. Clickbait PDF files do not contain any malware per se – instead, they try to coax users into clicking somewhere in the file, leading them to malicious web pages that have the potential to steal their data. Stivala and her colleagues were the first to examine clickbait PDFs in detail. They published their findings in a paper entitled "From Attachments to SEO: Click Here to Learn More about Clickbait PDFs!" at the Annual Computer Security Applications Conference (ACSAC) 2023.

This article will change your life! – Clickbait PDFs are the latest phishing scam

Giada Stivala

Just imagine: You've missed the deadline for your tax declaration. You open up your favorite search engine and type in the name of the tax form you're looking for. Annoyed and in a hurry, you click on the first PDF the search engine spits out. A captcha appears, instructing you to confirm that you're not a robot. You try to tick the box, but suddenly you're redirected to a web page that gives you all sorts of pop-ups, none of them looking very reassuring. With some bad luck, your device might now be infected. You have fallen prey to a clickbait PDF, a new type of phishing scam that aims to steal your data.

The latest phishing scam, disguised as a PDF

Clickbait PDFs are a perfect example of the proverbial cybersecurity "cat-and-mouse game": Hackers think of new attacks and deploy them, cybersecurity researchers develop countermeasures to stop the attacks, hackers in turn work around the countermeasures, continuing the cycle ad infinitum. Phishing scams themselves are nothing new – most users have probably encountered them in the form of sketchy emails that claim to be from their bank, asking them to enter login credentials or prompting them to visit sketchy websites that can infect their device. But as email clients get better at detecting and sorting out phishing mails, and web browsers block malicious web pages more effectively, scammers are looking for new ways to steal user data. "These existing protection mechanisms work pretty well, so attackers have to be ahead of the system and try not to be detected", says CISPA researcher Giada Stivala.

Clickbait PDFs bypass detection mechanisms

With the introduction of clickbait PDFs, scammers have found a new way to get ahead of the curve. "PDFs were already known to represent a threat to users, but these PDFs then contained malware", says Stivala. These files were usually emailed to users, and if opened, they would run code that infected user devices. As this kind of attack is already well-known and studied, malware scanners have gotten quite adept at catching them and warning users. Clickbait PDFs, however, do not contain malware. Code-wise, they are indistinguishable from

benign PDF files, such as a genuine tax declaration form. As normal detection mechanisms fall short of detecting their malicious intent, they can be listed in ordinary search results. Users looking for a specific file, such as a manual for a printer, might thus encounter a Clickbait PDF with a simple search query, as Stivala explains.

Designed to "steal your click"

Stivala and her colleagues were first approached by an industry contact working with large amounts of customer data, whose scanners had suddenly registered an uptick in PDF files. As these PDFs did not contain any malware, their purpose was unclear. Investigating these files, Stivala encountered a plethora of different scams: for example, PDFs pretending to be video players, streaming the newest movies for free or even promising free Bitcoin with just one click. The files are designed to "steal your click", as Stivala puts it. Scammers leverage the fact that all common browsers have integrated PDF support nowadays, so a PDF opens similarly to a regular webpage. Unsuspecting users might not even realize the difference between looking at a PDF or a webpage inside their browser. A single click inside one of these PDFs is enough to lead users to so-called "attack web pages" that might compromise their devices and data. These pages are similar to what users would encounter in a more traditional phishing scheme via email, as the challenge for scammers often is to get users to access their malicious web pages in the first place. "In a sense, the part after the PDF file does not change. But the PDF itself introduces a novelty, because it is harder to defend against", Stivala says.

SEO poisoning fuels clickbaiting attacks

To make sure that people actually encounter their clickbait PDFs in the wild, scammers employ what is called "Black Hat Search Engine Optimization (SEO)" or "SEO Poisoning". "Search Engine Optimization per se is not bad. It can be used for entirely ethical and legal reasons", Stivala says. It is essentially a method of optimizing a web page to make sure it is ranked high in search results. A company might do this for marketing reasons, for example. In SEO poisoning, however, malicious webpages are optimized to be ranked higher even though they are either irrelevant to the user's search query or downright dangerous to their devices. This works, for instance, by including huge numbers of keywords in a page. If a user is searching where to stream a movie for free, including keywords such as the name of the movie would make the page rank higher. Even worse, scammers managed to upload their PDFs to servers of legitimate websites that were insufficiently secured but had a "good reputation", such as pages of local businesses or schools. Because these sites do not appear to be malicious, search engines ranked these

files higher in the search results. And because malware scanners did not flag the files as malicious, affected website providers were not alerted for the most part. “They didn’t even realize that these files were on their servers before we notified anti-phishing entities and website owners”, Stivala says.

User awareness is the best protection

After the researchers notified these entities, things seem to have improved and less clickbait PDFs are featuring among search results. Stivala is currently working on a follow-up study to see how big the threat still is. Until then, what is the best way for users to protect themselves against this type of attack? “There is no silver bullet”, Stivala says. “These attacks exploit what is called the weak link in the system, which is usually the human.” Users can start by paying attention to tiny clues, such as the URL in the browser showing a PDF where there should be a normal webpage. And in general, users should be aware that if something seems too good to be true, such as the latest movies being streamed for free or a webpage gifting you free bitcoin, they’re probably looking at a phishing scam. That goes for webpages as much as for PDFs.

Stivala, Giada; Abdelnabi, Sahar; Mengascini, Andrea; Graziano, Mariano; Fritz, Mario; Pellegrino; Giancarlo (2023): From Attachments to SEO: Click Here to Learn More about Clickbait PDFs!. In: ACSAC 2023, 4-8 Dec 2023, Austin, Texas, USA. Conference: Annual Computer Security Applications Conference

Researcher: Giada Stivala
Author: Tobias Ebelshäuser

Publication date
01.03.2024

Providing a consistent user journey is a key principle in web design. This also applies to implementing new security standards such as two-factor authentication (2FA). For a new study, CISPA-Faculty Dr. Sven Bugiel and his colleague Dr. Sanam Ghorbani Lyastani have developed guidelines on how to compare the 2FA process on websites from a user perspective. They published their results in the paper "A Systematic Study of the Consistency of Two-Factor Authentication User Journeys on Top-Ranked Websites", and presented them at the Network and Distributed System Security Symposium (NDSS) 2023.

New approach to comparing the process of two-factor authentication on websites

Sven Bugiel

Humans are creatures of habit: The more similar processes and everyday actions are, the easier they seem to implement. The same goes for online activities. “When shopping online, we are generally used to the shopping cart being at the top right of the website”, explains CISPA-Faculty Dr. Sven Bugiel. This kind of experience allows users to quickly and easily switch between different websites. This observation described by Bugiel is an important heuristic from the field of user experience, which is also known as ‘Jakob’s Law of Internet User Experience’. While the user experience regarding password-protected login is considered to be fairly consistent, there has not been any research on how this applies to the process of two-factor authentication (2FA) to date. “Many studies have already dealt with individual factors of 2FA”, the CISPA researcher explains. “That is why we wanted to find out what the overall workflow of two-factor authentication looks like.”

Two-factor authentication

But what exactly makes two-factor authentication so interesting? “2FA is one of the technologies that become increasingly important to secure user accounts”, Bugiel explains. “Creating secure and unique passwords is a very difficult task, and 2FA creates a second security barrier.” That means users authenticate themselves with a password and an additional factor when logging in to a website. There is a wide range of methods available for the second level of authentication. They include examples like one-time passwords sent via text message or generated via an app, as well as hardware add-ons that scan fingerprints. Each of these methods comes with its own set of challenges. “A ‘gold standard’ for implementing 2FA has not yet been established”, continues Bugiel.

The CISPA researchers’ study design

In order to compare the process of two-factor authentication on websites, Bugiel and his colleague conducted their study based on the aforementioned “Jakob’s Law of Internet User Experience”. “To find out which websites actually use 2FA, we used the 2FA directory”, explains Bugiel. “This is a community-led data set of websites

that use 2FA in any way. Around 3000 websites are listed there." In order to effectively reduce the number of websites to examine, Bugiel and his colleague used Tranco, a scientific dataset that ranks websites. "We then extracted the top-ranked Tranco websites from the websites listed in 2FA", Bugiel continues. "As a result, our sample consisted of websites that most people are probably familiar with." These included websites such as google.com, amazon.com and icloud.com, which the majority of users might well know.

Comparison factors for 2FA user journeys

In a second step, the CISPA researchers developed factors to compare the websites with each other. "For this, we manually investigated the 85 websites with two researchers and recorded the process on video. We wanted to know, for example, where users first encounter 2FA, where the 2FA settings are located and how the login and logout process works." Based on the data collected, Bugiel and his colleague identified a total of 22 comparison factors, classified into five main categories of two-factor authentication: Discovery, Education, Setup, Usage and Deactivation. The comparison factors for Discovery included, e.g., how the website indicates the 2FA option, if it is mandatory and if there is a common naming. The category Setup included comparison factors such as the confirmation of a successful setup process and the offer of a recovery option.

Results show no consistency in user experience

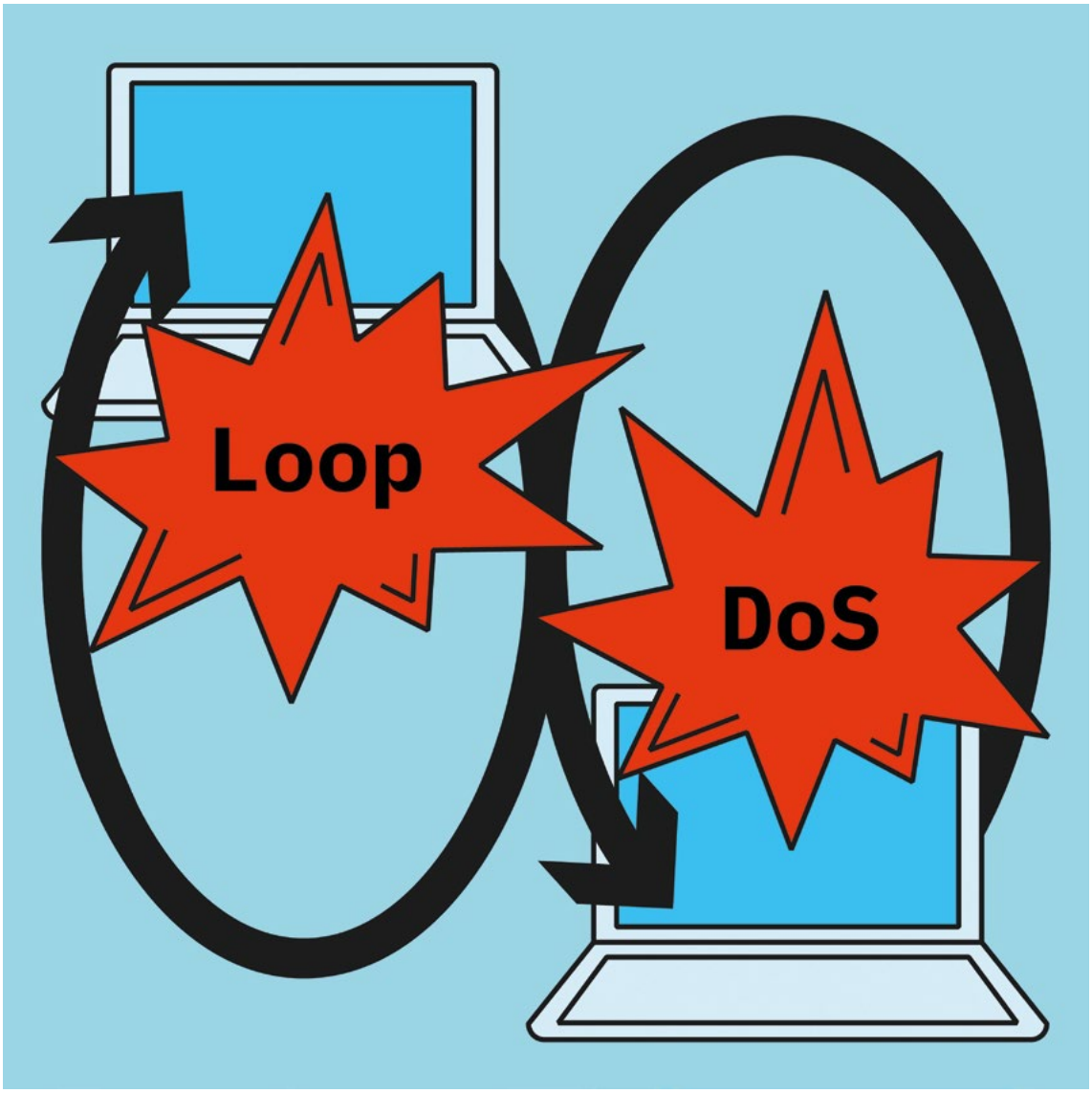
"If you look at the user journey on these top-ranked websites, the key message is that there is no consistent strategy implemented by all websites or even the majority of websites", Bugiel explains. "Instead, there are different strategies that are implemented by groups of websites. These are clusters of usage strategies that we defined in the analysis. This means that the 2FA user journeys are not really consistent." In terms of Jakob's Law, there is a risk that users will not activate 2FA or use the website for these reasons. "The core contribution of our work was to show that these inconsistencies in fact exist", continues Bugiel. "This leads to various new research questions. Our study only allows us to say whether the user experience on different websites is similar or different. However, that does not tell us user-friendly a website is." Taking a closer look at these differences and investigating them directly with users would be the next step. We can therefore look forward to the next study conducted by the CISPA-Faculty's research group.

»If you look at the user journey on these top-ranked websites, the key message is that there is no consistent strategy implemented by all websites or even the majority of websites.«

Ghorbani Lyastani, Sanam; Bugiel, Sven; Backes, Michael (2023): A Systematic Study of the Consistency of Two-Factor Authentication User Journeys on Top-Ranked Websites. In: NDSS 2023, 27 Febr-3 March 2023, San Diego, California USA. Conference: Network and Distributed System Security Symposium

Researcher: ***Sven Bugiel***
Author: ***Felix Koltermann***

Publication date
13.03.2024



© Lea Mosbach

A newly discovered denial-of-service (DoS) attack targets application-layer protocols that draw on the User Datagram Protocol (UDP) for end-to-end communication. 'Application-layer loop DoS attacks' entrap servers of these protocols in so-called loops, pairing them in such a way that they communicate with each other indefinitely. The vulnerability affects both legacy (e.g., QOTD, Chargen, Echo) and contemporary (e.g., DNS, NTP, and TFTP) protocols. Discovered by CISPA researchers, the attack puts an estimated 300,000 Internet hosts and their networks at risk. In August 2024, the paper "Loopy Hell(ow): Infinite Traffic Loops at the Application Layer" will be presented at the Usenix Security Symposium in Philadelphia.

Endlessly looping: New denial-of-service attack targets application-layer protocols

Christian Rossow

The newly discovered loop DoS attack is self-perpetuating and targets application-layer messages. It pairs two network services in such a way that they keep responding to one another's messages indefinitely. In doing so, they create large volumes of traffic that result in a denial of service for involved systems or networks. Once a trigger is injected and the loop set in motion, even the attackers themselves are unable to stop the attack. Previously known loop attacks occurred on the routing layer of a single network and were limited to a finite number of loop iterations.

An estimated 300,000 Internet hosts can be abused

Discovered by CISPA researchers Yepeng Pan, Anna Ascheman and Professor Dr. Christian Rossow, application-layer loop DoS attacks are likely to concern a total of 300,000 Internet hosts. So far, the researchers have confirmed vulnerabilities for TFTP, DNS and NTP implementations as well as for the six legacy protocols Daytime, Time, Active Users, Echo, Chargen and QOTD. These protocols are widely used to provide basic functionalities on the Internet. While NTP, for instance, allows for time synchronization between computers, DNS matches domain names to their corresponding IP addresses. TFTP enables the transmission of files without user authentication.

Attacks can be triggered from a single spoofing-capable host

Application-layer loop DoS attacks rely on IP spoofing and can be triggered from a single spoofing-capable host. "For instance, attackers could cause a loop involving two faulty TFTP servers by injecting one single, IP-spoofed error message. The vulnerable servers would then continue to send each other TFTP error messages, putting stress on both servers and on any network link between them", Rossow explains. Pan stresses the novelty of this attack vector: "The application-level loops we discovered differ from known network-layer loops. Hence, existing packet lifetime checks employed at the network level are unable to interrupt application-layer loops."

Easy to exploit

"As far as we know, this kind of attack has not yet been carried out in the field. It would, however, be easy for attackers to exploit this vulnerability if no action were taken to mitigate the risk", Rossow says. In December 2023, Rossow, Ascheman and Pan disclosed their discovery to the affected vendors and a trusted operator community. The CISPA researchers also coordinated a plan for the publication of an attack-specific advisory and started a notification campaign together with The Shadowserver Foundation.

»As far as we know, this kind of attack has not yet been carried out in the field. It would, however, be easy for attackers to exploit this vulnerability if no action were taken to mitigate the risk.«

Pan, Yepeng; Ascheman, Anna; Rossow; Christian (2024): Loopy Hell(ow): Infinite Traffic Loops at the Application Layer. In: 33rd USENIX Security Symposium, 14-16 Aug 2024, Philadelphia, PA, USA. Conference: USENIX Security Symposium

Researcher: ***Christian Rossow***
Author: ***Eva Michely***

Publication date
19.03.2024

© Chiara Schwarz

It's something of a truism: The quality of any study is only as good as the data collection and analysis that have gone before. This also applies to the handling of qualitative interviews, which are enjoying increasing popularity in cybersecurity research. The more precise the interview transcription, the better the basis for further analysis. A group from CISPA's Empirical Research Support (ERS) were the first to systematically compare the best-known transcription services on the market. They presented their results as a poster and a short paper at the Conference on Computer and Communications Security 2023 (CCS).

Manual transcription (still) beats AI: A comparative study of transcription services

Rafael Mrowczynski

Interviews are a popular method for collecting scientific data. Broadly speaking, a distinction is made between quantitative and qualitative interviews. The former are designed to obtain statistically usable information from a large number of participants using standardized questionnaires, while the latter focus on obtaining interview data that allow for interpretation by the researchers. The guided interview is a special form, where a prepared list of questions exists, but deviations from it are allowed during the conversation. “In cybersecurity research, these interviews are utilized when exploring the patterns of action and interpretation of actors who operate through digital means”, explains sociologist Dr. Rafael Mrowczynski from CISPA’s Empirical Research Support (ERS) team. The ERS team advises CISPA researchers on methodological issues.

Converting audio file into text

Transcription is a crucial step in qualitative data analysis. “The standard procedure is to convert the audio recordings of the interviews into text. It is important for the quality of the data that the transcriptions are adequate”, Mrowczynski explains. Depending on the scientific field, there are different standards for transcription. “In cybersecurity research, we usually work with transcripts that precisely reproduce the content of the conversation”, says Mrowczynski. For this reason, an adequate transcript only contains the relevant spoken words. Researchers have two options for conducting transcriptions: creating the transcripts themselves or within their research team, or outsourcing the task to third-party providers.

Besides manual transcription, there has recently been a real hype about automated, AI-based transcription among third-party providers. This is due to the exponential leaps in development and quality that AI applications have made in many areas over the last two years. The researchers from CISPA’s ERS team wanted to find out which provider achieved the best results and how automated, AI-based transcription performed in comparison to manual transcription. Their goal was to be able to provide CISPA researchers as well as the cybersecurity community with a recommendation for working with qualitative interviews.

The approach of the ERS team

For their research project, Mrowczynski and his colleagues Dr. Maria Hellenthal, Dr. Rudolf Siegel and Dr. Michael Schilling created a test dataset, which consisted of individual interviews lasting about ten minutes and group discussions with CISPA researchers in German and English. The content focused on the research field of cybersecurity. “It was important that technical terms from the community were included so that the precision of the transcription could be assessed”, Mrowczynski explains. In order to better reflect real research settings, background noise was also added to some of the interviews.

In December 2022, the data was sent to eleven providers. Among these were the transcription services Amberscript, GoTranscript, QualTranscribe, Rev, and Scribbl as well as the AI-based transcription providers Amazon Transcribe, AssemblyAI, Audiotranskription.de, Google Cloud, Microsoft Azure, and Whisper by OpenAI. For the assessment of the transcripts, Mrowczynski and his colleagues created a reference transcript that served as the basis for their comparative analysis. The analysis itself then focused on two central criteria. First, the researchers assessed the word error rate, which indicated by how many words a transcript differed from the reference transcript. Second, the qualitative deviation from the reference transcript was coded manually.

Manual transcription services beat AI

In their paper, Mrowczynski and his colleagues conclude that, in general, “most of the manual transcription services achieve a commendable level of performance, while AI-based services often show meaning-distorting discrepancies between recording and transcription.”

The distortion of meaning clearly shows when it comes to technical terms, Mrowczynski explains: “In the transcript, for example, the term ‘hashes’ became ‘ashes’. That is how we came up with the title of the paper.”

OpenAI’s Whisper achieved the best results among the AI-based providers. Most providers handled English better than German, while three providers did not offer German transcription at all. Background noise generally had a negative effect on the results. The AI-based providers particularly struggled with speaker attribution. In addition, transcripts created by AI had to be reformatted before they could be processed further in software for qualitative data analysis. However, the researchers point out that their analysis reflects the state of the art as of December 2022 and that recent developments could not be taken into account.

»It was important that technical terms from the community were included so that the precision of the transcription could be assessed.«

Siegel, Rudolf; Mrowczynski, Rafael; Hellenthal, Maria; Schilling; Michael (2023): Poster: From Hashes to Ashes - A Comparison of Transcription Services. In: CCS 2023, 26-30 Nov 2023, Copenhagen, Denmark. Conference: CCS ACM Conference on Computer and Communications Security

Researcher: ***Rafael Mrowczynski***
Author: ***Felix Koltermann***

Publication date
05.04.2024

© Chiara Schwarz

Zoom is one of the most popular software products for video conferencing in the world. It is used by millions of users every day in the confidence that their data is secure and their conversations cannot be intercepted. So far, this relies on the Zoom servers controlling the access to each of the groups: the Zoom servers check if all group members know the meeting password. Now, there is another way of doing this: CISPA-Faculty Professor Dr. Cas Cremers, his postdoc Mang Zhao and Dr. Eyal Ronen have developed a new method for access control where the Zoom servers do not know the passwords. They will present their paper "Multi-Stage Group Key Distribution and PAKEs: Securing Zoom Groups against Malicious Servers without New Security Elements" at the IEEE Symposium on Security and Privacy (S&P) in May 2024.

CISPA researchers develop new security concept for Zoom groups

Cas Cremers

Since the coronavirus pandemic, video conferencing software such as Zoom has found its way into the private and professional lives of many. Users usually require a password if they want to take part in a group conversation via Zoom. “At the moment, the password is shared with the server to determine who is allowed to participate”, explains CISPA-Faculty Cas Cremers. This, however, is a situation that Cremers does not agree with. Being in possession of the password, Zoom is theoretically able to interfere with the group’s members and add new members at will.

“We’re hoping, of course, that Zoom will say: ‘No, no, that is something that we’ll never do.’ But we don’t have a technical guarantee for this. We can only hope and trust that they won’t do that”, Cremers says. To him, it is important that security is not based solely on trust: “I want technology that is designed in such a way that we can convince ourselves that our connection is secure and that Zoom cannot eavesdrop. This is the guarantee I want to have.” The challenge for him was to develop a solution that did not require a complete redesign of Zoom. “In theory, you could come up with a system completely different to the one Zoom is currently using. But nobody would accept that”, Cremers continues.

Password exchange between users, not with the Zoom server

Cremers and his colleagues were faced with the task of designing a solution in which the Zoom server neither knows all the passwords nor uses them to control access. “Our idea was to no longer share the password with the server, but only with the participants”, Cremers explains. “Users have to be able to establish a secure connection with each other without ever having to share the password outside the group.” To achieve this, Cremers and his colleagues have developed a modified key exchange protocol that is only performed between Zoom users and does not involve Zoom’s servers. The process only takes place within the software, without the users having to actively do anything.

“We use a basic building block called PAKE (Password-authenticated Key Exchange Protocol), which we integrate into the Zoom protocol. We use PAKE to enable groups to perform access control themselves, without relying on the Zoom server”, Cremers explains. Zoom does not

publicly share its source code, so Cremers had to find another way to test his application: “We took the description of Zoom’s software from their white paper.” This is a technical description of the software published by the company itself, which explains the design of the software but does not include all details. “We can’t be 100 percent sure what Zoom actually uses. But from a developer’s perspective, the solution seems to work”, Cremers says.

»We demonstrate that more privacy and better security guarantees are not just a fantasy, but that there is a way to actually achieve them.«

A clear goal in mind: Showing what is possible

Cremers has not yet been in contact with Zoom Video Communications, although he would be open to it. In theory, the security mechanism he developed with his co-authors could be applied to other video conferencing software as well. Its practical implementation, however, is not something he focuses on so much. “In a sense, part of our work is about showing the community what options are available”, he says. “We demonstrate that more privacy and better security guarantees are not just a fantasy, but that there is a way to actually achieve them”. You also could say that Cremers’ research is holding up a mirror to the application-oriented IT industry, showing them what is, and is not, possible using the tools of foundational research. But Cremers also has another, more socio-political goal in mind: “We humans want to communicate in such a way that safeguards our privacy and prevents others from eavesdropping on our communications. This should even include the companies that provide the infrastructure for our communications.” His research ultimately aims to establish this wider societal goal.

Cremers, Cas; Ronen, Eyal; Zhao; Mang (2023): Multi-Stage Group Key Distribution and PAKEs: Securing Zoom Groups against Malicious Servers without New Security Elements. In: 45th IEEE Symposium on Security and Privacy, 20-22 May, 2024, San Francisco, CA, USA. Conference: SP IEEE Symposium on Security and Privacy

© Chiara Schwarz, Janine Wichmann-Paulus

AI-generated images, texts and audio files are so convincing that people are no longer able to distinguish them from human-generated content. This is the result of an online survey with around 3,000 participants from Germany, China, and the USA. This is the first time that a large transnational study has examined this particular form of media literacy. CISPA-Faculty Dr. Lea Schönherr and Professor Dr. Thorsten Holz presented the results at the IEEE Symposium on Security and Privacy 2024 (S&P). The corresponding paper "A Representative Study on Human Detection of Artificially Generated Media Across Countries" was realized in cooperation with Ruhr University Bochum, Leibniz University Hanover, and TU Berlin.

New results in AI research: Humans are barely able to recognize AI-generated media

Thorsten Holz

Due to the rapid developments in the field of artificial intelligence, masses of images, text and audio files can now be generated with just a few clicks. Professor Dr. Thorsten Holz explains the risks that are associated with this in his view: “Artificially generated content can be misused in many ways. We have important elections coming up this year, such as the elections to the EU Parliament or the presidential election in the USA. AI-generated media can be used very easily to influence political opinion. I see this as a major threat to our democracy.” Against this background, the automated recognition of AI-generated media is an important research challenge. “But this is a race against time”, CISPA-Faculty Dr. Lea Schönherr explains. “Media created with newly developed AI generation methods are becoming increasingly difficult to recognize using automatic methods. That’s why it ultimately depends on whether a human can make appropriate assessments.” This consideration was the starting point for investigating whether humans are able to identify AI-generated media at all.

Most participants classified AI-generated media as man-made

The results of their transnational cross-media study are astonishing: “We are already at the point where it is difficult, although not yet impossible, for people to tell whether something is real or AI-generated. And this applies to all types of media: text, audio, and images”, Holz says. Across all countries and media types, the majority of study participants classified AI-generated media as man-made. “We were surprised that there are very few factors that can be used to explain whether humans are better at recognizing AI-generated media or not. Even across different age groups and factors such as educational background, political attitudes or media literacy, the differences are not very significant”, Holz elaborates.

Study included socio-biographical data

Between June 2022 and September 2022, the quantitative study was conducted as an online survey in China, Germany, and the USA. Respondents were randomly assigned to one of the three media groups “text”, “image”, or “audio” and were shown 50 percent real and 50 percent

AI-generated media. In addition, socio-biographical data, knowledge of AI-generated media as well as factors such as media literacy, holistic thinking, general trust, cognitive reflection, and political orientation were collected. After data cleansing, 2,609 data sets remained (822 USA, 875 Germany, 922 China), which informed the analysis. The AI-generated audio and text files used in the study were generated by the researchers themselves, while the AI-generated images were taken from an existing study. The images they used were photorealistic portraits, the texts were news items, while the audio files were excerpts from literature.

Starting points for further research

The study results provide important takeaways for cybersecurity research: “There is a risk that AI-generated texts and audio files will be used for social engineering attacks. It is conceivable that the next generation of phishing e-mails will be personalized to me and that the text will match me perfectly”, Schönherr explains. She believes that developing defense mechanisms for precisely such attack scenarios is an important task for the future. However, further research desiderata also emerge from the study: “Firstly, we need to better understand how people can still recognize AI-generated media at all. We are planning a laboratory study where participants will have to explain to us how they recognize whether something is AI-generated or not. On the other hand, we need to consider how we can support this technically, for example through automated fact-checking processes”, Schönherr concludes.

»We are already at the point where it is difficult, although not yet impossible, for people to tell whether something is real or AI-generated. And this applies to all types of media: text, audio, and images.«

Frank, Joel; Herbert, Franziska; Jonas; Schönherr, Lea; Eisenhofer, Thorsten; Fischer, Asja; Dürmuth, Markus; Holz, Thorsten (2024): A Representative Study on Human Detection of Artificially Generated Media Across Countries. In: 45th IEEE Symposium on Security and Privacy, 20-22 May, 2024, San Francisco, CA, USA. Conference: SP IEEE Symposium on Security and Privacy

Researcher: ***Thorsten Holz***
Author: ***Felix Koltermann***

Publication date
21.05.2024

Many online services send out login notifications to inform users about unusual login activity on their accounts. Together with his colleagues from Ruhr University Bochum and Leibniz University Hannover, CISPA-Faculty Dr. Maximilian Golla has conducted a comprehensive study on this topic, examining how users react to login notifications. In May 2024, Golla and his colleagues presented their paper "Understanding Users' Interaction with Login Notifications" at the ACM Conference on Human Factors in Computing Systems.

Login notifications: An important security factor from a user's point of view

Max Golla

Due to the many online services that people use these days, users find so-called login notifications in their inboxes almost on a daily basis. "Typically, it's an email that you receive after logging in to an online service", explains CISPA-Faculty Dr. Maximilian Golla. "This email informs users that a login has just occurred. If they have indeed logged in, users can safely ignore the email. But if they are unsure if they did actually log in themselves, it is recommended that they change their password. In order to help users decide, the email also provides further information, such as where the login took place and what device was used." The widespread occurrence of login notifications in users' everyday lives inspired Golla and his colleagues to conduct a study on this topic and to find out how useful these notifications are in practice and how users react to them.

Golla and his colleagues started out with a comparative study of the login notifications from 72 different websites, including such well-known services as google.com and facebook.com, with the aim of ascertaining the specific contents of these emails. "Then we identified the most frequent and most common email components. They included information such as account name, browser, and operating system. Based on this, we created a generic login notification without any branding and used it for our study", explains Golla. To make sure that the participants would react without bias, the researchers hid their actual study behind another study. This study consisted of a test on spatial reasoning from the field of psychology, for which the participants had to register online. The participants were randomly divided into two groups and, after completing the test, they either received an email immediately with information about their actual login or after a few days reporting a fake login attempt. Subsequently, the participants, a group of 229 people from the US, were interviewed about their experiences.

Login notifications help prevent attacks

"The result of our study is that 20 percent of users from the group that was informed about a potentially dangerous login did change their password. In the group of people who received a notification after their actual login, none changed their password. And, of course, there was no need to do so. We conclude from this that people understand what login notifications are about." It is important for Golla to put the 20 percent into context: "It may not sound like much, but these emails do not replace a password. They are simply an additional security mechanism on top of everything else that we know. A strong password already fights off most attacks. In addition, there are login notifications, which help to prevent harm in 20 percent of the cases where the password fails. If you need even more protection, it is best to use two-factor authentication. Due to all these protective measures, an attack requires increasing amounts of effort." For this reason, login notifications might be a valuable asset in increasing account security.

»The question of what an ideal login notification would look like remains open for research. This would require testing different variants.«

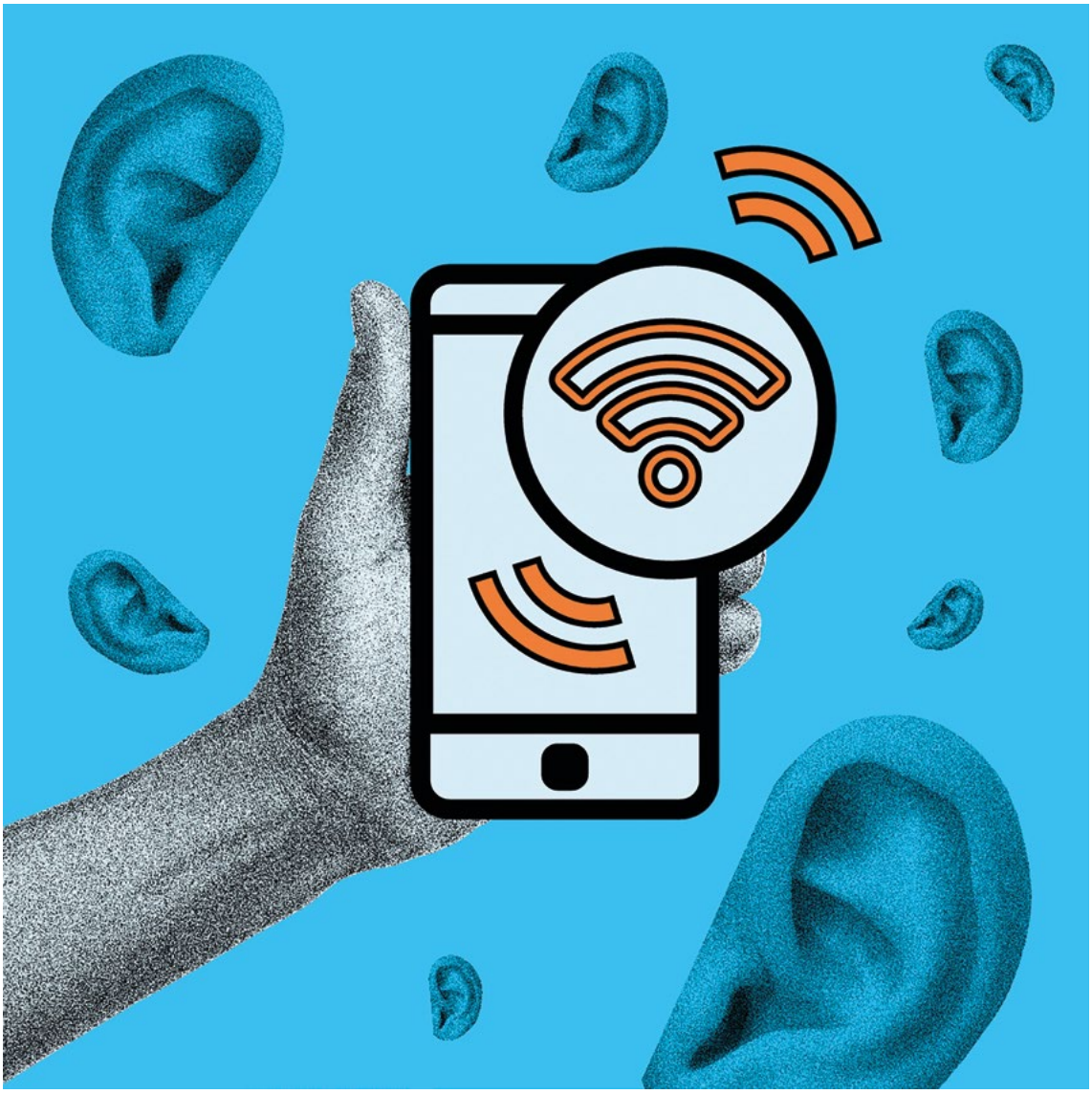
Recommendations for businesses and future research

What Golla considers to be the most important practical takeaway from the study is that users do want to receive login notifications, especially for suspicious logins, but not for every single regular login. In addition, the information in the email should be as specific as possible and already appear in the subject line. “In any case, account name, location, time, and device should be mentioned”, explains Golla. Based on this data, users can verify whether they have logged in themselves or not. “The question of what an ideal login notification would look like remains open for research”, he concludes. “This would require testing different variants. Besides, many of the analyzed login notifications have not been sufficiently tested. Especially if you live and work in the French-German border region, as we do here in Saarland, the services have problems processing and displaying location information correctly. Also, many of the tips we found in the emails, such as paying attention to HTTPS in the address bar, are questionable and outdated.” So, much remains to be done in this field of research.

Markert, Philipp; Lassak, Leona; Golla, Maximilian; Dürmuth, Markus (2024): Understanding Users’ Interaction with Login Notifications. In: CHI24, 11-16 May 2024, Honolulu, Hawaii, USA. Conference: CHI International Conference on Human Factors in Computing Systems

Researcher: ***Max Golla***
Author: ***Felix Koltermann***

Publication date
27.06.2024



© Alexandra Goweiler

CISPA researcher Adrian Dabrowski, together with colleagues from SBA Research and the University of Vienna, has discovered two major security vulnerabilities in the mobile protocol Voice over Wi-Fi (VoWi-Fi), also known as Wi-Fi calling. These vulnerabilities put the communication security of millions of mobile-phone customers worldwide at risk. Updates to fix the problems have in the meantime been implemented. A detailed description of the two security vulnerabilities can be found in "Diffie-Hellman Picture Show: Key Exchange Stories from Commercial VoWi-Fi Deployments", a research paper which will be presented at the USENIX Security Symposium 2024.

Critical security vulnerabilities in Voice over Wi-Fi revealed

Adrian Dabrowski

Modern smartphones can establish phone connections not only via mobile networks but also via Wi-Fi, thus ensuring connectivity even in places with poor mobile network quality, such as tunnels, basements, or on train journeys. So-called Wi-Fi calling, which has been around since 2016, is now offered by almost all major mobile network operators and available with all new smartphones. “The service itself is highly useful. However, in a study we conducted, we found that in some cases the connection between the smartphone and the mobile network was insecure”, explains Adrian Dabrowski.

Vulnerability on the side of mobile network providers

The vulnerability affected the services of 13 (of the 275 examined) mobile network providers based in, for instance, Austria, Slovakia, Brazil and Russia. As a result of this weakness alone, the communication security of around 140 million customers was at risk. “The fault lies with an important network component in LTE and 5G network architecture: the so-called Evolved Packet Data Gateway (ePDG)”, explains Dabrowski. The ePDG is the internet access point to the mobile network. For Wi-Fi calls, a smartphone registers with the mobile operator’s core network through a Wi-Fi connection via the internet. To ensure that this happens securely, so-called IPsec tunnels are set up between the device and the ePDG. IPsec tunnels are a type of VPN, or virtual private network, that cannot be read from the outside.

IPsec tunnels are built in several steps. Communication security is primarily guaranteed by the exchange of cryptographic keys according to the so-called Internet Key Exchange Protocol (IKE). “These are well-known methods and are usually secure. Unless you make a mistake with the keys”, explains Dabrowski. The keys have to be private, i.e. secret, and random. According to the researcher, neither of these conditions was met by the operators. To the researchers’ surprise, all 13 operators used the same global set of ten static private keys instead of random keys. “Anyone in possession of these not really private ‘private keys’ could easily eavesdrop on the communication between the smartphones and the mobile operators”, explains Gabriel Gegenhuber, security researcher at SBA Research and part of the Security and Privacy research group at the University of Vienna. “Anyone of

the affected mobile operators, the manufacturer, and possibly the security authorities of each of these countries has access to the keys." All of the affected networks were equipped with components manufactured by ZTE, a Chinese network equipment supplier.

Vulnerabilities in smartphone chips and configurations

As if that was not enough, the researchers also found that many new chips (including 5G) from the Taiwanese manufacturer MediaTek, which are used in some Android smartphones from manufacturers such as Xiaomi, Oppo, Realme and Vivo, have another vulnerability. "This chip works with the SIM card to register users in the mobile network using VoWi-Fi. We discovered that it is possible to reduce the encryption on the smartphone side to the weakest variant using targeted attacks", says Dabrowski. Their measurements and analyses of the configurations on the client and server sides of many other manufacturers, including Google, Apple, Samsung and Xiaomi, also showed that there is even more to be done in the area of mobile security. "In up to 80 percent of the cases in which we simulated a connection, we found that outdated cryptographic methods were used that no longer meet the standard", says Dabrowski.

Damage is unclear, updates have been installed

The researchers aren't able to confirm how many users worldwide were actually affected by attacks or were eavesdropped on via the vulnerability on the side of the mobile operators. However, they informed the Global System for Mobile Communications Association (GSMA) as well as the relevant providers and companies and gave them the opportunity to develop updates. These updates have now been implemented. Now that responsible disclosure is completed, the researchers will publish their work at the USENIX Security Symposium 2024, thus making their findings available to other researchers.

»We discovered that it is possible to reduce the encryption on the smartphone side to the weakest variant using targeted attacks.«

Gegenhuber, Gabriel; Holzbauer, Florian; Frenzel, Philipp; Weippl, Edgar; Dabrowski, Adrian (2024): Diffie-Hellman Picture Show: Key Exchange Stories from Commercial VoWiFi Deployments. In: 33rd USENIX Security Symposium, 14-16 Aug 2024, Philadelphia, PA, USA. Conference: USENIX Security Symposium

Researcher: ***Adrian Dabrowski***
Author: ***Annabelle Theobald***

Publication date
30.07.2024

A new vulnerability named GhostWrite fully compromises the integrity of the high-end RISC-V CPU XuanTie C910 manufactured by T-Head. GhostWrite not only grants attackers full read-and-write access to physical memory on the C910. It entirely bypasses virtual memory and caches and is invisible in performance counters. GhostWrite also concerns cloud services that rely on C910-based machines and can only be mitigated by disabling the vector extension. Two further architectural CPU vulnerabilities have been found, one affecting the T-Head XuanTie C906 and one affecting the C908. In August 2024, CISPA researcher Fabian Thomas is presenting the three vulnerabilities in a talk entitled "Arbitrary Data Manipulation and Leakage with CPU Zero-Day Bugs on RISC-V" at the Black Hat USA conference in Las Vegas.

GhostWrite vulnerability breaks integrity of RISC-V CPU ‘XuanTie C910’

Fabian Thomas

Using a new CPU fuzzing method for RISC-V implementations, CISPA researcher Fabian Thomas from the research group of Dr. Michael Schwarz has discovered three architectural vulnerabilities affecting the T-Head CPUs XuanTie C906, C908 and C910. GhostWrite, the most impactful of these three vulnerabilities, concerns the XuanTie C910. Not only can it create direct access to the DRAM, allowing unprivileged users to modify data directly in the physical memory. It can also interact with the hard drive and peripheral devices such as network cards and graphic cards. Thomas has further detected two “halt-and-catch-fire” CPU vulnerabilities, one concerning the XuanTie C906 and one concerning the XuanTie C908, which can be exploited for unprivileged denial-of-service attacks.

RISC-V: Young, open, flexible and potentially problematic

The starting point for Thomas and Schwarz’s discovery was the rise of RISC-V CPUs. RISC-V is a relatively young, open standard instruction set architecture (ISA) that has allowed new CPU manufacturers to emerge. In general terms, an ISA determines how software interacts with the CPU, specifying the instructions to which the CPU may respond. “Being very flexible, RISC-V enables manufacturers to implement their own customized ISA extensions. Problematically, there is no central registry for these custom extensions, so that different CPUs might use the same encoding for different instructions”, Thomas explains. “As a result, software developed to suit one manufacturer’s RISC-V CPU might elicit different behavior when used on another RISC-V CPU. This variance in CPU behaviors can prove problematic.” To date, RISC-V CPUs have found application in a small number of hardware cores that are used, for example, in laptops, smartphones, and servers. Currently available are five consumer-grade RISC-V CPUs.

Enter RISCVuzz: A differential fuzzing framework for RISC-V CPUs

Thomas and Schwarz hypothesized that the heterogeneity of RISC-V CPUs and their custom extensions might be used to detect architectural vulnerabilities across RISC-V implementations. To this end, they developed a differential CPU fuzzing method named RISCVuzz and ran it against all five consumer-grade RISC-V CPUs. Schwarz explains the logic underpinning their fuzzing approach: “Basically, we assumed that if we feed all our CPUs the same supported instruction, their responses should be the same, too. Every time a CPU came up with a response that deviated from the others CPUs’, we examined it more closely for vulnerabilities. In other words, if four out of five hotel safes remain locked when you enter ‘0000’ but the fifth one springs open, you have reason to assume that something is awry with that one.”

»Being very flexible, RISC-V enables manufacturers to implement their own customized ISA extensions. Problematically, there is no central registry for these custom extensions.«

Disclosure and mitigation

In February 2024, Thomas and Schwarz disclosed their findings to T-Head, an Alibaba subsidiary, and in April 2024 to Scaleway, a cloud service provider that had just begun using the C910 CPU in the cloud. To date, there are no updates to mitigate either of the three architectural vulnerabilities. GhostWrite as well as the vulnerability affecting the C908 can be mitigated by disabling the vector extension, which also renders core functionalities of the CPUs unusable. No viable mitigation has been identified for the vulnerability affecting the C906. “CPUs are written in code. It is important that we disclose the vulnerabilities we find to prevent these bugs from proliferating in other CPU developments”, Schwarz says.

Thomas, Fabian; Hetterich, Lorenz; Zhang, Ruiyi; Weber, Daniel; Gerlach, Lukas; Schwarz, Michael (2024): Arbitrary Data Manipulation and Leakage with CPU Zero-Day Bugs on RISC-V. In: Black Hat USA 2024, 3-8 Aug 2024, Las Vegas, NV, USA. Conference: Black Hat

© Chiara Schwarz

A common practice among software developers is to use so-called code snippets from the platform Stack Overflow. A study by CISPA researcher Alfusainey Jallow now reveals that this can lead to security risks in the long run. These risks are partly due to the fact that security-relevant updates to the code snippets often fail to make their way into the software where the snippets have been used. Jallow published the results of his study in a paper called "Measuring the Effects of Stack Overflow Code Snippet Evolution on Open-Source Software Security" at the IEEE Symposium on Security and Privacy 2024 (SP).

Outdated code snippets on Stack Overflow jeopardize software security

Alfusainey Jallow

In their everyday programming work, software developers frequently encounter problems for which they need a quick solution. “Earlier studies have shown that the most prominent information source developers consult is not textbooks but Stack Overflow”, explains CISPA researcher Alfusainey Jallow. As part of the Stack Exchange Network, Stack Overflow is a popular online platform for programmers and developers who are looking for answers to various programming issues and problems. “The popularity of Stack Overflow is due to the fact that it offers functional code snippets. A code snippet is a chunk of code, written in a particular programming language, that solves a specific problem. You can usually use it directly in your own project with little to no changes”, Jallow continues.

Search for outdated code snippets in GitHub projects

Research has already shown that there are security-critical variants of code snippets on Stack Overflow. Whether the code copied from Stack Overflow is secure can be checked, for instance, using browser plugins. It is also known that the code snippets are not static but are constantly being developed. “However, what had not yet been investigated is the question of whether developers who copy code snippets from Stack Overflow into their software also update them when changes are made to the snippets on Stack Overflow”, Jallow says. To find out about that, Jallow and his colleagues examined open software projects on GitHub, which is a popular platform. “GitHub is used to host code and to collaborate with others on specific software projects”, Jallow explains. He developed a multi-step procedure to detect outdated versions of code snippets in GitHub projects and to check whether or not security-relevant updates had been performed on these code snippets.

Missing updates to code snippets lead to vulnerabilities

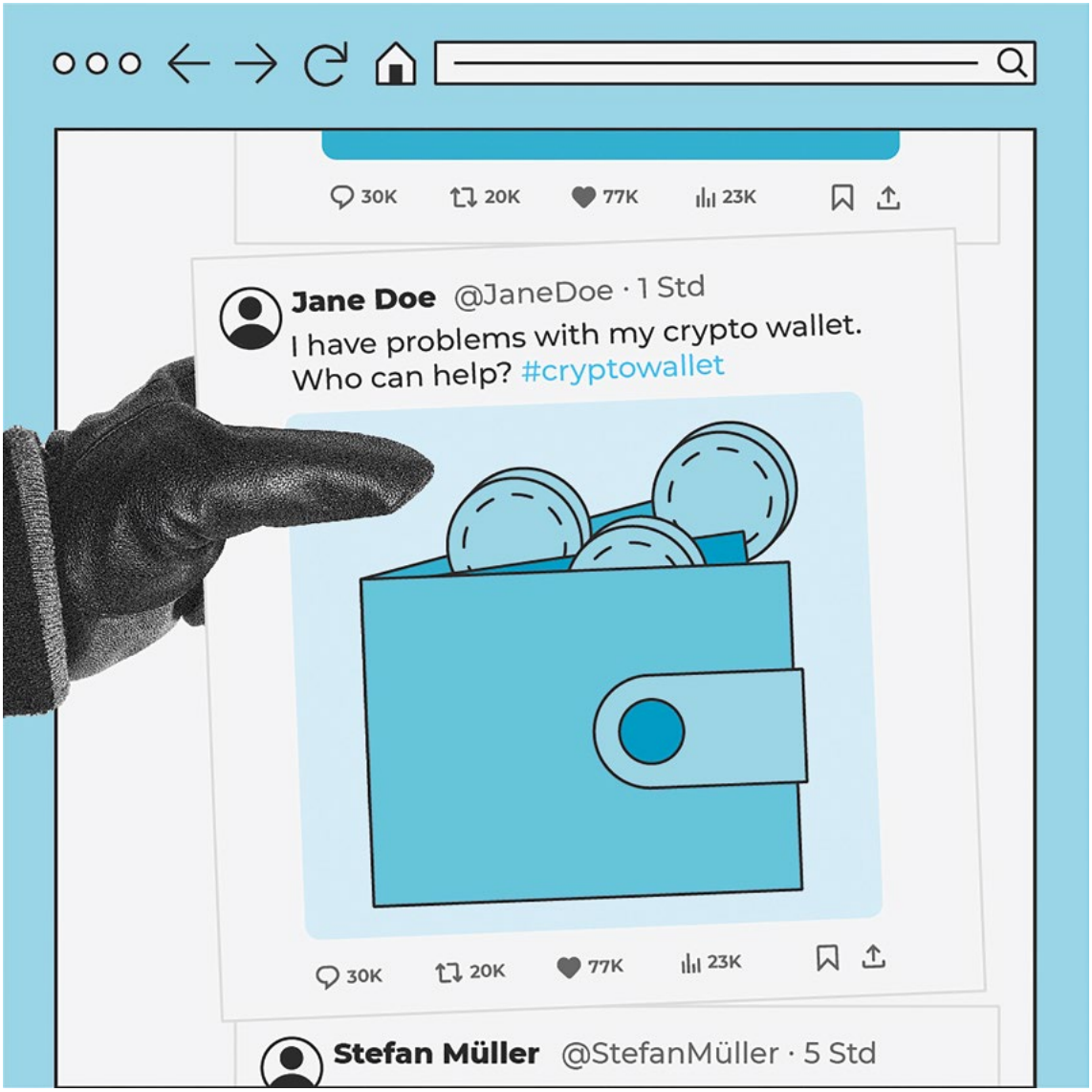
In their investigation of nearly 11,500 Github projects, Jallow and his colleagues found that every second reused code snippet was outdated, regardless of the programming language used. They found no evidence that GitHub developers had implemented updates to Stack Overflow code snippets into their projects. According to Jallow, the dangers associated with these findings lie in the almost unlimited distribution circles of software. “If you copy a code snippet from Stack Overflow that can violate users’ privacy, and they install the app on their phone, it will have a lot of social implications. If privacy is violated by a code snippet from Stack Overflow, it’s a really big problem”, he is convinced. Jallow and his colleagues conclude from their findings that “developers do not check the snippets copied from Stack Overflow for any updates, or are not aware that the code they reuse is being discussed and updated or fixed on Stack Overflow.”

Missing tool is a mission for the future

For developers, Jallow currently has one main piece of advice: “Be careful when using code snippets from Stack Overflow. And when you use them, find a way to remember them.” Since there is no automated tool available yet, developers have to regularly check themselves whether updates to the code snippets they use are available on Stack Overflow. This is what drives Jallow, as he explains in the interview: “In order to close this gap, I want to develop a tool. If it is not going to happen in the course of my PhD thesis, then at a later point in my career. CISPA has this amazing ecosystem that transfers research results to industry, and promotes spin-offs and startups. It’s a great opportunity that CISPA offers, and I would like to take advantage of it.”

»Be careful when using code snippets from Stack Overflow. And when you use them, find a way to remember them.«

Jallow, Alfusainey; Schilling, Michael; Backes, Michael; Bugiel, Sven (2024): Measuring the Effects of Stack Overflow Code Snippet Evolution on Open-Source Software Security. In: 45th IEEE Symposium on Security and Privacy, 20-22 May, 2024, San Francisco, CA, USA. Conference: SP IEEE Symposium on Security and Privacy



The increasing popularity of cryptocurrencies has turned social media into a central place for users to seek help with their crypto wallet or private key. Scammers can take advantage of this situation and make money with fake support offerings or gain access to wallets or keys. CISPA researcher Dr. Bhupendra Acharya has presented the first large-scale study on how these scams work and provided an end-to-end analysis of the scam operations in X (formerly known as Twitter). He presented his findings at the IEEE Symposium on Security and Privacy (S&P) 2024.

Seeking help for crypto wallet problems on social media can attract scammers

Bhupendra Acharya

Cryptocurrencies such as Bitcoin or Ethereum are gaining popularity because of their decentralized nature and the anonymity they grant their users. In order to manage and sell cryptocurrencies, users need so-called crypto wallets, which basically are digital wallets for cryptocurrencies. The best-known wallets are Metamask, Coinbase and Trust. Secret keys are essential and secure access to these wallets. And anyone with access to the secret keys can manage and access the wallets. In the event of secret key loss, the crypto wallets remain inaccessible.

"As cryptocurrencies have become more popular, we noticed that people have also been talking about them on social media. This includes technical support issues such as lack of wallet access, loss of private key phrases, etc., which attracts fraudsters. They fake technical support, effectively impersonating official support", explains CISPA researcher Bhupendra Acharya. Many people prefer to seek help in a chat group or via a tweet instead of directly contacting the official crypto wallet support channels. "In our study, we uncovered how scammers exploit users on social media to either gain access to crypto wallets or simply ask for payment in return for a technical support they are faking", says Acharya.

Tracking down scammers with HoneyTweet

In order to investigate how support scam on social media actually works, Acharya developed a tool called HoneyTweet. "HoneyTweet automatically sends out unique tweets with keywords for technical support requests to bait scammers", Acharya explains. "Scammers offering fake support are contacted via a semi-automated tool to detect the scamming payment methods or their modus operandi", he continues. The scammers come up with various fake offers such as the software tool "Zeus", which they claim will retrieve wallet access, and ask for money as part of the support. During the conversations, users were often directed to external communication channels to avoid scam detection on the original platform. With the help of HoneyTweet, Acharya and his colleagues baited more than 9,000 scammers within three months and traced them on six social media platforms including

PayPal and cryptocurrency addresses, which were used as scamming payment methods.

The key results of the study

In their study, Acharya and his colleagues were able to show that crypto wallet support scams are a widespread phenomenon on social media platforms like X. “We found that social media still has some work to do to stop these scams”, Acharya says. “And we also discovered that scammers often use multiple social media platforms for their scam attempts. Beyond X, the scammers ask to be contacted via direct messages on Instagram, Facebook, Telegram, WhatsApp and others.” Basically, the scammers work in chain operations that link multiple social media platforms together. During the scam process, the scammers first try to build trust. Later, they perform social engineering tricks, initiating direct message communication where the actual scams take place. Upon direct messaging, the potential victim is asked to either release their private key or pay for the “fake” support via the scammer’s provided payment method. By collaborating with PayPal and sharing the detected scam accounts with the payment service provider, the researchers were able to further validate the scams’ financial impact.

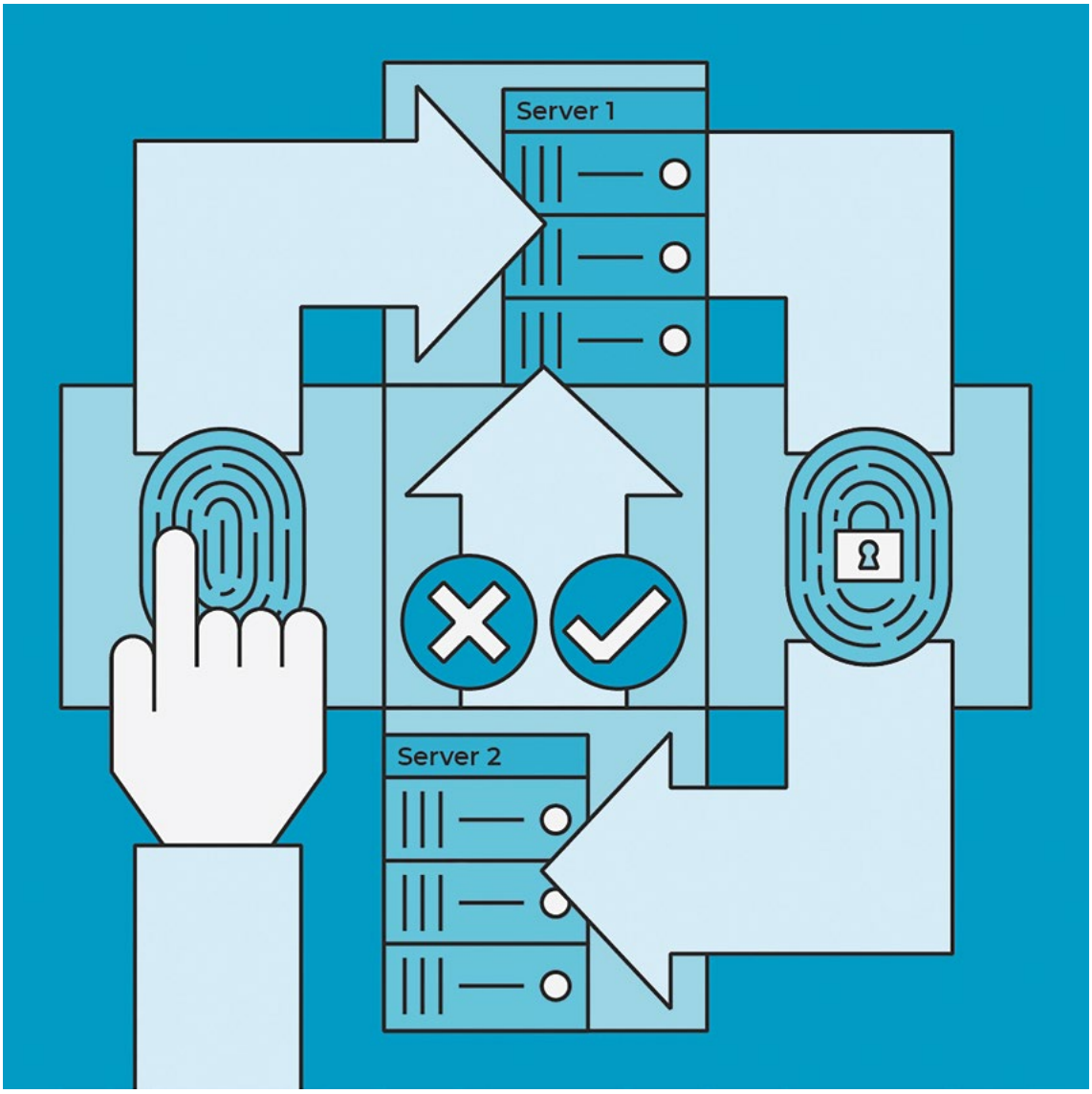
Takeaways for businesses and users

“There are two groups that could adopt our recommendations”, Acharya explains. “The first one consists of the involved services, like the crypto wallet providers. They should monitor all activity directly associated with their brand name and take action if scammers attempt to impersonate their brand. The second group consists of social media platforms like X, Instagram, Facebook, Telegram and others. It is important to jointly monitor scam chains because the scam does not necessarily occur on the platform where the chat started. The final scam might take place at the end of the chain, i.e. on another platform. In order to break those chains, cooperation between the social media services is crucial.” Users of crypto wallets can also take action. Acharya recommends making sure to engage only with official cryptocurrency wallet providers and being cautious with all unofficial channels. Never should the information be shared via Google Forms or similar platforms. “Crypto wallets or social media accounts affiliated with official crypto wallets will never ask their users for their secret keys”, the CISPA researcher concludes.

The future belongs to (secure) digital currencies

Acharya, who during the conversation revealed himself as a big fan of digital currencies and a cryptocurrency user, sees a lot of potential in cryptocurrencies. “I believe that digital currencies like cryptocurrencies are the next generation of currencies and that they will replace existing currencies in the future”, he is convinced. “However, what we need is a system that is secure enough to create and operate a digital currency.” As a researcher, he wants to continue contributing to this goal. “One project is using ChatGPT to chat with the scammers based on HoneyTweet”, he explains. “In this context, we also focus on different categories of fraud, such as alleged account recovery. In another follow-up study, we will use a deepfake-based method to chat and communicate with the scammers via Zoom video and phone to identify further types of fraud mechanisms.” It will be exciting to see what fraud mechanisms in the area of cryptocurrencies Acharya and his colleagues will uncover.

Acharya, Bhupendra; Saad, Muhammad; Cinà, Antonio Emanuele; Schönherr, Lea; Nguyen, Hoang Dai; Oest, Adam; Vadrevu, Phani; Holz, Thorsten (2024): Conning the Crypto Conman: End-to-End Analysis of Cryptocurrency-based Technical Support Scams. In: 45th IEEE Symposium on Security and Privacy, May 20-22, 2024, San Francisco, CA, USA. Conference: SP IEEE Symposium on Security and Privacy



Millions of people around the world rely on humanitarian aid. One of the challenges when it comes to distributing aid is that resources are almost always scarce. Therefore, humanitarian organizations want to ensure that people can only register once. CISPA-Faculty Dr. Wouter Lueks and his colleagues at EPFL in Lausanne recently developed a tool in cooperation with the International Committee of the Red Cross (ICRC) that enables organizations to overcome this challenge by using biometric data safely. The paper "Janus: Safe Biometric Deduplication for Humanitarian Aid Distribution" was presented at the IEEE Symposium on Security and Privacy 2024 (S&P).

JANUS: Using biometrics to avoid multiple registrations in humanitarian aid

Wouter Lueks

The possibility of people registering multiple times for humanitarian aid hangs over these programs like the Sword of Damocles. “Humanitarian organizations try to help as many people as possible”, explains CISPA-Faculty Dr. Wouter Lueks. “In achieving that goal, they want to make sure that they do not give aid to the same recipient twice because in that case someone else cannot receive aid.” Lueks was looking for an approach to prevent the duplication of humanitarian aid distribution. Since the use of ID documents is often impossible or risky in regions with humanitarian crises, using biometric data was the method of choice. “The core of what we design is to say we want to use biometric data for one purpose only: We want to be able to determine whether the biometric data of the person in front of us was already registered”, explains Lueks.

But how does the method actually work in practice? “When a person comes to a registration station and asks for registration, biometric data, such as a fingerprint, is taken from this person”, explains Lueks. This requires a reader that is connected to a computer as well as an internet connection. “Then, a so-called cryptographic protocol is run between the computer at the registration station and a second computer at another location, in our case at the ICRC headquarters in Geneva”, Lueks continues. “The result of this protocol is a yes-or-no decision. Yes, I found the biometric data in the database or no, I didn’t find it. In the latter case, the recipient’s data can be added.” On the local computer, the data is only saved for the moment of data recording and then deleted again.

Ensuring security

According to Lueks, “the fact that biometric data cannot be changed makes storing it in databases very risky. They leave traces of information about the fact that certain people have been here, that they have registered and so on. In the past, for example after the US withdrawal from Afghanistan, we have seen that the simple fact that people registered for a certain program can have very far-reaching consequences for their future life and might threaten their security.” This is why Lueks and his

colleagues have implemented various security mechanisms into their system. “The decisive factor is that the two computers have to work together to make this yes-or-no decision”, explains Lueks. “If one of the two computers refuses to cooperate, or more specifically, if someone in Geneva decides to shut down the system, no further information is made available from the system.” Not even physical access to one of the two computers will reveal biometric data of recipients: the system is designed to prevent data access.

»The fact that biometric data cannot be changed makes storing it in databases very risky. They leave traces of information about the fact that certain people have been here, that they have registered and so on.«

Embedding the registration process in the distribution of humanitarian aid

The method that Lueks and his colleagues present in their recent paper focuses on the registration process. This, however, is only one part of the complex process of distributing humanitarian aid. Another critical part is the actual distribution of goods. Here, too, it is essential to prevent individuals from receiving aid more than once. To this end, Lueks and his colleagues developed a token-based system for distributing humanitarian aid last year. Specifically, this means that aid recipients, after successful registration, would receive a token, such as a smart card, allowing them to collect the goods they are entitled to. The design of the token ensures that no individual can receive more than one allocation per distribution round. Although the previous solution focused on households rather than individuals, the approach could easily be combined with the newly developed method. Looking to the future, Lueks can imagine developing a prototype for the application of both methods. His cooperation partners at the ICRC would certainly be interested in this.

EdalatNejad, Kasra; Lueks, Wouter; Justinas, Sukaitis; Graf Narbel, Vincent; Massimo, Marelli; Carmela, Troncoso (2024): Janus: Safe Biometric Deduplication for Humanitarian Aid Distribution. In: 45th IEEE Symposium on Security and Privacy, May 20-22, 2024, San Francisco, CA, USA. Conference: SP IEEE Symposium on Security and Privacy

© Chiara Schwarz

In a study entitled "Prompt Stealing Attacks Against Text-to-Image Generation Models", which was presented at the USENIX Security Symposium 2024, CISPA researcher Xinyue Shen demonstrates that reverse engineering can be used with AI-generated images. Developing a tool called PromptStealer, Shen and her colleagues were able to extract the original prompt from AI-generated images. In doing so, she uncovered a new attack scenario for text-to-image generation models, while also providing a protection mechanism called PromptShield.

Prompt stealing: CISPA researcher discovers new attack scenario for text-to-image generation models

Xinyue Shen

Recently, AI image generators have become very popular, not least because the results they achieve have made huge quality leaps. Most image generators, such as Stable Diffusion or DALL-E, are text-to-image generators. To generate the perfect image, it is crucial for the text input, the so-called prompts, to be precise. As this requires highly specialized knowledge, prompt engineers have emerged as a new profession. There is another peculiarity with AI images, however, as CISPA researcher Xinyue Shen explains: “To get an image in a certain style, you need a precise description as well as a so-called modifier, which describes the style of the image. Without this, the results tend to be arbitrary.”

The term “unsafe images”

And there was more that caught Shen’s attention: “I realized that as a result of the importance of prompts, a new market has emerged”, says Shen. “Prompt engineers sell their text input for generating AI images on platforms like Promptbase.” With just a few clicks and some euros, anyone interested can purchase a prompt for a specific image and save themselves the time-consuming trial-and-error process. However, digital marketplaces often bring new attack scenarios with them. “We wanted to find out if there was a way to obtain the prompts without paying for them”, explains Shen. “We called this scenario prompt stealing.” According to Shen and her colleagues, this means that the prompt is extracted from an AI-generated image without the consent of the prompt engineer, depriving platforms such as Promptbase of their commercial basis.

A new tool named PromptStealer

Initial attempts to generate the prompt using a text decoder did not bring the desired results, so Shen decided to develop her own tool. Importantly, she found that both the image description as well as a specific modifier are crucial for a precise prompt. “We named the new method PromptStealer”, Shen says. “As both the subject

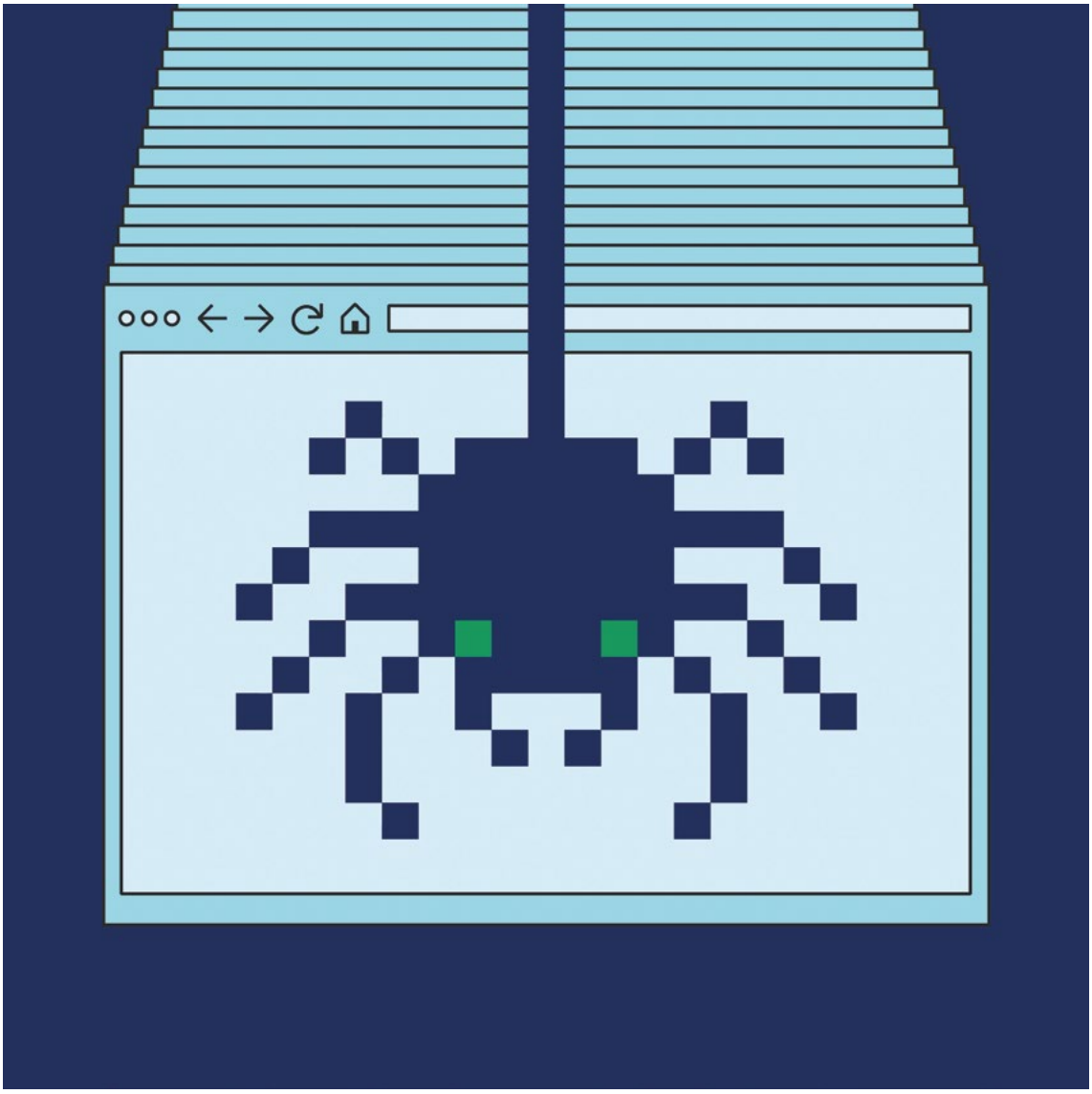
»To get an image in a certain style, you need a precise description as well as a so-called modifier, which describes the style of the image. Without this, the results tend to be arbitrary.«

and the modifiers are important, we solve the issue step by step in our tool. First, we use a subject generator in order to obtain the subject depicted in the picture. Then we use a detector for the modifiers to predict them precisely, too." Shen conducted both a quantitative and a qualitative analysis to prove that PromptStealer provides better results than other methods such as Image Captioning or CLIP Interrogator. The AI images generated using the prompts of PromptStealer were the ones that came closest to the original image.

PromptShield against attacks

Being cybersecurity researchers, Shen and her colleagues have already been thinking about how to prevent prompt stealing attacks. "An obvious idea was to consider ways to reduce the performance of machine learning models", she explains. "Our aim was to prevent models such as PromptStealer from recognizing the modifier used. That's because recognizing the exact modifier is crucial for a precise prompt." She successfully prevented this by adding perturbations to the AI-generated image. The relevance of the attack scenario that Shen discovered is illustrated by the fact that Microsoft has already added it to the Vulnerability Severity Classification for AI Systems. Shen has made the data from her study freely available on the Internet. It includes a curated dataset with 61,467 AI-generated images from the Lexica platform, as well as the code for PromptStealer.

Shen; Xinyue; Qu ,Yiting; Backes, Michael; Zhang, Yang (2024): Prompt Stealing Attacks Against Text-to-Image Generation Models. In: 33rd USENIX Security Symposium, 14-16 Aug 2024, Philadelphia, PA, USA. Conference: USENIX Security Symposium



© Chiara Schwarz

A study by CISPA researcher Aleksei Stafeev is the first to systematize the knowledge about tools for the automated analysis of websites, so-called web crawlers, in the field of web security measurement. Stafeev examined hundreds of papers published at the most important international conferences over the last 12 years. The results show that many papers describe the crawlers inadequately and that randomized algorithms perform best when it comes to navigating crawlers on websites. Stafeev published the complete results in a paper called "SoK: State of the Krawlers - Evaluating the Effectiveness of Crawling Algorithms for Web Security Measurements", which he presented at the USENIX Security Symposium in August 2024. The paper was written as part of the TESTABLE project coordinated by CISPA-Faculty Dr. Giancarlo Pellegrino.

Study of web crawlers reveals shortcomings

Aleksei Stafeev

Studies measuring web security, for example in relation to the implementation of data protection measures or website security, are very popular in the field of cybersecurity research. Crawlers are the tool of choice for conducting such studies. “Crawlers aim to automate data collection on a website”, explains CISPA researcher Aleksei Stafeev. They are based on an algorithm that determines how the crawler automatically scans a website, visits different pages and collects data from them. “But web crawling is not as simple as it sounds”, Stafeev continues. "In theory, these tools simply visit websites. But in reality, the internet is very complex: There are a lot of different buttons on every website and each of them may or may not lead to a different page. You have an exponential growth of different pages and you have to figure out which ones you actually need to visit to get the data relevant to your research question.” Despite the great importance of web crawlers, their performance has so far only been studied to a very limited extent. Stafeev’s study is now closing this research gap.

Stafeev took a two-step approach. “First, we conducted an overview of the current work on web measurements that use crawlers”, he explains. This yielded a data corpus of 407 papers published between 2010 and 2022. “We tried to extract information about which crawlers are used and how to get a general picture of what is used in web measurements”, Stafeev says. Second, Stafeev examined papers from the last three years that propose new crawlers. “We evaluated the crawlers in terms of what data they collect for the purpose of web security measurement”, Stafeev continues. To examine the crawlers in terms of code coverage, source coverage and JavaScript collection, Stafeev developed an experimental setup called Arachnarium.

Insufficient descriptions and the randomization paradox

One of the key findings of the first part of the study was that most papers offered inadequate descriptions of web crawlers. “It was really difficult to extract and understand the information about what technology they use to crawl and what techniques they use. And there were usually not enough details about the code and algorithms used. Often it was just ‘we use crawling’ and that was it. One of the key learnings was that we can do better as a community by providing more information about the crawlers we use and how they are configured”, Stafeev summarizes. This is particularly important in order to be able to

guarantee the reproducibility of studies, which is a key criterion for scientific quality.

The second part of the study produced another astonishing result. “According to our data, web crawlers that use randomized algorithms seem to perform best”, he explains. “This is actually quite surprising, as it means that no matter what navigation strategies we’ve developed, we still haven’t found a better solution than just clicking on things at random.” Stafeev tested crawlers using three different metrics. He found that there was no single winner among the crawlers across all three metrics. “So we can’t give a one-size-fits-all recommendation that says: ‘Everyone should use this crawler’”, the he continues. It therefore depends critically on the context and specific objective as to which crawler is suitable.

Takeaways and further handling of the research data

Stafeev created a huge data set to be able to conduct the study. “We believe that we can learn a lot more from it”, he says. “And it would be really nice if others could gain more insights from the data we have collected.” For this reason, Stafeev has made the complete data set freely accessible online. In future, he wants to devote himself to his real passion again: developing new crawlers. Initially, Stafeev had not planned on carrying out such a large study. He only wanted to improve his own crawler and look at how others had dealt with the problem. “Systematizing knowledge, which this study is based on, is quite an undertaking”, he says. “But I learned a lot from this project about how to carry out such experiments and work with such large data sets. I will capitalize on this knowledge in my future work”, he concludes.

»But web crawling is not as simple as it sounds. In theory, these tools simply visit websites. But in reality, the internet is very complex: There are a lot of different buttons on every website and each of them may or may not lead to a different page.«

Stafeev, Aleksei; Pellegrino, Giancarlo (2024): SoK: State of the Krawlers - Evaluating the Effectiveness of Crawling Algorithms for Web Security Measurements. In: 33rd USENIX Security Symposium, 14-16 Aug 2024, Philadelphia, PA, USA. Conference: USENIX Security Symposium

© Chiara Schwarz

Accessing virtual worlds from a home computer via a web browser while interacting securely and privately with others: This is the promise of metaverse platforms. CISPA researcher Andrea Mengascini put this promise to the test and discovered significant risks in terms of inadequate privacy protection and the threat of cyberattacks. He presented his study "The Big Brother's New Playground. Unmasking the Illusion of Privacy in Web Metaverses from a Malicious User's Perspective" at the renowned Conference on Computer and Communications Security (CCS) in fall 2024.

Study reveals vulnerability of metaverse platforms to cyber attacks

Andrea Mengascini

"I've always been interested in virtual reality and online games", CISPA researcher Andrea Mengascini tell us. When he and his research group leader, CISPA-Faculty Dr. Giancarlo Pellegrino, started investigating the security of VR headsets, they discovered something interesting: "We realized that it was the same technology used in online games that is also used in metaverses", says Mengascini. He defines a metaverse as a "virtual social space in which people can interact according to rules that in some way mirror the rules of the physical world." While the security of online games has been researched and protective mechanisms implemented, this remained an unresolved issue for metaverse platforms. This is what caught Mengascini's interest.

"Accessing a metaverse has become much easier in recent years", explains Mengascini. "Today, all you need is a normal web browser to enter these rooms. Thanks to the WebXR API interface, it is also possible to use a VR headset." In the metaverse, people find a kind of digital copy of the real world: There are rooms for private meetings, large or small public events, fun and entertainment. "These platforms run as web-based clients and use JavaScript to manage complex 3D environments, the avatars of users and real-time interactions. All of this is not only crucial for the smooth operation of the metaverse, but also plays a major role in its security", Mengascini says. His goal was to find out if there are any security gaps when accessing the metaverse via web browsers.

Research questions and method

In his study, Mengascini posed three specific questions: 1. Which entities, such as users and objects, exist in metaverses and which attributes, such as position, appearance, etc., are assigned to them? 2. Where exactly are these elements stored in the memory, and what access can attackers gain to this memory? 3. How can the memory be exploited for attacks? Via a Google search, Mengascini first identified 27 metaverse platforms that use the WebXR API interface. In a next step, he examined three of them in more detail, as they performed best in terms of popularity, user activity, internet traffic and coverage of

real events. Mengascini's method was to create so-called memory snapshots, which recorded the objects stored in the memory at a given point in time. The snapshots were taken before and after executing a specific action, such as moving an avatar from A to B. Afterwards, an algorithm was used to check if any changes had occurred and if this information could be read from the web browser's memory.

Memories are very easy to access

"The most important finding is that these platforms lack the most basic security mechanisms", Mengascini explains. "The main issue is that the browsers' memories are too easy to access." Even a non-expert could access both the source code and the actual objects in the memory with a little practice. "We also found that these platforms have messed up common good coding practices in web application development", he continues. "The developers of these platforms have missed the fact that due to a combination of unverified client-side information and excessive disclosure of information to the client, attacks are possible."

To illustrate the implications of this, Mengascini gives an example: "Let's assume there is a CISPA metaverse featuring an exact replica of our building. This would mean that every user's computer would receive all the information about what is currently happening at CISPA: Who is talking to whom in which room, where individual people are physically located and how they are moving, including the exact positions of the walls. Based on this, my computer calculates the virtual environment and ensures, for example, that I cannot listen to conversations in the Director's office because of a wall. However, the browser receives information about what is being said in the room. And that is bad. Even if you are not able to listen in with a normal client, this information can be extracted quite easily by attackers. Therefore, it is important to not overshare information."

Potential attack scenarios

According to Mengascini, this security gap gives rise to a number of possible attack scenarios. The key finding is that attackers can control their victims' avatar and camera positions and appearances, as well as their own, independently of each other. For example, attackers can move their camera independently from their avatar. "This allows attackers to position themselves undetected in the room and to listen in", Mengascini continues. Another possibility is that attackers can secretly access another user's camera content. "It is like attackers putting on the user's VR glasses without them realizing it", he says. To prevent this, as much information as possible would have to be kept on the server, which would, however, require more computing power. Exactly this is, according to

Mengascini, one of the reasons why the metaverse platforms rely so heavily on web browsers.

New research questions as takeaway

As is common practice in cybersecurity research, the three platforms that Mengascini had examined were informed of the security gaps and given time to fix them. None of the three platforms has done this yet, which is why their names remain anonymized in the published paper. “From a researcher’s perspective, I am obviously concerned that the platforms don’t want to focus on security or don’t have the manpower to do so”, says Mengascini. “But at the same time, I think that we as researchers now have an open research question. Maybe it’s time for us to propose security mechanisms to prevent attacks or at least make it harder to carry them out." Already, he has ideas about the protection mechanisms that could be implemented. In particular, he plans to use the knowledge gained from the development of online games and transfer it to the metaverse. However, Mengascini is aware that many approaches come with disadvantages and require extensive testing. A challenge that he wants to tackle in the near future.

Mengascini, Andrea; Aurelio, Ryan; Pellegrino, Giancarlo (2024): The Big Brother’s New Playground: Unmasking the Illusion of Privacy in Web Metaverses from a Malicious User’s Perspective. In: CCS 2024, 14-18 Oct 2022, Salt Lake City, USA. Conference: CCS ACM Conference on Computer and Communications Security

ABOUT CISPA

The CISPA Helmholtz Center for Information Security is a national Big Science institution within the Helmholtz Association of German Research Centers. CISPA researchers explore all aspects of information security. They conduct cutting-edge foundational research as well as application-oriented research, addressing the most pressing challenges in cybersecurity, artifical intelligence and privacy. Research results achieved at CISPA find their way into industrial applications and products that are available worldwide. CISPA thus contributes to German as well as European competitiveness.

CISPA offers a world-class research environment as well as extensive resources to a large number of researchers. It strongly supports the undergraduate and graduate education of cybersecurity students and seeks to become an elite training ground for the next generation of cybersecurity experts and leading scientists in this field. CISPA is located in Saarbrücken and St. Ingbert. The center's proximity to France and Luxembourg puts it in an ideal position for cross-border cooperation with other research institutions.

Our research currently focuses on the following six research areas:

Algorithmic Foundations and Cryptography

Trustworthy Information Processing

Reliable Security Guarantees

Threat Detection and Defenses

Secure Connected and Mobile Systems

Empirical and Behavioral Security

IMPRINT

CISPA – Helmholtz Center for Information Security gGmbH
Stuhlsatzenhaus 5
66123 Saarbrücken, Germany

Publisher

Sebastian Klöckner

Editor-in-Chief

Tobias Ebelshäuser,
Sandra Engel,
Felix Koltermann,
Eva Michely,
Annabelle Theobald

Editors

Alexandra Goweiler,
Lea Mosbach,
Chiara Schwarz,
Janine Wichmann-Paulus

Illustration

Alexandra Goweiler,
Chiara Schwarz

Design

Tobias Ebelshäuser

Photography

Januar 2025

Information as of

T: +49 681 87083 2867
M: pr@cispa.de
W: https://cispa.de/en

Contact Corporate Communications

CISPA
HELMHOLTZ CENTER FOR INFORMATION SECURITY