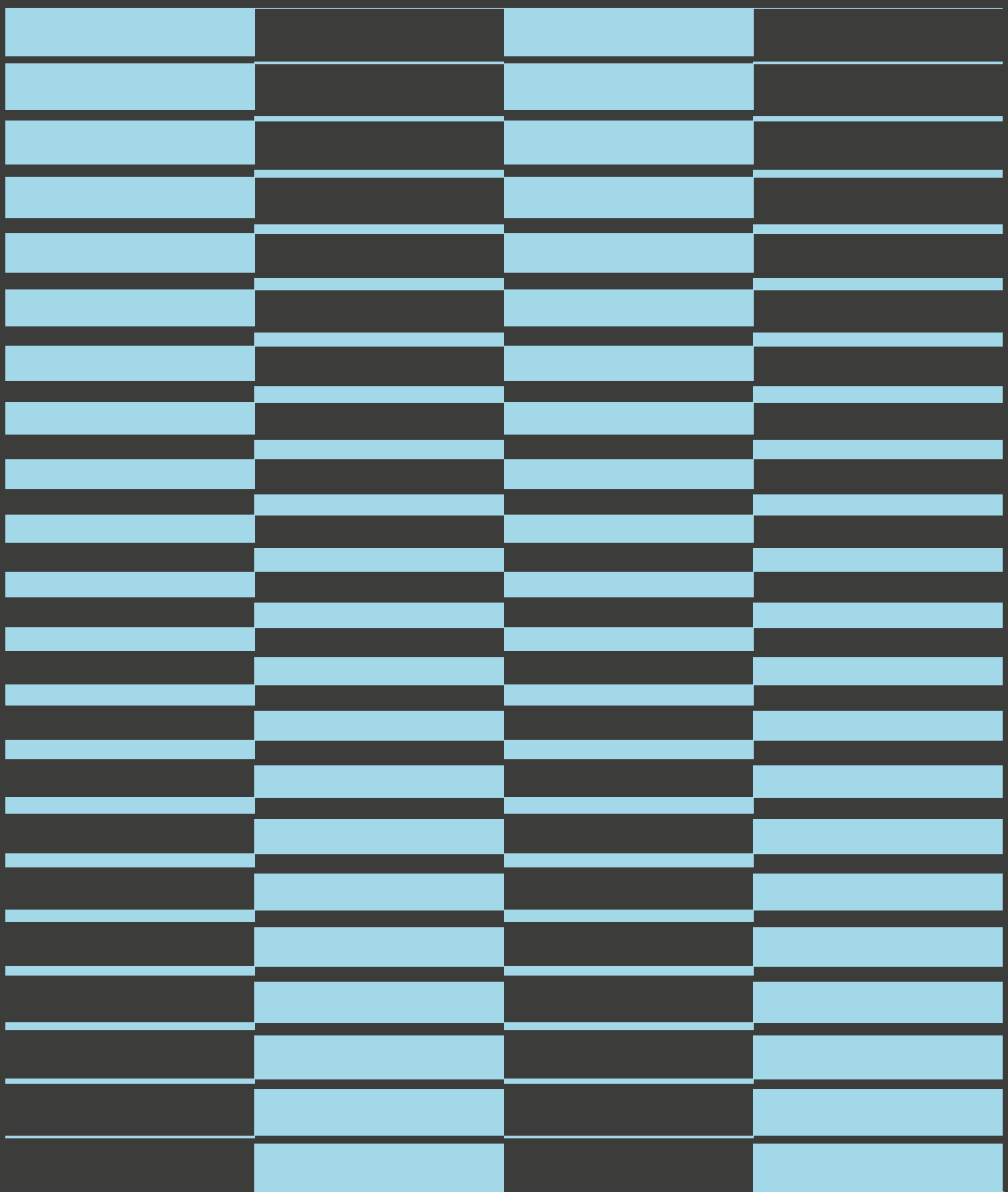
CISPA DISPLAY

DE

EDITION 2025



VORWORT

Forschung lebt von Neugier, kritischem Denken und dem Streben nach Erkenntnis. Doch um sie uns wirklich nutzbar zu machen, brauchen wir den Brückenschlag zwischen Forschung und Gesellschaft. In unserer Zeit, in der Informationen in beispielloser Geschwindigkeit und Menge verfügbar sind, ist es entscheidend, dass wissenschaftliche Erkenntnisse verständlich und zugänglich vermittelt werden. Mit dieser zweiten Ausgabe des CISPA Display, einer Art wissenschaftlichem Jahrbuch, möchten wir Ihnen einen Einblick in die Themen geben, die uns und unsere Forschenden am CISPA im Jahr 2024 bewegt und herausgefordert haben. Wir wollen Ihnen zeigen, wie breit das Spektrum unserer Forschung ist, und welchen Beitrag das CISPA für die Gesellschaft leistet.

Die Bedeutung der Wissenschaft für die Gesellschaft

In einer demokratischen Gesellschaft ist Wissen kein Selbstzweck. Es bildet das Fundament für mündige Entscheidungen, für die Lösung von Herausforderungen und die Gestaltung einer lebenswerten Zukunft. Die am CISPA gewonnen wissenschaftlichen Erkenntnisse zu Fragen der Sicherheit unserer IT-Systeme und zur Gestaltung vertrauenswürdiger künstlicher Intelligenz können uns zum Beispiel helfen, persönliche Informationen und kritische Infrastrukturen zu schützen, transparente und faire Algorithmen zu entwickeln, die nachvollziehbare Entscheidungen treffen. Doch wem nutzen unsere Forschungsergebnisse, wenn wir sie nicht auch vermitteln können?

Herausforderungen der Wissenschafts-kommunikation

Komplexe Inhalte so aufzubereiten, dass sie verständlich und relevant werden – ohne dabei die notwendige Präzision zu verlieren – das ist eine der größten Herausforderungen in der Wissenschaftskommunikation. Wir als Kommunikator:innen müssen eine Balance zwischen Verständlichkeit und Tiefe finden. In unserer Abteilung arbeiten wir deshalb eng mit unseren Forschenden zusammen, um die Essenz ihrer Arbeit zu erfassen und diese aufzugreifen, ohne dabei wichtige Nuancen zu verlieren. Gleichzeitig stoßen wir immer wieder an die Grenzen dessen, was sich einfach erklären lässt – nicht, weil die Forschung unzugänglich ist, sondern weil sie in ihrer Tiefe eine geduldige und differenzierte Betrachtung erfordert.

In der heutigen Medienlandschaft, die oft von schnellen Schlagzeilen und leicht konsumierbaren Inhalten geprägt ist, können die Feinheiten der Wissenschaft

Wir wollen mit dem CISPA Display die nötige Brücke zwischen Wissenschaft und Gesellschaft schlagen. Dieses Jahrbuch soll verdeutlichen, wie unsere Forschungs-arbeit Impulse für gesellschaftliche Fragen liefert.

schnell verloren gehen. Eine sorgfältige, fundierte Wissenschaftskommunikation braucht Zeit, Ressourcen und vor allem das Verständnis, dass Wissen nicht immer auf simple Antworten reduziert werden kann. Unser Anspruch ist es, nicht nur Ergebnisse zu liefern, sondern auch den Weg, den unsere Forschenden gegangen sind, anschaulich zu machen. Nur so kann es auch Vertrauen in den wissenschaftlichen Prozess geben.

Wir wollen mit dem CISPA Display die nötige Brücke zwischen Wissenschaft und Gesellschaft schlagen. Dieses Jahrbuch soll verdeutlichen, wie unsere Forschungarbeit Impulse für gesellschaftliche Fragen liefert. Es geht darum, Neugier zu wecken, Reflexion anzuregen und die Relevanz wissenschaftlicher Erkenntnisse für die eigene Lebenswelt sichtbar zu machen.

Grenzen und Verantwortung der Forschung

Wissenschaft ist eine Quelle der Erkenntnis. Sie kann Wissen schaffen, Orientierung bieten und die Grundlage schaffen, um fundierte Entscheidungen in Bezug auf aktuelle Herausforderungen zu treffen. Beispiele wie der Klimawandel, die Bedrohung durch gezielte Desinformation sowie der Schutz unserer sensibelsten Daten zeigen uns, dass Forschungsergebnisse oft erst durch das Zusammenspiel vieler Disziplinen zu tragfähigen Lösungen führen können. Forschung kann und sollte Anstöße geben, doch die Umsetzung liegt letztlich in der Verantwortung der Gesellschaft als Ganzes.

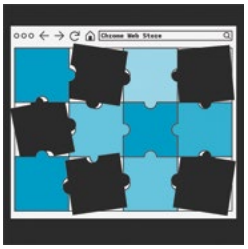
Wert der Wissenschaft

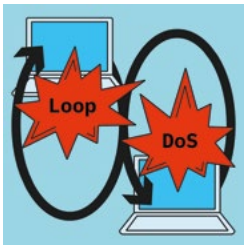
Zum Abschluss wollen wir unseren Forschenden danken. Die Zusammenarbeit mit ihnen ist für uns als Kommunikator:innen unendlich bereichernd. Nur durch ihre Hingabe, ihren Wissensdurst und ihre intensive Arbeit kann es eine Publikation wie das CISPA Display überhaupt geben.

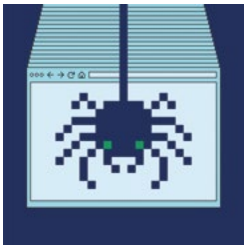
Wir hoffen, dass dieses Jahrbuch Ihnen nicht nur Einsichten, sondern auch Freude an der Vielfalt und Tiefe der Forschung bringt – und dass es dazu beiträgt, den Wert der Wissenschaft für unsere Gesellschaft zu unterstreichen.

INDEX

INDEX







© Lea Mosbach

Online-Shops, Social-Media-Konten, Online-Banking – überall brauchen Internetnutzer:innen Passwörter. Diese müssen möglichst lang und komplex sein, um die Konten ausreichend abzusichern. Eine Mammut-Denkaufgabe oder noch schlimmer: Zettelwirtschaft. Passwortmanager können hier Abhilfe schaffen. Allerdings kommt das Sicherheitsplus, das sie bringen, in der Praxis häufig nicht richtig zum Tragen. Der Grund: Das richtige Aufsetzen der Tools ist häufig umständlich und zeitintensiv. Das zeigt eine qualitative Studie von CISPA-Forscherin Sabrina Amft, die im Team von CISPA-Faculty Prof. Dr. Sascha Fahl in Hannover arbeitet. Das dazugehörige 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" hat sie auf dem Symposium on Usable Privacy and Security 2023 (SOUPS) vorgestellt.

Worin Passwortmanager besser werden müssen

Sabrina Amft

Passwortmanager sind weit mehr als ein digitales Pendant zum Passwort-Büchlein. Denn die Programme speichern nicht nur die Login-Daten für verschiedene Internetdienste, sie haben zwei weitere nützliche Funktionen: Sie können starke Passwörter für die Nutzenden generieren und checken bei einem Login, ob sich die Nutzenden wirklich auf der avisierten Webseite einloggen und nicht etwa auf eine Fake-Seite gelockt werden. „Damit die hilfreichen Funktionen dieser Programme auch wirklich greifen können, müssen die Nutzenden sie richtig einrichten. Und das ist oft viel Arbeit“, sagt Sabrina Amft. Die CISPA-Forscherin liefert mit der Studie keine repräsentativen Zahlen. Vielmehr geht es ihr darum, eine Bestandsaufnahme zu machen, wie die Tools genutzt werden und welche Hürden bei deren Konfiguration bestehen. Dazu hat sie gemeinsam mit Forschenden des CISPA, der Leibniz Universität, der George Washington University und der Uni Paderborn 279 Nutzer:innen von Passwortmanagern befragt sowie 14 populäre Tools und deren Funktionsweisen untersucht.

Passwortmanagement am Fließband

„Unserer Erfahrung nach haben Nutzer:innen häufig ein Passwort, das sie in Abwandlung für viele Accounts nutzen. Nicht selten ist dieses zudem eher schwach. Passwortmanager erlauben ihnen, für jeden Account ein einzigartiges, komplexes Passwort zu erstellen und einfach zu verwalten. Allerdings müssen sie dafür erstmal ihre bestehenden Accounts mit einem neuen Passwort versehen und in den Passwortmanager speichern. Bei durchschnittlich 100 Internetkonten pro Person keine leichte Aufgabe“, erklärt Amft. Und so wundert es nicht, dass ihre Studie zeigt, dass Nutzende meist nicht alle Internetkonten in die Programme aufnehmen. „Erstaunlich ist allerdings, dass sie das aus konträren Gründen nicht tun. So gaben die Einen an, für sie unwichtige Konten nicht in den Passwortmanager zu übernehmen, weil es da nicht so sehr auf Sicherheit ankäme. Andere haben beispielsweise wichtige Daten wie ihr Online-Banking-Passwort nicht erfasst, weil sie Passwortmanagern nicht ausreichend trauen.“

Berechtigte Sorge oder Übervorsicht?

Es gab in der Vergangenheit Angriffe auf große Passwortmanager wie LastPass oder Norton. „Die Sorge ist also nicht ganz unbegründet“, sagt Amft. Die Folgen solcher Angriffe können laut der Forscherin unterschiedlich ausfallen: „Wenn die Hersteller:innen eine ordentliche

Verschlüsselung haben, dann können Hacker:innen zwar den verschlüsselten Datensatz klauen, aber letztlich müssen sie viel Energie in den Versuch stecken, an die Daten auch ranzukommen.“ Dass Angreifer:innen diese Mühe nicht scheuen, zeigt ein Bericht des IT-Fachmagazin Heise aus dem September 2023 über Cyberkriminelle, die Passworttresore knacken und so Zugangsdaten zu Krypto-Wallets erhalten. Norton Life Lock warnte seine Nutzer:innen im Januar 2023, dass Hacker:innen versucht hatten, durch massenhaftes Durchprobieren beliebter Passwörter Zugriff auf Kundendaten zu bekommen – und zum Teil erfolgreich waren. Ein Grund mehr, die Passwortmanager selbst mit einem starken Passwort zu-schützen. Für Amft ist trotzdem klar, dass die Entscheidung gegen Passwortmanager dennoch die schlechtere Wahl ist: „Schwache Passwörter, die für mehr als einen Account genutzt werden, sind ein sehr viel größeres Sicherheitsproblem. Auch weil Vorfälle bei Passwortmanagern kommuniziert und auf kompromittierte Daten hingewiesen wird.“

Bequemlichkeit vor Sicherheit

Amfts Befragung der Nutzenden von Passwortmanagern zeigt deutlich: Bequemlichkeit geht über Sicherheit. So gaben viele der Befragten an, dass sie die Tools vor allem nutzten, weil sie sich so die Eingabe von Passwörtern und deren Verwaltung sparen wollen. „Sicherheit ist für sie eher ein untergeordneter Faktor“, sagt Amft. So wundert es nicht, dass den sichersten Weg, alle Konten zu erfassen und die dazugehörigen Passwörter auf eine stärkere Alternative upzudaten, nahezu keine:r der Studien-Teilnehmenden wählte. Die Mehrheit der Nutzenden gab an, Accounts und deren Passwörter erst dann in den Passwortmanager zu übernehmen, wenn sie im Alltag die entsprechenden Seiten besuchen. „Dabei spielt neben der Tatsache, dass das direkte Erfassen aller Konten sehr aufwendig ist, auch eine Rolle, dass viele Nutzenden gar keine Übersicht über ihre Internetkonten haben“, erklärt Amft. Ein Großteil der Befragten gab an, zumindest einige Passwörter gegen sicherere Alternativen ausgetauscht zu haben.

Integrierte Passwortmanager werden anders genutzt

Unterschiede im Nutzungsverhalten zeigten sich vor allem im Vergleich zwischen gekauften Passwortmanagern und in den Browsern integrierten. „Oft sind sich Menschen gar nicht bewusst, dass sie einen Passwortmanager nutzen, wenn sie beispielsweise in Google Chrome oder Mozilla Firefox ihre Passwörter hinterlegen.“ In diesen integrierten Versionen der Programme werden Passwörter selten manuell erfasst. „Eigentlich ist es ein gutes Zeichen, wenn Sicherheitstools so designt sind, dass Nutzende kaum merken, dass sie welche benutzen. Früher waren die integrierten Versionen der Passwort-

manager leider häufig nicht stark genug abgesichert, aber es gab in den vergangenen Jahren Fortschritte."

Empfehlungen an Entwickler:innen

„Einige Anbieter:innen haben schon gute Ansätze. Zum Beispiel scannen einige Passwortmanager von den Nutzenden besuchte Websites und deren Mailaccounts, um für sie eine Liste mit Vorschlägen zu generieren, wo überall in der Vergangenheit ein Passwort angelegt wurde. Laufen solche Scans ausschließlich lokal, können sie auch datenschutzkonform umgesetzt werden", erklärt Amft. Auch das Anzeigen beliebter Seiten könne eine Lösung sein, falls das Scannen nicht möglich ist. „Zudem brauchen wir insgesamt mehr Automatisierung. Der Prozess, Passwörter hinzuzufügen und upzudaten muss so gestaltet sein, dass er möglichst reibungslos abläuft. Der Import vorhandener Passwörter muss zudem sicher gestaltet werden. Die Passwortmanager sollten dafür eigene Schnittstellen anbieten, damit keine lokalen Passwortlisten im Klartext gespeichert werden müssen." Dem Misstrauen den Programmen gegenüber könnten Entwickler:innen laut Amft damit begegnen, Datenschutz-Labels einzuführen, die die genutzte Verschlüsselung und andere Sicherheitsmechanismen bewerten und Nutzer:innen eine einfache Möglichkeit geben, die Sicherheit der Programme zu beurteilen.

Amft, Sabrina; Höltervennhoff, 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

© Lea Mosbach

Menschen nutzen Online-Sicherheitsmechanismen aus einer Vielzahl von Gründen. In manchen Fällen werden auch verschiedene Mechanismen miteinander kombiniert. So etwa, wenn zum Anonymisierungsnetzwerk Tor zusätzlich eine VPN-Verbindung genutzt wird. Oft ist dabei unklar, woher die Informationen stammen, dass ein bestimmter Mechanismus nützlich ist und tatsächlich mehr Sicherheit bietet. Dr. Matthias Fassl aus dem Team von CISPA-Faculty Dr. Katharina Krombholz hat nun untersucht, wie häufig Nutzer:innen diese Kombination wählen und was sie davon erwarten. Die Ergebnisse hat er im Paper „Investigating Security Folklore: A Case study on the Tor over VPN Phenomenon" bei der Conference on Computer-Supported Cooperative Work & Social Computing 2023 (CSCW) veröffentlicht und dafür eine Honorable Mention Award und eine Methods Recognition erhalten.

Das Beispiel Tor und VPN: Cybersicherheit zwischen Tatsachen und Erzählungen

Matthias Fassl

Tor und VPN sind zwei IT-Anwendungen, von denen vermutlich fast alle Nutzer:innen schon einmal gehört haben. Die Gründe sind ihre hohe Präsenz im medialen Diskurs und bei VPN auch die breite Nutzer:innenbasis. Tor ist ein Anonymisierungsnetzwerk. Dessen bekanntestes Tool ist der Tor-Browser, mit dem anonymes Surfen im Netz möglich ist, erklärt CISPA-Forscher Matthias Fassl. VPN ist die Abkürzung für Virtual Private Network. Damit werden verschlüsselte Datenleitungen zwischen zwei Servern über ein virtuelles Netzwerk aufgebaut. Ein neues Phänomen ist, dass Nutzer:innen die beiden Anwendungen kombinieren, in der Fachsprache „Tor over VPN" genannt. „Wir sind darauf in Online-Foren gestoßen und haben uns gefragt, wie viele Leute das überhaupt verwenden", so Fassl. „Das Interessante ist dabei prinzipiell erstmal die Kombination der Tools. Da sie dafür nicht entwickelt wurden, ist nicht ganz klar, was dabei passiert. Und für uns aus der Usable Security-Forschung ist spannend, welche Vorstellung die Menschen vom Nutzen einer Kombination der Tools haben", so der Forscher weiter. Die Usable Security-Forschung ist ein Forschungszweig der Cybersicherheit, der den Fokus weniger auf die Anwendungen an sich, als auf den Umgang der Menschen damit richtet.

Dreistufiges Vorgehen

Um herauszufinden, was es mit dem Phänomen „Tor over VPN" auf sich hat, sind Fassl und Kolleg:innen dreistufig vorgegangen. „Wir haben zuerst untersucht, wie viele Nutzer:innen die Kombination überhaupt verwenden", erzählt der CISPA-Forscher. Durch Messungen an den Knotenpunkten des Tor-Netzwerkes konnten er und sein Team herausfinden, dass 6,23 Prozent der Zugriffe über VPN erfolgten. „In einem zweiten Schritt haben wir dann in einer Befragung geschaut, was Leute sich von der Kombination erhoffen und ob sie damit bestimmte Sicherheitsvorteile erzielen wollen", so Fassl weiter. Zuerst einmal zeigte sich, dass es zwei Arten von Nutzer:innen gibt: diejenigen, die VPN immer nutzen, egal in welchem Kontext, und diejenigen, die gezielt eine VPN-Verbindung für das Tor-Netzwerk nutzen. Vor allem die letzte

Gruppe war stark vertreten, mit ganz unterschiedlichen Motivationen wie etwa dem Wunsch Geo-Blocking, also das Sperren von Websites beim Zugriff aus bestimmten geografischen Regionen, zu umgehen oder IP-Adressen zu verstecken. „Zuletzt haben wir Onlinemedien, Social-Media und ähnliches nach Artikeln und Diskussionen zu dem Thema durchsucht, um herauszufinden, wie in diesen über die Kombination der Mechanismen gesprochen wird“, erklärt der CISPA-Forscher. Dabei fanden sich viele Empfehlungen, in denen die Kombination aus Tor und VPN beschrieben wurde, aber ohne den tatsächlichen Nutzen darzulegen. Den Glauben vieler Nutzer:innen daran, dass ein VPN-Zugang sie vor Gefahren im Tor-Netzwerk schützt, erklärt Fassl mit der Rolle der VPN-Provider. Diese würden die Gefahren des Tor-Netzwerkes, wie etwa Darknet Markets für illegale Produkte, aufbauschen, um ihre eigenen Produkte zu promoten. „Klar ist, dass ein VPN nicht notwendig ist, um den Tor-Browser sicher und anonym zu verwenden“, so Fassl. „Mögliche Sicherheitsvorteile von ‚Tor over VPN‘ sind bis heute unklar.“

»Wir hätten es natürlich am liebsten, dass die Menschen Sicherheitsmechanismen verwenden, weil diese für sie passen und von denen sie verstehen, was sie bewirken. Das ist offensichtlich in der Realität nicht so.«

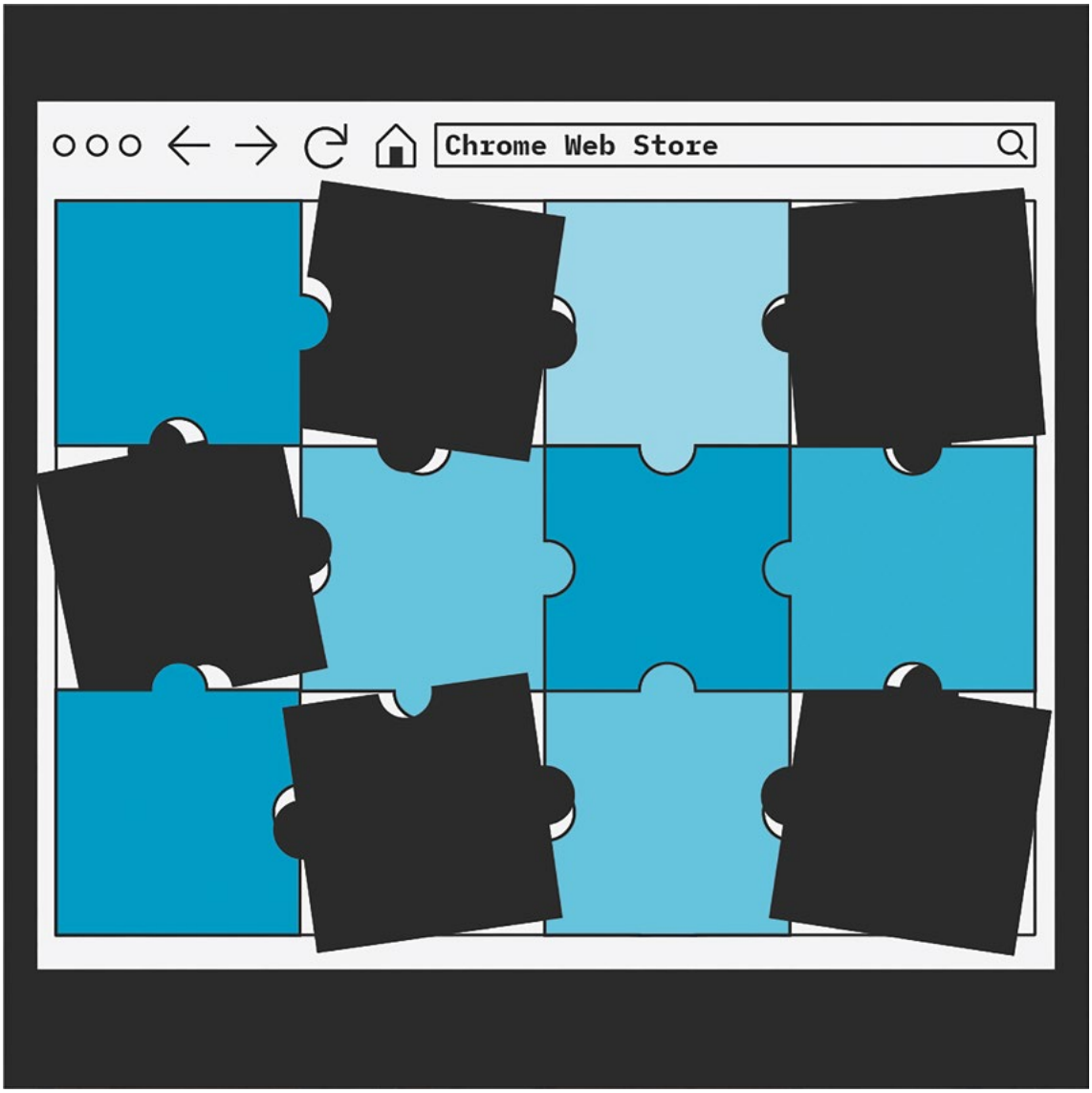
Der Begriff Security Folklore als Erklärungsmodell

Um zu erklären, warum Menschen die Kombination aus Tor und VPN trotzdem nutzen, arbeiten Fassl und seine Kolleg:innen mit dem Begriff der Security Folklore. Fassl versteht darunter „die Weitergabe von Praktiken und Tipps in sozialen Gruppen die Security und Privacy betreffen. Die können explizit aber auch oft implizit passieren, eben durch Erzählen oder durch Vorführen und müssen auch nicht unbedingt niedergeschrieben sein.“ Wenn also Nutzer:innen beim Surfen in sozialen Netzwerken einen Post zu dem Thema lesen oder in einem Film sehen, wie jemand diese Kombination nutzt, kann sich bei ihnen die Vorstellung verfestigen, dass dies sinnvoll ist. Die Erzählung darüber, dass die Kombination von Tor mit VPN besseren Schutz bietet, wäre dann eine sogenannte Security Folklore. Verstärkt wird dies durch normative Überzeugungen. So sind Menschen eher geneigt, bestimmte Sicherheitsmechanismen anzuwenden, wenn sie diese bei anderen beobachtet haben.

Take-Aways für die Cybersicherheitsforschung

Für die Cybersicherheitsforschung ist das Forschungsergebnis insofern interessant, als damit gezeigt wird, dass nicht nur sachliche Informationen von Expert:innen, sondern auch der popkulturelle Umgang mit und der mediale Diskurs über Sicherheitsmechanismen eine wichtige Rolle spielen. Aber was hat das für Folgen für die Forschung? „Für uns als Forscher macht es das etwas schwerer“, erklärt Fassl. „Wir hätten es natürlich am liebsten, dass die Menschen Sicherheitsmechanismen verwenden, weil diese für sie passen und von denen sie verstehen, was sie bewirken. Das ist offensichtlich in der Realität nicht so. Die Menschen machen Dinge aus den verschiedensten Gründen, auch wenn sie sie nicht verstehen.“ Dagegen anzuarbeiten, ist jedoch eine große Herausforderung: „Wenn wir zum Beispiel sehen, dass in popkulturellen Medien wie Fernsehserien Sicherheitsmechanismen vorkommen, könnten wir etwa darauf hinarbeiten, dass dort bessere oder allgemeingültigere Verfahren vorgestellt werden.“ Da sieht Fassl durchaus noch einigen Forschungsbedarf: „Ich bin fasziniert von Sozialdynamiken sowie dem Einfluss sozialer Normen. Deswegen würde ich mir gerne systematischer anschauen, wie in Hollywoodfilmen und Fernsehserien auf Netflix Sicherheitsmechanismen zum Thema gemacht werden.“ Wir dürfen gespannt sein, was er dabei zu Tage fördert.

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



© Janine Wichmann-Paulus

Millionen von Menschen nutzen täglich Browser-Erweiterungen, etwa um Werbung auf Websites zu blockieren. Aber ist die Nutzung der von Drittanbietern zur Verfügung gestellten Erweiterungen überhaupt sicher? CISPA-Faculty Dr. Aurore Fass hat dies nun anhand von Erweiterungen für Chrome, den Webbrowser von Google, zusammen mit ihren Studentinnen Sheryl Hsu und Manda Tran untersucht und damit zum ersten Mal eine große Studie über den Chrome Web Store vorgelegt. Ihr zugehöriges Paper „What is in the Chrome Web Store?“ wurde auf der ACM ASIA Conference on Computer and Communications Security 2024 vorgestellt.

Sicherheitslücken bei Browserweiterungen im Chrome Web Store

Aurore Fass

Wenn Nutzer:innen auf das Internet zugreifen wollen, benötigen sie dafür einen Webbrowser wie Chrome, Safari, Mozilla Firefox oder Microsoft Edge. Wenn die Standard-Features der Browser nicht ausreichen, können Erweiterungen von Drittanbietern genutzt werden. „Browser-Erweiterungen sind sehr nützlich, um die Funktionalität des Browsers zu erweitern. Fügt man zum Beispiel Erweiterungen wie einen Ad-Blocker hinzu, lässt sich damit Werbung auf Websites blockieren oder einschränken“, erklärt CISPA-Faculty Dr. Aurore Fass. Die Erweiterungen lassen sich über die Browser downloaden und mit wenigen Klicks installieren. Alle gängigen Web-Browser bieten Erweiterungen an. Für die Studie fiel die Wahl der CISPA-Faculty auf Google Chrome. „Wir verwenden Chrome, weil es der beliebteste Browser ist“, erläutert die Fass. „Und Chrome hat eine Web-Erweiterungs-API, die browserübergreifend funktioniert. Aus Entwickler:innenperspektive sind also Erweiterungen für Chrome oder Firefox sehr ähnlich.“ Ein weiterer wichtiger Faktor war, dass ein Tool namens „Chrome-Stats“ den Datenzugang zu Chrome erleichtert. „Chrome-Stats sammelt Längsschnittdaten für Erweiterungen im Chrome Web Store. Das war sehr wichtig, denn sobald eine Erweiterung aus dem Store entfernt wird, haben wir keinen Zugriff auf die Metadaten oder den Quellcode dieser Erweiterungen“, so Fass weiter.

Das Feld der sicherheitskritischen Erweiterungen

Für ihre Untersuchung arbeitet die Forscherin mit der Unterscheidung von harmlosen und sicherheitskritischen Erweiterungen, auf Englisch „Security Noteworthy Extensions (SNE)“ genannt, die sie in drei Kategorien unterteilt. „Zunächst gibt es Erweiterungen, die Malware enthalten“, erklärt Fass. „Diese Erweiterungen sind bösartig, da sie speziell von Leuten entwickelt wurden, die Benutzer:innen schaden wollen. Die zweite Kategorie sind Erweiterungen, die gegen die Datenschutzrichtlinien von Google verstoßen. Und die dritte Kategorie sind Erweiterungen, die Schwachstellen enthalten.“ Letztere wurden zwar von Entwickler:innen in guter Absicht entwickelt, aber sie enthalten Fehler, die Sicherheitslücken zur Folge haben können. Die Gefahr von SNEs ist, dass diese von Angreifer:innern genutzt werden, um Malware zu versenden, Nutzer:innen zu tracken und auszuspionieren oder Daten zu stehlen. Untersucht wurden von Fass und ihren

Kolleg:innen Erweiterungen, die zwischen Juli 2020 und Februar 2023 im Chrome Web Store verfügbar waren.

Lebensdauer und Sicherheitsrisiken von Erweiterungen

Die erste wichtige Erkenntnis von Fass war, dass Erweiterungen sehr kurze Lebenszyklen haben. „60 Prozent bleiben weniger als ein Jahr im Chrome Web Store", erklärt Fass. „Das ist verrückt! Damit braucht es regelmäßige Analysen, um zu wissen, was im Store vorhanden ist." Die zweite Erkenntnis bezieht sich auf die Präsenz von sicherheitskritischen Erweiterungen. „Wir haben im Chrome Web Store viele sicherheitskritische Erweiterungen analysiert, die Hunderte Millionen von Nutzer:innen betreffen", so Fass weiter. „Einige davon bleiben zehn Jahre lang im Store und beeinträchtigen die Sicherheit und die Privatsphäre der Nutzer:innen für eine sehr lange Zeit." Die dritte Erkenntnis bezieht sich auf Ähnlichkeiten zwischen Erweiterungen. „Mit Hilfe von Clustering-Prozessen konnten wir Erweiterungen erkennen, die eine ähnliche Code-Basis haben", erläutert Fass. „Das hilft, um sicherheitskritische Erweiterungen aufzuspüren. Denn wenn eine Erweiterung einer sicherheitskritischen Erweiterung ähnelt, können wir stark davon ausgehen, dass sie ebenfalls sicherheitskritisch ist. Das kann helfen, bis dato unbekannte sicherheitskritische Erweiterungen zu erkennen." Die letzte Erkenntnis hängt mit der mangelnden Wartung des Chrome Web Store zusammen. „60 Prozent der Erweiterungen wurden seit ihrer Veröffentlichung im Store nicht aktualisiert. Das bedeutet, dass sie nicht von den neuen APIs oder Funktionen von Chrome profitieren, die die Sicherheit und Privatsphäre verbessern, wie dem neuen Manifest V3", so Fass.

»Wir haben im Chrome Web Store viele sicherheitskritische Erweiterungen analysiert,die Hunderte Millionen von Nutzer:innen betreffen.«

Erkenntnisse zum Quellcode der Erweiterungen

In einem weiteren Schritt hat Fass auch den Quellcode der Erweiterungen im Chrome Web Store näher untersucht. Dahinter stand die Annahme, dass die Suche nach ähnlichem Quellcode dabei helfen kann, SNEs einfacher und schneller zu entdecken. Und tatsächlich entdeckte Fass tausende Cluster mit ähnlichem Quellcode. Das ist nicht verwunderlich, denn Entwickler:innen greifen in ihrer Arbeit häufig auf vorgefertigte Codes zurück, sogenannte Bibliotheken, die zum Ausführen bestimmter Aufgaben genutzt werden und den Prorgammierungsaufwand verringern. „30 Prozent der Browser-Erweiterungen haben eine verwundbare Bibliothek in ihrem Quellcode“, erklärt Fass. „Wir haben zwar nicht untersucht, ob dies tatsächlich ausgenutzt werden kann, aber wir halten es trotzdem für eine unsaubere Praxis, diese anfälligen Bibliotheken zu verwenden. Man fordert eigentlich heraus, dass etwas Schlimmes passiert.“ Das Problem besteht in der Abhängigkeit von Drittanbietern und deren mangelnder Wartung der Codes. „Dies führt dazu, dass die Entwickler:innen einen veralteten, nicht gewarteten Code verwenden, der Sicherheitslücken enthalten könnte“, so Fass. Besonders häufig nutzten Entwickler:innen Quellcode aus einem Tool namens Extensionizr.

Was können Nutzer:innen, Entwickler:innen und Google tun?

Danach gefragt, was Entwickler:innen tun könnten, um ihre Erweiterungen sicherer zu machen, antwortet Fass: „Entwickler:innen mit guten Intentionen sollten sich darüber bewusst werden, was bei Erweiterungen schiefgehen kann. Gut wäre es, wenn sie Bedrohungsmodelle im Kopf haben und darüber nachdenken würden, was Einfallstore für Angreifer:innen sein könnten.“ Auch regelmäßige Updates sind ein wichtiger Faktor. Schwieriger ist es für die Nutzer:innen von Erweiterungen. „Für die gibt es nur wenige Möglichkeiten herauszufinden, ob eine Erweiterung gefährlich ist oder nicht“, erklärt Fass. „Theoretisch kann man sich die Berechtigungen von Erweiterungen ansehen, aber die meisten Nutzer:innen haben sich damit nicht beschäftigt und verstehen die Details nicht.“ Umso wichtiger ist eine bessere Kontrolle durch Google. „Google hat ein Überprüfungssystem, in dem Erweiterungen vor der Veröffentlichung im Chrome Web Store kontrolliert werden“, so die CISPA-Faculty weiter. Fass hat auch eine Idee, wie sich das Überprüfungssystem verbessern ließe: „In einem älteren Paper zeige ich, wie anfällige Erweiterungen automatisch erkannt werden könnten. Dies könnte in die Pipeline von Google aufgenommen werden.“

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

© Lea Mosbach

Clickbait-PDFs sind noch schlimmer als Clickbait-Überschriften: Sie sind eine neue Art von Phishing-Attacke, die erstmals von der CISPA-Forscherin und Doktorandin Giada Stivala und ihren Kolleg:innen untersucht wurde. Clickbait-PDF-Dateien enthalten per se keine Schadsoftware – stattdessen versuchen sie, Benutzer:innen dazu zu verleiten, auf irgendeine Stelle im Dokument zu klicken, wodurch sie auf bösartige Websites gelangen, die möglicherweise ihre Daten stehlen. Stivala und ihre Kolleg:innen waren die ersten, die Clickbait-PDFs eingehend untersuchten. Ihre Ergebnisse publizierten sie im Paper „From Attachments to SEO: Click Here to Learn More about Clickbait PDFs!“ und stellten sie auf der Annual Computer Security Applications Conference (ACSAC) 2023 vor.

Dieser Artikel wird Ihr Leben verändern! – Clickbait-PDFs sind die neueste Phishing-Masche

Giada Stivala

Stellen Sie sich vor: Sie haben die Frist für Ihre Steuererklärung verpasst. Sie öffnen Ihre Lieblingssuchmaschine und tippen den Namen des Steuerformulars ein, das Sie suchen. Genervt und in Eile klicken Sie auf die erste PDF-Datei, die die Suchmaschine ausspuckt. Es erscheint ein Captcha, das Sie auffordert, zu bestätigen, dass Sie kein Roboter sind. Sie versuchen, das Kästchen anzukreuzen, aber plötzlich werden Sie auf eine Website umgeleitet, die Ihnen alle möglichen Pop-ups zeigt, von denen keines besonders beruhigend aussieht. Mit etwas Pech könnte Ihr Gerät jetzt infiziert sein. Sie sind einem Clickbait-PDF zum Opfer gefallen, einer neuen Art von Phishing-Masche, die darauf abzielt, Ihre Daten zu stehlen.

Die neueste Phishing-Masche, getarnt als PDF

Clickbait-PDFs sind ein perfektes Beispiel für das sprichwörtliche „Katz-und-Maus-Spiel" im Bereich der Cybersicherheit: Hacker:innen denken sich neue Angriffe aus, Cybersicherheitsforscher:innen entwickeln Gegenmaßnahmen, Hacker:innen wiederum umgehen die Gegenmaßnahmen und so setzt sich der Kreislauf endlos fort. Phishing-Betrug an sich ist nichts Neues: Die meisten Benutzer:innen sind wahrscheinlich schon einmal Phishing-E-Mails begegnet. Diese geben zum Beispiel vor, von der eigenen Bank zu stammen, und fordern dazu auf, Anmeldedaten einzugeben oder zweifelhafte Websites zu besuchen, die Geräte infizieren können. Doch da E-Mail-Programme zunehmend besser in der Lage sind, Phishing-Mails zu erkennen und auszusortieren, und Webbrowser bösartige Websites immer effektiver blockieren, suchen Betrüger:innen nach neuen Wegen, um Benutzerdaten zu stehlen. „Diese bestehenden Schutzmechanismen funktionieren ziemlich gut, sodass die Angreifer:innen dem System voraus sein und versuchen müssen, nicht entdeckt zu werden", so die CISPA-Forscherin Giada Stivala.

Clickbait-PDFs umgehen Erkennungsmechanismen

„Mit der Einführung von Clickbait-PDFs haben Internet-Betrüger:innen eine neue Möglichkeit gefunden, der Gegenseite einen Schritt voraus zu sein. PDFs waren bereits dafür bekannt, dass sie eine Bedrohung für Benutzer:innen darstellen können, aber diese PDFs

enthielten dann Malware", sagt Stivala. Diese Dateien wurden in der Regel per E-Mail an Benutzer:innen verschickt und führten nach der Öffnung Programmcode aus, der dann das jeweilige Gerät infizierte. Da diese Art von Angriffen bereits bekannt und erforscht ist, sind Malware-Scanner inzwischen recht gut darin, sie als solche zu erkennen und Benutzer:innen zu warnen. Clickbait-PDFs enthalten jedoch keine Malware. Vom Code her sind sie nicht von harmlosen PDF-Dateien, wie zum Beispiel einem echten Steuererklärungsformular, zu unterscheiden. Da normale Erkennungsmechanismen nicht in der Lage sind, die bösartige Absicht hinter den Dateien zu erkennen, werden diese ganz normal in Suchergebnissen aufgeführt. Benutzer:innen, die dann nach einer bestimmten Datei suchen, zum Beispiel einer Bedienungsanleitung für einen Drucker, könnten so bei einer einfachen Suchanfrage auf ein Clickbait-PDF stoßen, erklärt Stivala.

Darauf ausgelegt, „Klicks zu stehlen"

Stivala und ihre Kolleg:innen wurden ursprünglich von einem Industriepartner angesprochen. Dessen Scanner registrierte plötzlich einen Anstieg an PDF-Dateien. Da diese PDFs keine Schadsoftware enthielten, war ihr eigentlicher Zweck unklar. Bei der Untersuchung dieser Dateien stieß Stivala auf verschiedene Betrugsversuche: PDFs, die sich als Videoplayer ausgeben, um die neuesten Filme kostenlos zu streamen oder solche, die kostenlose Bitcoin mit nur einem Klick versprechen. Die Dateien sind darauf ausgelegt, „Ihren Klick zu stehlen", wie Stivala es ausdrückt. Die Betrüger machen sich die Tatsache zunutze, dass alle gängigen Browser heutzutage über integrierte PDF-Unterstützung verfügen, so dass sich eine PDF-Datei ähnlich wie eine normale Website öffnet. Ahnungslose Benutzer:innen erkennen möglicherweise nicht einmal den Unterschied zwischen der Anzeige einer PDF-Datei und einer Website in ihrem Browser. Ein einziger Klick auf eine dieser PDFs reicht aus, um die Benutzer:innen auf so genannte "Angriffswebsites" zu führen, die ihre Geräte und Daten gefährden können. Diese Seiten ähneln dann dem, was man bei einem Phishing-Versuch per E-Mail vorfinden würden. Die Herausforderung für Betrüger:innen besteht oft darin, Benutzer:innen überhaupt erst dazu zu bringen, bösartige Websites aufzurufen. „In gewisser Weise ändert sich der Teil des Angriffs nach der PDF-Datei nicht. Aber die PDF-Datei selbst stellt eine Neuheit dar, weil es schwieriger ist, sich dagegen zu schützen", sagt Stivala.

SEO-Poisoning nährt Clickbaiting-Angriffe

Um sicher zu stellen, dass tatsächlich jemand auf ihre Clickbait-PDFs stößt, wenden Betrüger:innen eine Methode an, die als "Black Hat Search Engine Optimization (SEO)" oder "SEO Poisoning" bezeichnet wird.

„Suchmaschinenoptimierung ist nicht per se schlecht. Sie kann aus völlig ethischen und legalen Gründen eingesetzt werden", sagt Stivala. Es handelt sich im Wesentlichen um eine Methode zur Optimierung einer Website, damit sie in Suchergebnissen weit oben platziert wird. Unternehmen nutzen dies zum Beispiel aus Marketinggründen. Beim SEO-Poisoning werden jedoch bösartige Website so optimiert, dass sie in den Suchergebnissen höher platziert werden, obwohl sie für die Suchanfrage der Nutzer:innen irrelevant oder für dessen Geräte geradezu gefährlich sind. Das funktioniert zum Beispiel, indem man eine Menge Schlüsselwörter in eine Seite einbaut. Wenn Nutzer:innen dann nach einer Seite suchen, auf der sie einen Film kostenlos streamen können, wird die Seite durch Schlüsselwörter wie Filmnamen höher eingestuft. Noch schlimmer ist allerdings, dass es den Betrüger:innen gelang, ihre PDFs auf die Server legitimer Websites hochzuladen, die zwar unzureichend gesichert waren, aber einen guten Ruf hatten: zum Beispiel die Seiten lokaler Unternehmen oder Schulen. Da diese Seiten nicht bösartig zu sein scheinen, stuften die Suchmaschinen diese Dateien in den Suchergebnissen höher ein. Und da Malware-Scanner die Dateien nicht als bösartig einstuften, wurden die betroffenen Website-Betreiber:innen meist nicht alarmiert. „Sie wussten nicht einmal, dass sich diese Dateien auf ihren Servern befanden, bevor wir Anti-Phishing-Organisationen und Website-Betreiber:innen benachrichtigten", sagt Stivala.

Aufmerksamkeit ist der beste Schutz

Nach der Benachrichtigung durch die Forscher:innen, scheint sich die Lage verbessert zu haben. Es werden weniger dieser Clickbait-PDFs in Suchergebnissen angezeigt. Stivala arbeitet an einer Folgestudie, um festzustellen, wie groß diese Bedrohung noch ist. Doch wie können sich die Nutzer:innen bis dahin am besten vor dieser Art von Angriffen schützen? „Es gibt kein Patentrezept", sagt Stivala. „Diese Angriffe nutzen das schwächste Glied der Kette aus, und das ist in der Regel der Mensch." Benutzer:innen können damit beginnen, auf winzige Hinweise zu achten, zum Beispiel, wenn die URL im Browser eine PDF-Datei anzeigt, wo eigentlich eine normale Website sein sollte. Und ganz allgemein sollten sich Benutzer:innen darüber bewusst sein, dass es sich wahrscheinlich um einen Phishing-Betrug handelt, wenn etwas zu schön erscheint, um wahr zu sein. Zum Beispiel wenn behauptet wird, die neuesten Filme kostenlos anzubieten. Das gilt sowohl für Website als auch für 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

Konsistenz in der Benutzerführung herzustellen, ist ein zentraler Grundsatz im Webdesign. Dies gilt auch bei der Implementierung neuer Sicherheitsstandards wie etwa der Zwei-Faktor-Authentifizierung (2FA). CISPA-Faculty Dr. Sven Bugiel und seine Kollegin Dr. Sanam Ghorbani Lyastani haben für eine neue Studie Kriterien entwickelt, wie sich der 2FA-Prozess auf Websites aus Nutzer:innenperspektive vergleichen lässt. Die Ergebnisse haben sie in ihrem Paper „A Systematic Study of the Consistency of Two-Factor Authentication User Journeys on Top-Ranked Websites“ veröffentlicht, das auf dem Network and Distributed System Security Symposium (NDSS) 2023 vorgestellt wurde.

Neuer Ansatz, um den Prozess der Zwei-Faktor-Authentifizierung auf Websites zu vergleichen

Sven Bugiel

Der Mensch ist ein Gewohnheitstier: Je mehr sich Prozesse und Alltagshandlungen gleichen, umso einfacher erscheint die Umsetzung. Dies gilt auch für das Agieren im Internet. „Wir sind daran gewöhnt, dass sich im Online-Shop der Warenkorb meistens oben rechts auf der Website befindet“, erzählt CISPA-Faculty Dr. Sven Bugiel. Diese Erfahrungswerte ermöglichen es, dass Nutzer:innen schnell und problemlos zwischen Websites verschiedener Anbieter:innen wechseln können. Die von Bugiel geschilderte Beobachtung ist eine wichtige Heuristik aus dem Bereich der User Experience, zu Deutsch Nutzererfahrung, die auch unter „Jakob’s Law of Internet User Experience“ bekannt geworden ist. Während die Nutzererfahrung beim Passwort-gestützten Login als weitgehend konsistent gilt, gibt es bisher keine Forschung darüber, wie dies für den Prozess der 2FA aussieht. „Studien, die sich mit einzelnen Faktoren der Zwei-Faktor-Authentifizierung beschäftigt haben, gibt es schon sehr viele“, erklärt der CISPA-Forscher. „Wir haben uns deswegen die Frage gestellt, wie der Gesamtfluss der Zwei-Faktor-Authentifizierung aussieht.“

Die Zwei-Faktor-Authentifizierung

Aber was genau, macht die Zwei-Faktor-Authentifizierung so interessant? „2FA ist eine der Techniken, die beim Sichern von Nutzer-Accounts immer wichtiger wird“, erklärt Bugiel. „Da sichere und einzigartige Passwörter zu erstellen eine sehr schwierige Aufgabe ist, bietet 2FA die Möglichkeit, eine zweite Sicherheitsbarriere aufzubauen.“ Nutzer:innen identifizieren sich dann beim Login auf einer Website nicht nur mit einem Passwort, sondern zusätzlich mit einem weiteren Faktor. Für die zweite Authentifizierungsebene gibt es viele verschiedene Ansätze. So kann etwa ein Einmal-Code per SMS versendet oder per App generiert werden, aber auch Hardware-Zusätze, die zum Beispiel den Fingerabdruck scannen, sind eine Option. Jede dieser Verfahren kommt mit ihren eigenen Herausforderungen.

»Wenn man sich die User-Journey auf diesen Top-Ranked Websites anschaut, ist die Kernaussage, dass es keine einheitliche Strategie gibt, die alle Websites oder auch nur die Mehrzahl der Websites umsetzen.«

„Ein einheitlicher 2FA-Standard hat sich bisher nicht durchgesetzt“, so Bugiel.

Das Studiendesign der CISPA-Forschenden

Um den Prozess der Zwei-Faktor-Authentifizierung auf Websites zu vergleichen, haben Bugiel und seine Kollegin ihrer Studie das schon erwähnte ‚Jakob's Law of Internet User Experience' zu Grunde gelegt. „Um zu wissen, welche Websites überhaupt die 2FA verwenden, haben wir das 2FA-Directory genutzt“, erzählt Bugiel. „Das ist ein community-geführtes Datenset von Websites, die 2FA in irgendeiner Form unterstützen. Dort sind circa 3.000 Websites gelistet.“ Um die Anzahl der zu untersuchenden Websites sinnvoll zu reduzieren, haben Bugiel und seine Kollegin auf das Tranco-Datenset zurückgegriffen, ein wissenschaftliches Datenset, das Websites rankt. „Aus den bei 2FA gelisteten Websites haben wir dann die bei Tranco weit oben gelisteten Websites rausgefiltert“, so der CISPA-Forscher weiter. „Damit hatten wir Web-

sites in unserem Sample, die wahrscheinlich die meisten Menschen auch kennen.“ Darunter waren Websites wie google.com, amazon.com oder icloud.com, die einer Mehrzahl der Nutzer:innen bekannt sein dürften.

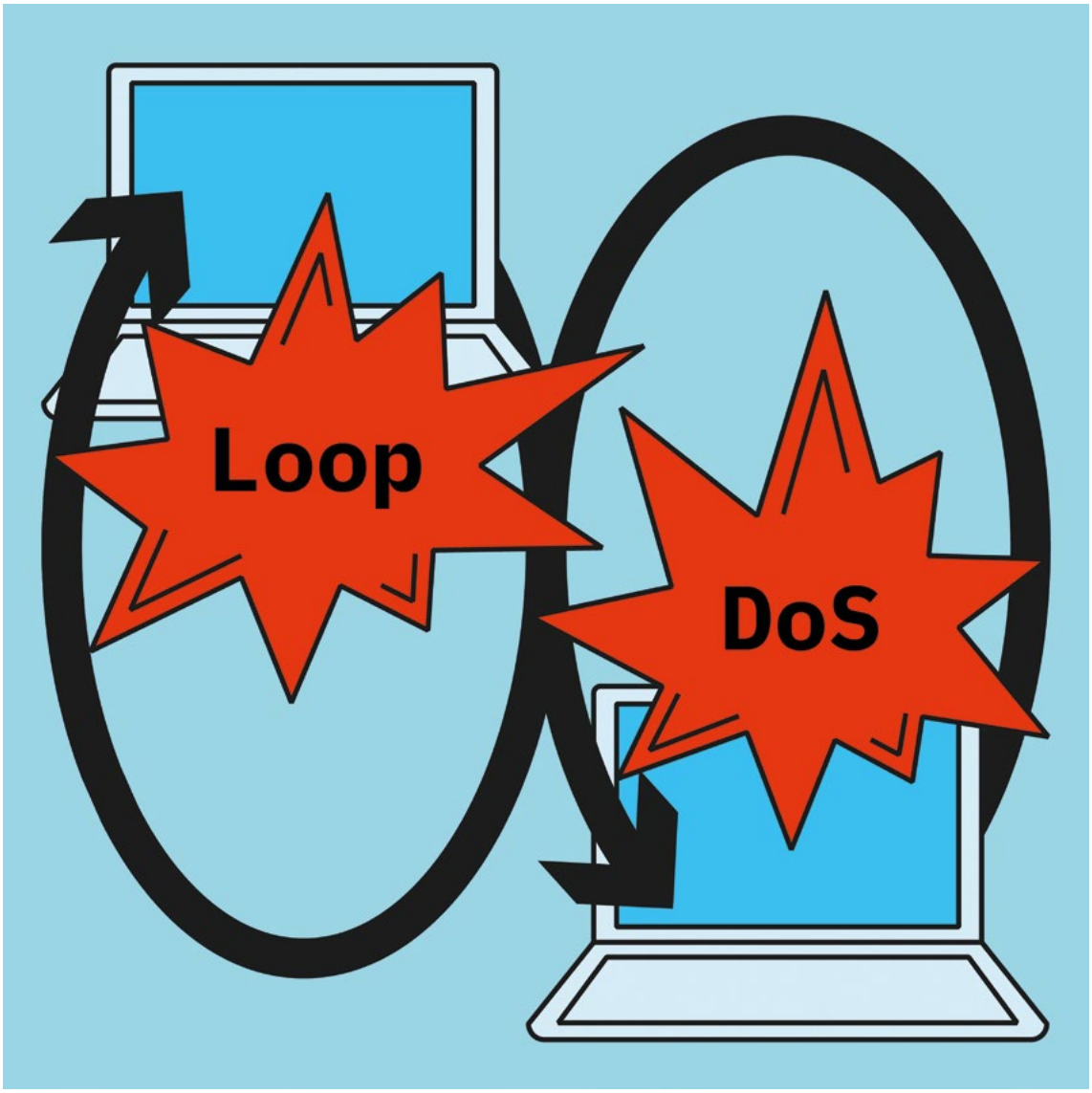
Vergleichs-faktoren für die 2FA-Nutzer-erfahrung

In einem zweiten Schritt entwickelten die CISPA-Forschernden Vergleichsfaktoren, um damit die Websites miteinander vergleichen zu können. „Dazu haben wir die 85 Websites mit zwei Forschenden manuell untersucht und den Prozess auf Video aufgezeichnet. Wir wollten zum Beispiel wissen, an welcher Stelle wir zum ersten Mal auf die 2FA hingewiesen werden, wo die 2FA-Settings liegen und wie das Login und das Logout funktionieren.“ Aus dem gesammelten Datenmaterial identifizierten Bugiel und seine Kollegin insgesamt 22 Vergleichsfaktoren, die sie den fünf Oberkategorien Entdeckung, Einführung, Setup, Nutzung und Deaktivierung der Zwei-Faktor-Authentifizierung zuordneten. Zu den Vergleichsfaktoren für die Entdeckung zählten sie etwa wie die Website auf die Option der 2FA hinweist, ob die Nutzung zwingend vorgegeben ist und ob die Benennung einheitlichen Standards unterliegt. In die Kategorie Setup fielen Vergleichsfaktoren wie eine Bestätigung des Setup-Prozesses, oder ob das Angebot einer Recovery Option besteht.

Ergebnis zeigt keine Konsistenz der Nutzungser-fahrung

„Wenn man sich die User-Journey auf diesen Top-Ranked Websites anschaut, ist die Kernaussage, dass es keine einheitliche Strategie gibt, die alle Websites oder auch nur die Mehrzahl der Websites umsetzen“, erklärt Bugiel. „Stattdessen gibt es diverse Strategien, die von Gruppen von Websites umgesetzt werden. Das sind Cluster von Nutzungsstrategien, die wir in der Analyse definiert haben. Dies bedeutet, dass es keine wirkliche Konsistenz bei diesen 2FA-User-Journeys gibt.“ In Bezug auf Jakob’s Law heißt das, dass damit ein Risiko besteht, dass Benutzer:innen aus diesen Gründen 2FA nicht aktivieren oder die Website nicht nutzen. „Unser Kernbeitrag war zu zeigen, dass es diese Inkonsistenzen überhaupt gibt“, so Bugiel weiter. „Damit öffnen sich dann diverse neue Forschungsfragen. Denn unsere Untersuchung erlaubt uns nur, zu sagen, ob die Nutzerfahrung auf verschiedenen Websites sich ähnelt oder unterscheidet. Aber damit ist noch keine Aussage darüber verbunden, ob dies mehr oder weniger nutzerfreundlich ist.“ Sich diese Unterschiede genauer anzuschauen und gezielt mit Benutzer:innen zu untersuchen, wäre der nächste Schritt. Man darf also auf die nächste Untersuchung aus der Forschungsgruppe des CISPA-Faculty gespannt sein.

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



© Lea Mosbach

Ein neu entdeckter Denial-of-Service-Angriff gefährdet Internetprotokolle auf der Anwendungsschicht, die zur Datenübertragung auf das User Datagram Protocol (UDP) zurückgreifen. Die Angriffsart trägt den Namen „Application-Layer Loop DoS Attacks“ und verbindet immer zwei Server in endlosen Anfrageschleifen, den sogenannten Loops. Aktuelle Internetprotokolle (z.B. DNS, NTP, and TFTP) sind ebenso anfällig für den Angriff wie Legacy-Protokolle (z.B. QOTD, Chargen, Echo). Die Angriffsart wurde von CISPA-Forschenden entdeckt und bedroht schätzungsweise 300.000 Internethosts und deren Netzwerke. Das zugehörige Paper „Loopy Hell(ow): Infinite Traffic Loops at the Application Layer“ wird im August 2024 auf dem Usenix Security Symposium in Philadelphia vorgestellt.

Schleifen ohne Ende: Neuer Denial-of-Service-Angriff gefährdet Protokolle auf der Anwendungsschicht

Christian Rossow

Der neu entdeckte Loop-DoS-Angriff verursacht endlose Anfrageschleifen auf der Anwendungsschicht von Netzwerkprotokollen. Diese Loops entspinnen sich zwischen zwei Netzwerkdiensten, die unablässig auf die Nachricht des jeweils anderen Systems antworten. Dabei entsteht ein so großer Datenverkehr, dass die betroffenen Systeme oder Netzwerke außer Betrieb gesetzt werden. Ist die Attacke erst einmal ausgelöst, können auch die Angreifenden selbst die Anfrageschleife nicht mehr unterbrechen. Zuvor bekannte Loop-Attacken fanden auf der Netzwerkschicht einzelner Netzwerkdienste statt und waren auf eine limitierte Anzahl von Schleifen begrenzt.

Schätzungsweise 300.000 Internethosts bedroht

Entdeckt wurden die „Application-Layer Loop DoS Attacks“ von den CISPA-Forschern Yepeng Pan, Anna Ascheman und Prof. Dr. Christian Rossow. Die Forscher schätzen, dass die neue Angriffsart ca. 300.000 Hosts gefährdet. Entsprechende Schwachstellen haben sie bereits bei TFTP-, DNS- und NTP-Protokollen sowie den sechs Legacy-Protokollen Daytime, Time, Active Users, Echo, Chargen und QOTD identifiziert. Diese Protokolle werden genutzt, um grundlegende Internetfunktionalitäten zu gewährleisten. NTP, oder Network Time Protocol, ermöglicht es mehreren Rechnern in einem Netzwerk, sich auf eine gemeinsame Zeitvorstellung zu einigen. Das DNS-Protokoll, kurz für Domain Name System, ordnet Domain-Namen ihre entsprechenden IP-Adressen zu. TFTP, oder Trivial File Transfer Protocol, organisiert den Austausch von Dateien innerhalb eines Netzwerks ohne vorherige Nutzerauthentifizierung.

Ein einziger Host kann den Angriff auslösen

„Application-Layer Loop DoS Attacks“ basieren auf IP-Spoofing und können von einem einzigen Host ausgelöst werden. „Angreifende könnten beispielsweise einen Loop zwischen zwei anfälligen TFTP-Servern auslösen, indem sie nur eine einzige Fehlermeldung mit einer gefälschten IP-Adresse absetzen. Die beiden Server würden sofort

damit beginnen, sich gegenseitig unablässig TFTP-Fehlermeldungen zuzusenden. Das würde nicht nur beide Server belasten, sondern auch die Netzwerkverbindung zwischen ihnen“, erklärt Rossow. Pan unterstreicht den Neuigkeitswert des entdeckten Angriffs: „Die Loops auf der Anwendungsschicht, die wir entdeckt haben, unterscheiden sich von den bereits bekannten Loops auf der Netzwerkschicht. Deshalb sind bestehende Erkennungsverfahren für Endlosschleifen auf der Netzwerkebene auch nicht in der Lage, sie zu unterbrechen.“

Leichte Beute

„Soweit wir wissen, ist dieser Angriff in der Praxis noch nicht verübt worden. Allerdings wäre es für Angreifende leicht, diese Angriffsart auszunutzen, wenn wir keine Maßnahmen ergreifen würden, um das Risiko einzudämmen“, sagt Rossow. Im Dezember 2023 haben Rossow, Ascheman und Pan ihre Entdeckung an die betroffenen Hersteller und eine vertrauenswürdige Betreiber-Community gemeldet. Zudem haben die Forschenden auch die Veröffentlichung eines angriffsspezifischen Ratgebers koordiniert und gemeinsam mit The Shadowserver Foundation eine Benachrichtigungskampagne angestoßen.

»Soweit wir wissen, ist dieser Angriff in der Praxis noch nicht verübt worden. Allerdings wäre es für Angreifende leicht, diese Angriffsart auszunutzen, wenn wir keine Maßnahmen ergreifen würden, um das Risiko einzudämmen.«

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

Forscher: ***Christian Rossow***
Autorin: ***Eva Michely***

Veröffentlichung
19.03.2024

© Chiara Schwarz

Es ist eine Binsenweisheit: Jede Studie ist nur so gut, wie die Sammlung und Auswertung der Daten. Dies gilt auch für den Umgang mit qualitativen Interviews, die sich in der Cybersicherheitsforschung zunehmender Beliebtheit erfreuen. Je präziser die Interviewtranskription, umso besser sind die Ausgangsvoraussetzungen für die weitere Analyse. Eine Gruppe aus dem Team des Empirical Research Support (ERS) am CISPA hat nun zum ersten Mal systematisch die bekanntesten Transkriptionsservices auf dem Markt miteinander verglichen. Die Ergebnisse haben sie als Poster und kurzen Aufsatz mit dem Titel „From Hashes to Ashes – A Comparison of Transcription Services“ auf der Conference on Computer and Communications Security 2023 (CCS) vorgestellt.

Manuelles Transkribieren schlägt (noch) KI: Eine vergleichende Studie über Transkriptionsservices

Rafael Mrowczynski

Interviews sind eine beliebte Methode zur Erhebung wissenschaftlicher Daten. Ganz grundsätzlich wird dabei zwischen quantitativen und qualitativen Interviews unterschieden. Während erste darauf ausgerichtet sind, mithilfe standardisierter Fragebögen von einer großen Anzahl Befragter statistisch verwertbare Informationen zu bekommen, geht es bei Letzteren um die Gewinnung von Interviewdaten, die den Forschenden Interpretationsmöglichkeiten bieten. Eine besondere Form stellt das Leitfadeninterview dar, beim dem es zwar einen vorbereiteten Fragenkatalog gibt, von dem im Gespräch jedoch abgewichen werden kann. „In der Cybersicherheitsforschung kommen diese Interviews zum Einsatz, wenn es um die Erschließung von Handlungs- und Deutungsmustern von Akteuren geht, die digital vermittelt handeln“, erklärt der Soziologe Dr. Rafael Mrowczynski vom Team des Empirical Research Support (ERS) am CISPA. Das ERS-Team berät die Forschenden des Zentrums bei Methodenfragen.

Die Überführung einer Audiodatei in Text

Ein entscheidender Arbeitsschritt für die qualitative Datenanalyse ist die Transkription. „Die Standardprozedur ist, dass die Audioaufnahmen der Interviews in Text überführt werden. Wichtig für die Qualität der Daten ist, dass die Transkriptionen adäquat sind“, erklärt Mrowczynski. Je nach wissenschaftlicher Disziplin gibt es unterschiedliche Standards für die Transkription. „In der Cybersicherheitsforschung wird meist mit Transkripten gearbeitet, die präzise den Gesprächsinhalt wiedergeben“, so Mrowczynski. Ein adäquates Transkript beinhaltet damit nur die relevanten gesprochenen Wörter. Zur Durchführung der Transkription bieten sich den Forschenden zwei Optionen: Die Transkripte selbst bzw. im Forschungsteam anzufertigen oder sie außer Haus an Drittanbieter zu vergeben.

Unter den Drittanbietern hat neben der manuellen Transkription zuletzt die automatisierte, KI-gestützte

Transkription einen regelrechten Hype erfahren. Dies geht auf die exponentiellen Entwicklungs- und Qualitätssprünge zurück, die KI-Anwendungen in den letzten beiden Jahren in vielen Bereichen erfahren haben. Die CISPA-Forschenden aus dem ERS-Team wollten wissen, welcher Anbieter auf dem Markt die besten Ergebnisse erzielt und wie sich automatisierte, KI-gestützte Angebote im Vergleich zur manuellen Transkription schlagen. Ziel war den Forschenden am CISPA sowie der Cybersicherheits-Community eine Empfehlung für die Arbeit mit qualitativen Interviews geben zu können.

Das Vorgehen des ERS-Teams

Für ihr Forschungsvorhaben erstellten Mrowczynski und seine Kolleg:innen Dr. Maria Hellenthal, Dr. Rudolf Siegel und Dr. Michael Schilling ein Test-Datenset. Dieses bestand aus etwa zehnminütigen Einzelinterviews und Gruppengesprächen mit CISPA-Forschenden auf Deutsch und Englisch. Inhaltlich ging es um das Forschungsfeld der Cybersicherheit. „Wichtig war, dass Fachbegriffe aus der Community fallen, um daran die Präzision der Transkription überprüfen zu können“, erläutert Mrowczynski. Einige Interviews wurden zusätzlich mit Hintergrundgeräuschen angereichert, um realen Settings im Forschungsalltag näher zu kommen.

Die Daten wurden im Dezember 2022 zu elf Anbietern geschickt. Darunter waren die Transkriptionsdienste Amberscript, GoTransript, QualTranscribe, Rev und Scribble sowie die KI-basierten Transkriptionsanbieter Amazon Transcribe, AssemblyAI, Audiotranskription.de, Google Cloud, Microsoft Azure und Whisper AI von OpenAI. Zur Auswertung der erhaltenen Transkripte erstellte Mrowczynski mit seinen Kolleg:innen manuell ein Referenz-Transkript, das als Ausgangspunkt für die vergleichende Analyse diente. In der Analyse selbst ging es dann um zwei zentrale Kriterien. Zum einen wurde die Word-Error-Rate untersucht, die anzeigt, wie viele Wörter sich zwischen einer Abschrift und dem Referenz-Transkript unterscheiden. Zum anderen wurde die qualitative Abweichung vom Referenz-Transkript manuell kodiert.

Manuelle Transkriptionsdienste schlagen KI

Mrowczynski und seine Kolleg:innen kommen in ihrem Aufsatz zu dem Schluss, dass im Allgemeinen „die meisten der manuellen Transkriptionsdienste ein lobenswertes Leistungsniveau [haben], während KI-basierte Dienste häufig bedeutungsverzerrende Abweichungen zwischen Aufnahme und Transkription aufwiesen.“ Die Bedeutungsverzerrung lässt sich gut an Fachbegriffen festmachen, erläutert Mrowczynski: „Im Transkript wurde zum Beispiel aus ‚hashes‘ das Wort ‚ashes‘. So kamen wir auch auf den Aufsatztitel.“

Die besten Ergebnisse unter den KI-Anbietern lieferte Whisper AI von OpenAI. Mit Englisch kamen die meisten

Anbieter besser klar als mit Deutsch. Drei Anbieter boten gar keine deutsche Transkription an. Hintergrundgeräusche wirkten sich generell negativ auf das Ergebnis aus. Probleme hatten die KI-basierten Anbieter vor allem mit der Sprecherzuordnung. Darüber hinaus war bei den von einer KI erstellten Transkripten eine Neuformatierung nötig, bevor die Weiterverarbeitung in einer Software für die qualitative Datenanalyse möglich war. Einschränkend weisen die Forschenden darauf hin, dass ihre Analyse den Stand der Technik im Dezember 2022 wiedergibt und aktuelle Entwicklungen nicht berücksichtigt werden konnten.

»Wichtig war, dass Fachbegriffe aus der Community fallen, um daran die Präzision der Transkription überprüfen zu können.«

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

© Chiara Schwarz

Zoom ist eine der bekanntesten Video-Konferenz-Softwares der Welt. Täglich wird sie von Millionen Nutzer:innen in dem Vertrauen verwendet, dass ihre Daten sicher sind und ihre Unterhaltungen nicht abgehört werden können. Bislang hängt dies von den Zoom-Servern ab, die den Zugang zu den einzelnen Gruppen kontrollieren: Die Zoom-Server überprüfen, ob alle Gruppenmitglieder das Passwort für das Meeting kennen. Nun gibt es einen neuen Weg: CISPA-Faculty Prof. Dr. Cas Cremers, sein Postdoc Mang Zhao und Dr. Eyal Ronen haben eine neue Methode zur Zugangskontrolle entwickelt, bei der der Zoom-Server keine Kenntnis der Passwörter hat. Das dazugehörige Paper „Multi-Stage Group Key Distribution and PAKEs: Securing Zoom Groups against Malicious Servers without New Security Elements“ wird auf dem IEEE Symposium on Security and Privacy 2024 (S&P) vorgestellt.

CISPA-Forscher entwickeln neues Sicherheitskonzept für Zoom-Gruppen

Cas Cremers

Spätestens mit der Corona-Pandemie haben Video-Konferenz-Softwares wie Zoom den Weg in den privaten und beruflichen Alltag vieler Menschen gefunden. Wenn Nutzer:innen an einer Gruppen-Unterhaltung über Zoom teilnehmen wollen, benötigen sie dafür in der Regel ein Passwort. „Im Moment wird das Passwort dem Server mitgeteilt, um zu entscheiden, wer teilnehmen darf", erklärt CISPA-Faculty Prof. Dr. Cas Cremers. Genau dieser Umstand behagt dem Forscher jedoch nicht. Da Zoom im Besitz des Passworts ist, ist Zoom theoretisch in der Lage, auf die Mitglieder der Gruppe zuzugreifen und neue Mitglieder nach Belieben hinzuzufügen.

„Wir hoffen natürlich, dass Zoom sagt: ‚Nein, nein, das werden wir nie tun'. Aber wir haben keine technische Garantie dafür. Uns bleibt nur zu vertrauen, dass sie es nicht tun", erzählt er. Cremers ist es wichtig, dass Sicherheit nicht ausschließlich auf Vertrauen basiert: „Ich möchte eine Technologie, die so beschaffen ist, dass wir uns selbst davon überzeugen können, dass wir eine sichere Verbindung zwischen uns haben und Zoom nicht mithören kann. Diese Garantie will ich haben." Die Herausforderung für den CISPA-Forscher bestand darin, eine Lösung zu entwickeln, ohne dass ein komplettes Re-Design von Zoom notwendig wird. „Theoretisch könnte man sich ein völlig anderes System ausdenken, als das, was Zoom derzeit verwendet. Aber das würde niemand akzeptieren", so Cremers weiter.

Passwortaustausch zwischen Nutzer:innen, anstatt mit dem Zoom-Server

Cremers und seine Kollegen sahen sich also mit der Aufgabe konfrontiert, eine Lösung zu entwickeln, bei der der Zoom-Server nicht alle Passwörter kennt und darüber den Zugang kontrolliert. „Unsere Idee besteht darin, das Passwort nicht mehr an den Server weiterzugeben, sondern nur an die Teilnehmer:innen", erklärt Cas. „Sie sollen untereinander eine sichere Verbindung herstellen können, ohne das Passwort jemals außerhalb der Gruppe weitergeben zu müssen." Dafür haben Cremers und seine Kolleg:innen ein modifiziertes Protokoll zum Austausch der Schlüssel entwickelt, das nur zwischen den Zoom-Nutzer:innen abläuft und die Zoom-Server außen vor lässt.

Der Prozess läuft nur innerhalb der Software ab, ohne dass die Nutzer:innen aktiv etwas tun müssen.

„Wir verwenden dafür einen grundlegenden Baustein namens PAKE (Password-authenticated Key Exchange Protocol) und integrieren ihn in das Zoom-Protokoll. Wir verwenden PAKE, damit Gruppen die Zugangskontrolle selbst durchführen können, ohne sich auf den Zoom-Server zu verlassen“, erklärt Cremers. Da Zoom seinen Source-Code nicht öffentlich macht, musste der CISPA-Forscher sich anderweitig behelfen, um seine Anwendung zu testen: „Wir haben die Beschreibung der Software von Zoom aus ihrem White Paper übernommen,“ erklärt Cremers. Das ist eine vom Unternehmen selbst veröffentlichte, technische Beschreibung der Software, die jedoch keine Details enthält. „Deshalb wir können nicht hundertprozentig sicher sein, was Zoom tatsächlich verwendet. Aber aus unserer Entwicklerperspektive scheint die Lösung zu funktionieren“, so der CISPA-Faculty.

»Wir beweisen, dass mehr Privatsphäre und bessere Sicherheitsgarantien nicht nur ein Hirngespinst sind, sondern dass es einen Weg gibt, wie man diese umsetzen kann.«

Ein klares Ziel vor Augen: Aufzeigen, was möglich ist

Kontakt zum Unternehmen Zoom gab es bisher noch nicht, wenngleich sich der Forscher offen dafür zeigt. Und theoretisch ließe sich der von Cremers zusammen mit seinen Co-Autoren entwickelte Sicherheitsmechanismus auch auf andere Video-Konferenz-Softwares anwenden. Wobei die praktische Umsetzung nicht so stark in seinem Fokus steht. „In gewissem Sinne besteht ein Teil unserer Arbeit auch darin, der Community zu zeigen, was für Möglichkeiten es gibt“, erzählt er. „Wir beweisen, dass mehr Privatsphäre und bessere Sicherheitsgarantien nicht nur ein Hirngespinst sind, sondern dass es einen Weg gibt, wie man diese umsetzen kann.“ Man könnte auch sagen, Cremers‘ Forschung ist wie eine Art Spiegel, um der anwendungsorientierten IT-Wirtschaft mit den Mitteln der Grundlagenforschung aufzuzeigen, was möglich ist und was nicht. Aber der CISPA-Forscher hat auch noch ein anderes, eher gesellschaftspolitisches Ziel vor Augen: „Wir Menschen wollen auf eine Art und Weise kommunizieren, bei der unsere Privatsphäre gewahrt bleibt und andere daran gehindert werden, unsere Kommunikation zu belauschen. Dies müssen auch die Unternehmen berücksichtigen, die die Infrastruktur für unsere Kommunikation bereitstellen.“ Seine Forschung zielt letztlich darauf ab, dieses breite gesellschaftliche Ziel zu erreichen.

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 und Janine Wichmann-Paulus

KI-generierte Bilder, Texte und Audiodateien sind so überzeugend, dass Menschen diese nicht mehr von menschengemachten Inhalten unterscheiden können. Dies ist das Ergebnis einer Online-Befragung mit etwa 3.000 Teilnehmer:innen aus Deutschland, China und den USA. Es ist das erste Mal, dass eine große länderübergreifende Studie diese Form der Medienkompetenz überprüft hat. Die CISPA-Faculty Dr. Lea Schönherr und Prof. Dr. Thorsten Holz präsentierten die Ergebnisse auf dem IEEE Symposium on Security and Privacy 2024 (S&P). Das Paper „A Representative Study on Human Detection of Artificially Generated Media Across Countries" entstand in Kooperation mit der Ruhr-Universität Bochum, der Leibniz Universität Hannover sowie der TU Berlin.

Neue Ergebnisse aus der KI-Forschung: Menschen können KI-generierte Medien kaum erkennen

Thorsten Holz

Die rasanten Entwicklungen der letzten Jahre im Bereich der künstlichen Intelligenz haben zur Folge, dass mit nur wenigen Klicks massenhaft Bilder, Texte und Audiodateien generiert werden können. Prof. Dr. Thorsten Holz erläutert, welche Risiken aus seiner Sicht damit verbunden sind: „Künstlich erzeugter Content kann vielfältig missbraucht werden. Wir haben in diesem Jahr wichtige Wahlen, wie die Wahlen zum EU-Parlament oder die Präsidentschaftswahl in den USA: Da können KI-generierte Medien sehr einfach für politische Meinungsmache genutzt werden. Ich sehe darin eine große Gefahr für unsere Demokratie“. Vor diesem Hintergrund ist eine wichtige Forschungsherausforderung die automatisierte Erkennung von KI-generierten Medien. „Das ist allerdings ein Wettlauf mit der Zeit“, erklärt CISPA-Faculty Dr. Lea Schönherr. „Medien, die mit neu entwickelten Methoden zur Generierung mit KI erstellt sind, werden immer schwieriger mit automatischen Methoden erkannt. Deswegen kommt es im Endeffekt darauf an, ob ein Mensch das entsprechend einschätzen kann.“ Dies war der Ausgangspunkt, um zu untersuchen, ob Menschen überhaupt in der Lage sind, KI-generierte Medien zu identifizieren.

KI-generierte Medien werden mehrheitlich als menschengemacht klassifiziert

Die Ergebnisse der medien- und länderübergreifenden Studie sind erstaunlich: „Wir sind jetzt schon an dem Punkt, an dem es für Menschen schwierig ist – wenn auch noch nicht unmöglich – zu unterscheiden, ob etwas echt oder KI-generiert ist. Und das gilt eben für alle Arten von Medien: Text, Audio und Bild“, erklärt Holz. Die Studienteilnehmer:innen klassifizierten KI-generierte Medien über alle Medienarten und Länder hinweg mehrheitlich als menschengemacht. „Überrascht hat uns, dass es sehr wenige Faktoren gibt, anhand derer man erklären kann, ob Menschen besser im Erkennen von KI-generierten Medien sind oder nicht. Selbst über verschiedene Altersgruppen hinweg und bei Faktoren wie Bildungshintergrund, politischer Einstellung oder Medienkompetenz, sind die Unterschiede nicht sehr signifikant“, so Holz weiter.

Medien-Erkennung mit Abfrage sozio-biografischer Daten kombiniert

Die quantitative Studie wurde als Online-Befragung zwischen Juni 2022 und September 2022 in China, Deutschland und den USA durchgeführt. Per Zufallsprinzip wurden die Befragten einer der drei Mediengruppen „Text“, „Bild“ oder „Audio“ zugeordnet und sahen 50 Prozent reale und 50 Prozent KI-generierte Medien. Darüber hinaus wurden sozio-biografische Daten, das Wissen zu KI-generierten Medien sowie Faktoren wie Medienkompetenz, holistisches Denken, generelles Vertrauen, kognitive Reflexion und politische Orientierung erhoben. Nach der Datenbereinigung blieben 2609 Datensätze übrig (822 USA, 875 Deutschland, 912 China), die in die Auswertung einflossen. Die in der Studie verwendeten KI-generierten Audio- und Text-Dateien wurden von den Forscher:innen selbst generiert, die KI-generierten Bilder übernahmen sie aus einer existierenden Studie. Die Bilder waren fotorealistische Porträts, als Texte wurden Nachrichten gewählt und die Audio-Dateien waren Ausschnitte aus Literatur.

Ausgangspunkte für weitere Forschung

Das Ergebnis der Studie liefert wichtige Take-Aways für die Cybersicherheitsforschung: „Es besteht das Risiko, dass vor allem KI-generierte Texte und Audio-Dateien für Social-Engineering-Angriffe genutzt werden. Denkbar ist, dass die nächste Generation von Phishing-Emails auf mich personalisiert ist und der Text perfekt zu mir passt“, erläutert Schönherr. Abwehrmechanismen für genau solche Angriffsszenarien zu entwickeln, darin sieht sie eine wichtige Aufgabe für die Zukunft. Aber aus der Studie ergeben sich auch weitere Forschungsdesiderata: „Zum einen müssen wir besser verstehen, wie Menschen überhaupt noch KI-generierte Medien unterscheiden können. Wir planen eine Laborstudie, wo Teilnehmer:innen uns erklären sollen, woran sie erkennen, ob etwas KI-generiert ist oder nicht. Zum anderen müssen wir überlegen, wie wir das technisch unterstützen können, etwa durch Verfahren zum automatisierten Fakt-Checking,“ so Schönherr abschließend.

»Wir sind jetzt schon an dem Punkt, an dem es für Menschen schwierig ist – wenn auch noch nicht unmöglich – zu unterscheiden, ob etwas echt oder KI-generiert ist. Und das gilt eben für alle Arten von Medien: Text, Audio und Bild.«

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

© Lea Mosbach

Der Rückgriff auf Anmeldebenachrichtigungen, um Nutzer:innen über ungewöhnliche Login-Aktivitäten auf ihren Accounts zu informieren, gehört zum Standard vieler Online-Dienste. CISPA-Faculty Dr. Maximilian Golla hat sich zusammen mit Kolleg:innen der Ruhr-Universität Bochum und der Leibniz Universität Hannover in einer umfangreichen Studie dem Thema gewidmet. Die Forschenden haben untersucht, wie Nutzer:innen auf die Anmeldebenachrichtigungen reagieren. Das Paper „Understanding Users' Interaction with Login Notifications" haben sie im Mai 2024 auf der ACM Conference on Human Factors in Computing Systems vorgestellt.

Anmeldebenachrichtigungen: Ein wichtiger Sicherheitsfaktor aus Nutzerperspektive

Max Golla

Die Vielzahl von Online-Diensten, die heute ganz selbstverständlich von den Menschen genutzt werden, bringt es mit sich, dass Nutzer:innen fast täglich sogenannte Anmeldebenachrichtigungen in ihrem E-Mail-Postfach finden. „Das ist typischerweise eine E-Mail, die man nach dem Login bei einem Online-Dienst bekommt“, erklärt CISPA-Faculty Dr. Maximilian Golla. „Darin werden Nutzer:innen darüber informiert, dass gerade eine Anmeldung stattgefunden hat. Wenn sie sich tatsächlich eingeloggt haben, können sie die E-Mail ignorieren. Haben sie aber Zweifel, ob sie das tatsächlich waren, wird empfohlen, sein Passwort zu ändern. Um die Entscheidung zu erleichtern, gibt der Dienst in der E-Mail noch weitere Informationen, etwa von wo der Login stattgefunden hat und mit welchem Gerät.“ Die weite Verbreitung der Anmeldebenachrichtigungen im Nutzer:innen-Alltag hat Golla und seine Kolleg:innen dazu motiviert, dem Thema eine eigene Studie zu widmen um herauszufinden, wie nützlich die Benachrichtigungen in der Praxis sind und wie Nutzer:innen darauf reagieren.

Kollision der Daten im Cache

Zu Beginn führten die Forschenden eine vergleichende Untersuchung der Anmeldebenachrichtigungen von 72 verschiedenen Websites durch, darunter so bekannte Dienste wie google.com oder facebook.com. Ziel war herauszufinden, was die konkreten Inhalte der E-Mails sind. „Aus den genutzten Inhalten haben wir die häufigsten und gängigsten Komponenten identifiziert. Dazu gehörten etwa Informationen wie Account-Name, benutzter Browser oder Betriebssystem. Daraus haben wir dann eine generische Anmeldebenachrichtigung ohne Branding erstellt und für unsere Studie verwendet“, erklärt Golla. Damit die Teilnehmer:innen unvoreingenommen reagieren konnten, haben die Forschenden die eigentliche Studie hinter einer anderen Studie verschleiert. Dabei handelte es sich um einen Test zur räumlichen Wahrnehmung aus der Psychologie, für den die Teilnehmer:innen sich auf einer Website registrieren mussten. Per Zufall in zwei Gruppen eingeteilt, bekamen sie nach der Durchführung des Tests entweder direkt eine E-Mail mit

Informationen zu ihrem tatsächlichen Login oder nach ein paar Tagen mit einem vorgetäuschten Loginversuch. Im Anschluss wurden die 229 Teilnehmer:innen aus den USA nach ihren Erfahrungen befragt.

Anmeldebenachrichtigungen helfen, Angriffe zu verhindern

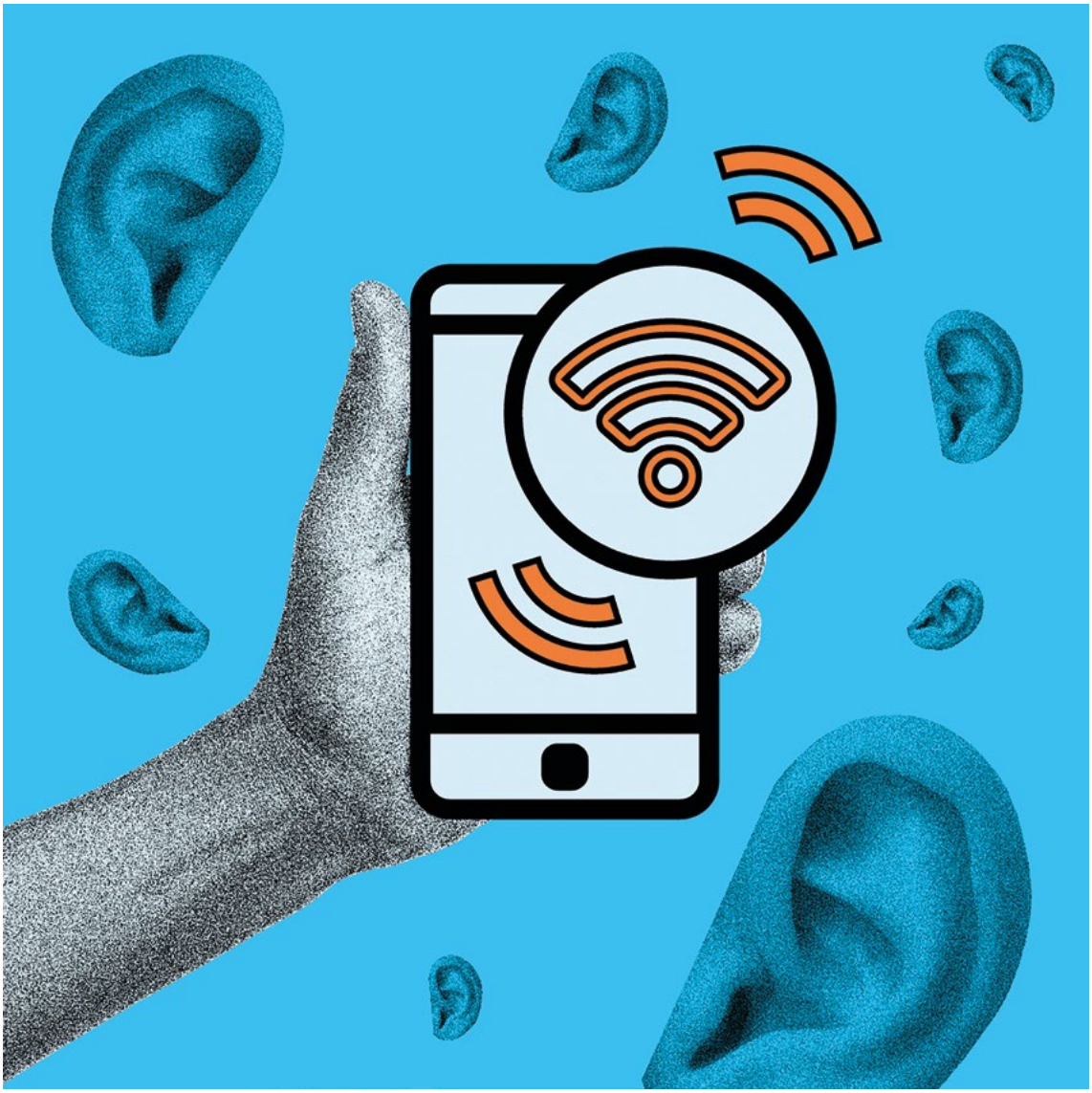
„Ergebnis unserer Messung ist, dass 20 Prozent der Nutzer:innen aus der Gruppe, die über einen potentiell gefährlichen Login informiert wurden, korrekterweise ihr Passwort geändert haben. Aus der Gruppe derjenigen, die nach ihrem tatsächlichen Login eine E-Mail bekommen haben, hat keiner sein Passwort geändert. Aber da bestand ja auch keine Notwendigkeit. Wir schlussfolgern daraus, dass die Leute verstehen, um was es bei den Anmeldebenachrichtigungen geht.“ Wichtig ist Golla, die 20 Prozent in Kontext zu setzen: „Das mag wenig klingen, aber die E-Mails ersetzen ja kein Passwort. Sie sind einfach nur ein weiterer Sicherheitsmechanismus zu allem, was man so kennt. Ein starkes Passwort wehrt bereits die meisten Angriffe ab. Dazu kommen dann die Anmeldebenachrichtigungen, die in 20 Prozent der Fälle, in denen das Passwort versagt, helfen können, Schlimmeres zu verhindern. Wer noch mehr Schutz benötigt, setzt am besten auf eine Zwei-Faktor-Authentifizierung. Aufgrund all dieser Schutzmaßnahmen wird ein Angriff immer aufwendiger.“ Insofern lässt sich schlussfolgern, dass Anmeldebenachrichtigungen eine wertvolle Hilfe sein können, um die eigene Konto-Sicherheit zu erhöhen.

»Für die Forschung bleibt die Frage offen, wie eine ideale E-Mail-Benachrichtigung aussieht.«

Empfehlungen für Unternehmen und die weitere Forschung

Für Golla ist das wichtigste Take-Away der Studie für die Praxis, dass Nutzer:innen sich zwar Anmeldebenachrichtigungen wünschen, jedoch nicht bei jedem normalen Login, sondern nur bei verdächtigen Anmeldungen. Darüber hinaus sollten die Informationen in der E-Mail möglichst konkret sein und auch schon in der Betreffzeile auftauchen. „Auf jeden Fall erwähnt werden sollte der Account-Name, der Standort, die Uhrzeit und das eingesetzte Gerät“, erklärt Golla. Anhand dieser Daten können die Nutzer:innen abgleichen, ob sie sich selbst eingeloggt haben oder nicht. „Für die Forschung bleibt die Frage offen, wie eine ideale E-Mail-Benachrichtigung aussieht“, so der CISPA-Forscher abschließend. „Dafür müsste man verschiedene Varianten durchtesten. Darüber hinaus sind viele Anmeldebenachrichtigungen nicht ausreichend getestet. Insbesondere, wenn man in der deutsch-französischen Grenzregionen lebt und arbeitet, wie wir hier im Saarland, haben die Dienste Probleme mit dem Verarbeiten und Darstellen der Standortinformationen. Des Weiteren sind viele Hilfestellungen, die wir in den E-Mails gefunden haben, wie etwa auf https in der Adresszeile zu achten, fragwürdig und veraltet.“ Es bleibt also noch einiges zu tun in diesem Forschungsfeld.

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



© Alexandra Goweiler

CISPA-Forscher Adrian Dabrowski hat gemeinsam mit Kollegen von SBA Research und der Universität Wien zwei weitreichende Sicherheitslücken im Mobilfunkprotokoll Voice over Wi-Fi (VoWi-Fi), auch WLAN-Calling genannt, aufgedeckt. Durch diese Schwachstellen war die Kommunikationssicherheit von Millionen Mobilfunk-Kund:innen weltweit gefährdet. Entsprechende Updates zum Beheben der Probleme sind inzwischen durchgeführt worden. Eine ausführliche Beschreibung der Sicherheitslücken findet sich im Paper „Diffie-Hellman Picture Show: Key Exchange Stories from Commercial VoWi-Fi Deployments“, das auf dem USENIX Security Symposium 2024 vorgestellt wird.

Kritische Sicherheitslücken in Voice over Wi-Fi aufgedeckt

Adrian Dabrowski

Moderne Smartphones können Telefonverbindungen nicht nur über das Mobilfunknetz, sondern auch über WLAN aufbauen, um so auch an Orten mit schlechter Mobilfunkqualität wie etwa in Tunneln, Kellern oder auf Bahnfahrten Erreichbarkeit zu garantieren. Das sogenannte Wi-Fi- oder WLAN-Calling, das es bereits seit 2016 gibt, bieten mittlerweile fast alle großen Mobilfunknetzbetreiber an und ist bei allen neuen Smartphones voreingestellt. „Der Dienst ist an sich sehr praktisch. Allerdings haben wir bei einer Untersuchung festgestellt, dass der Verbindungsaufbau zwischen Smartphone und Mobilfunknetzen in einigen Fällen nicht sicher erfolgt“, erklärt Adrian Dabrowski.

Schwachstellen auf Seiten der Mobilfunkanbieter

Von der Sicherheitslücke betroffen waren die Dienste von 13 (der insgesamt 275 untersuchten) Mobilfunkanbieter, unter anderem aus Österreich, der Slowakei, Brasilien und Russland und resultierend aus dieser Schwachstelle alleine rund 140 Millionen Kund:innen, deren Kommunikationssicherheit gefährdet war. „Schuld ist eine wichtige Netzwerkkomponente in der LTE- und 5G-Netzarchitektur: Das sogenannte Evolved Packet Data Gateway (ePDG)“, erklärt Dabrowski. Bei WLAN-Calls muss sich ein Smartphone im Kernnetz des Mobilfunkanbieters anmelden. Damit das sicher passieren kann, werden zwischen dem Gerät und den ePDG, das der internetseitige Zugangspunkt zum Mobilfunknetz ist, sogenannte IPsec-Tunnels aufgebaut.

Es handelt sich bei IPSec-Tunnels um eine Art VPN, also ein virtuelles privates Netzwerk, das von außen nicht eingesehen werden kann. IPsec-Tunnels werden in mehreren Schritten aufgebaut. Die Kommunikationssicherheit wird vor allem durch den Austausch von kryptografischen Schlüsseln nach dem sogenannten Internet Key Exchange-Protokoll (IKE) garantiert. „Das sind an sich uralte Verfahren und eigentlich sicher. Außer man macht das mit den Schlüsseln falsch“, erklärt Dabrowski. Denn die müssen privat, also geheim, und zufällig sein. Beides war laut dem Forscher bei den Betreibern nicht der Fall. Zur Überraschung der Forschenden verwendeten die 13 Betreiber statt zufälliger Schlüssel denselben globalen Satz von zehn statischen privaten Schlüsseln. „Jeder, der im Besitz dieser nicht wirklich privaten „privaten Schlüssel“ war, konnte ohne Probleme die Kommunikation

zwischen den Smartphones und den Mobilfunkern mithören“, erklärt Gabriel Gegenhuber, Sicherheitsforscher bei SBA Research und Mitglied in der Forschungsgruppe Security and Privacy der Universität Wien. „Zugriff auf die Schlüssel hat jeder der betroffenen Mobilfunker, der Hersteller, und eventuell die Sicherheitsbehörden jedes dieser Länder.“ Die betroffenen Netze waren alle mit Komponenten des chinesischen Netzwerkausrüsters ZTE bestückt.

Schwachstellen in Smartphone-Chips und bei der Konfiguration auf Smartphones

Damit nicht genug fanden die Forschenden zudem heraus, dass bei vielen neuen Chips (inklusive 5G) des taiwanesischen Herstellers MediaTek, die in einigen Android-Smartphones von Herstellern wie Xiaomi, Oppo, Realme und Vivo stecken, eine weitere Schwachstelle sitzt. „Dieser Chip arbeitet mit der SIM-Karte zusammen um Benutzer:innen bei VoWi-Fi im Mobilfunknetz anzumelden. Wir haben entdeckt, dass es mit gezielten Attacken möglich ist, die Verschlüsselung auf Seite der Smartphones auf die schwächste Variante zu reduzieren“, sagt Dabrowski. Dass im Bereich der Mobilfunksicherheit noch mehr im Argen liegt, zeigten auch ihre Messungen und Analysen der Konfigurationen auf Client- und Serverseite vieler anderer Hersteller, darunter Google, Apple, Samsung und Xiaomi. „In bis zu 80 Prozent der Fälle, in denen wir einen Verbindungsaufbau simuliert haben, haben wir festgestellt, dass veraltete kryptografische Verfahren zum Einsatz kommen, die nicht mehr dem Standard entsprechen“, sagt Dabrowski.

Schaden ist unklar, Updates sind eingespielt

Wie viele Nutzer:innen weltweit tatsächlich von Angriffen betroffen waren oder durch die Schwachstelle auf Seiten der Mobilfunker:innen abgehört wurden, können die Forschenden nicht sagen. Sie haben allerdings die weltweite Industriellenvereinigung der Mobilfunkanbieter (GSMA) sowie die betreffenden Provider und Firmen informiert und Gelegenheit zur Entwicklung von Updates gegeben. Diese wurden inzwischen auch durchgeführt. Erst nachdem diese vertrauensvolle Offenlegung (responsible disclosure) passiert ist, veröffentlichen sie ihre Arbeit auf dem USENIX Security Symposium 2024 und stellen damit ihre Erkenntnisse auch anderen Forschenden zur Verfügung.

»Wir haben entdeckt, dass es mit gezielten Attacken möglich ist, die Verschlüsselung auf Seite der Smartphones auf die schwächste Variante zu reduzieren.«

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

Forscher: ***Adrian Dabrowski***
Autorin: ***Annabelle Theobald***

Veröffentlichung
30.07.2024

© Janine Wichmann-Paulus

Eine neu entdeckte Sicherheitslücke namens GhostWrite kompromittiert die Integrität der RISC-V-CPU „XuanTie C910“ des Anbieters T-Head. Sie gibt Angreifern vollen Lese- und Schreibzugriff auf den physikalischen Speicher der C910. GhostWrite umgeht zudem den virtuellen Speicher sowie alle Caches und ist unsichtbar in Performance Countern. Cloud Services, deren Server eine C910-CPU verwenden, sind ebenfalls von GhostWrite betroffen. Die Schwachstelle kann nur durch das Deaktivieren der Vector Extension behoben werden. Die ebenfalls von T-Head hergestellten RISC-V-CPUs „XuanTie C906“ und „XuanTie C908“ sind von jeweils einer weiteren Schwachstelle betroffen. Im August 2024 präsentiert CISPA-Forscher Fabian Thomas die Schwachstellen in seinem Vortrag „Arbitrary Data Manipulation and Leakage with CPU Zero-Day Bugs on RISC-V“ auf der „Black Hat USA“-Konferenz in Las Vegas.

Sicherheitslücke „GhostWrite“ untergräbt Integrität der RISC-V-CPU „XuanTie C910“ von T-Head

Fabian Thomas

Mit einer neuen Fuzzing-Methode für RISC-V-CPUs hat CISPA-Forscher Fabian Thomas aus der Forschungsgruppe von CISPA-Faculty Dr. Michael Schwarz architekturelle Schwachstellen in den T-Head-CPUs XuanTie C906, C908 und C910 entdeckt. Die bedeutendste dieser drei Schwachstellen trägt den Namen GhostWrite und betrifft die XuanTie C910. GhostWrite ermöglicht unbefugten Nutzenden direkten Zugriff auf das DRAM (Dynamic Random-Access Memory); so können Daten direkt im physikalischen Speicher geändert werden. Außerdem kann sowohl mit der Festplatte als auch mit Peripheriegeräten wie z.B. Netzwerkkarten und Grafikkarten interagiert werden. Neben GhostWrite hat Thomas auch zwei sogenannte „halt-and-catch-fire“ CPU-Schwachstellen entdeckt, die für Denial-of-Service-Angriffe ausgenutzt werden können.

RISC-V: Jung, offen, flexibel und potentiell problematisch

Die wachsende Verbreitung von RISC-V-CPUs hat das Forschungsinteresse von Thomas und Schwarz geweckt. RISC-V ist eine relativ junge, offene Befehlssatzarchitektur, die es neuen CPU-Herstellern ermöglicht hat, in den Markt einzutreten. Allgemein gesprochen bestimmt eine Befehlssatzarchitektur, wie Software und CPU miteinander interagieren. Sie legt fest, auf welche Befehle die CPU reagieren darf. „RISC-V ist eine sehr flexible Befehlssatzarchitektur, die es den Herstellern erlaubt, ihre eigenen Erweiterungen zu implementieren. Das ist problematisch, weil es kein zentrales Register für diese individualisierten Erweiterungen gibt. Es kann also passieren, dass verschiedene CPUs dieselbe Kodierung für unterschiedliche Befehle verwenden“, sagt Thomas. „Das bedeutet, dass Software, die für die RISC-V-CPU eines speziellen Herstellers entwickelt wurde, ein abweichendes Verhalten hervorrufen kann, wenn sie auf der RISC-V-CPU eines anderen Herstellers verwendet wird. Diese Varianz im

Verhalten von CPUs kann Probleme verursachen.“ RISC-V-CPUs finden sich bis dato in einer geringen Zahl von Hardwarecores, die etwa in Laptops, Smartphones und Servern verbaut werden. Aktuell erhältlich sind fünf verbraucherorientierte RISC-V-CPUs.

»RISC-V ist eine sehr flexible Befehlssatzarchitektur, die es den Herstellern erlaubt, ihre eigenen Erweiterungen zu implementieren. Das ist problematisch, weil es kein zentrales Register für diese individualisierten Erweiterungen gibt.«

RISCVuzz: Differenzielle Fuzzing-Methode für RISC-V-CPUs

Thomas und Schwarz haben die Heterogenität von RISC-V-CPUs und deren individuellen Erweiterungen dazu genutzt, architekturelle Schwachstellen an RISC-V-Anwendungen aufzudecken. Mit RISCVuzz haben sie eine neue differentielle Fuzzing-Methode für CPUs entwickelt und sie auf alle fünf am Markt erhältlichen RISC-V-CPUs angewandt. „Wir sind davon ausgegangen,

dass alle CPUs dieselbe Reaktion zeigen sollten, wenn sie zuvor denselben Befehl erhalten haben. Jedes Mal, wenn die Reaktion einer CPU von der Reaktion aller anderen CPUs abwich, haben wir sie genauer auf Schwachstellen hin untersucht“, erklärt Schwarz die Logik hinter RISC-Vuzz. „Anders ausgedrückt: Wenn vier von fünf Hotelsafes verschlossen bleiben, wenn man ‚0000‘ eingibt, der fünfte aber plötzlich aufspringt, dann hat man Grund zur Annahme, dass mit diesem fünften etwas nicht stimmt.“

Offenlegung und Gegenmaßnahmen

Im Februar 2024 meldeten Thomas and Schwarz ihre Forschungsergebnisse an T-Head, ein Tochterunternehmen von Alibaba, und im April 2024 an den Cloud-Computing-Anbieter Scaleway, der kurz zuvor begonnen hatte, die C910-CPU in der Cloud einzusetzen. Keine der drei Schwachstellen können derzeit mit Updates behoben werden. GhostWrite, ebenso wie die Sicherheitslücke der C908, kann durch das Deaktivieren der Vector Extension geschlossen werden. Allerdings werden damit auch Kernfunktionalitäten der CPUs ausgeschaltet. Für die Schwachstelle der C906 gibt es derzeit keine umsetzbare Lösung. „CPUs werden mit Code geschrieben. Wenn wir Schwachstellen finden, müssen wir sie unbedingt offenlegen, um zu verhindern, dass diese Bugs sich in anderen CPU-Entwicklungen fortsetzen“, sagt Schwarz.

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

Forscher: ***Fabian Thomas***
Autorin: ***Eva Michely***

Veröffentlichung
07.08.2024

© Chiara Schwarz

Eine weit verbreitete Praxis unter Software-Entwickler:innen ist es, sogenannte Codeschnipsel von der Plattform Stack Overflow zu verwenden. Eine Studie des CISPA-Forschers Alfusainey Jallow zeigt jetzt auf, dass damit langfristig Sicherheitsrisiken einhergehen können. Diese liegen unter anderem darin begründet, dass sicherheitsrelevante Updates der Codeschnipsel oft nicht den Weg in die Software finden, in der sie zum Einsatz kommen. Die Studienergebnisse publizierte Jallow im Paper „Measuring the Effects of Stack Overflow Code Snippet Evolution on Open-Source Software Security“ beim IEEE Symposium on Security and Privacy 2024 (S&P).

Veraltete Codeschnipsel von Stack Overflow gefährden Software-sicherheit

Alfusainey Jallow

Im Programmier-Alltag stoßen Software-Entwickler:innen immer wieder auf Probleme, für die sie eine schnelle Lösung suchen. „Frühere Studien haben gezeigt, dass die prominenteste Plattform, die Entwickler:innen konsultieren, nicht Lehrbücher sind, sondern Stack Overflow“, erklärt CISPA-Forscher Alfusainey Jallow. Stack Overflow gehört zum Netzwerk Stack Exchange und ist eine populäre Onlineplattform für Programmierer:innen und Entwickler:innen, auf der sie Antworten auf verschiedene Programmierthemen und -probleme finden. „Die Beliebtheit von Stack Overflow liegt darin, dass es funktionale Codeschnipsel anbietet. Ein Codeschnipsel ist eine Verbindung von Code in einer bestimmten Programmiersprache, die ein bestimmtes Problem löst. Man kann ihn meist mit wenigen oder gar keinen Änderungen direkt im eigenen Projekt verwenden“, so Jallow weiter.

Suche nach veralteten Codeschnipseln in GitHub-Projekten

Aus der Forschung ist bereits bekannt, dass es bei den Codeschnipseln auf Stack Overflow auch sicherheitskritische Varianten gibt. Ob der von Stack Overflow kopierte Code sicher ist, lässt sich etwa mit Hilfe von Browser-Plugins überprüfen. Darüber hinaus ist auch bekannt, dass die Codeschnipsel nicht statisch sind, sondern immer weiterentwickelt werden. „Bisher nicht untersucht wurde jedoch die Frage, ob Entwickler:innen, die Codeschnipsel von Stack Overflow in ihre Software kopieren, diese auch updaten, wenn es Veränderungen an den Codeschnipseln auf Stack Overflow gibt“, so Jallow. Um dies herauszufinden, haben sich Jallow und seine Kollegen Open-Software-Projekte auf der populären Plattform GitHub angeschaut. „GitHub wird verwendet, um Code zu hosten und mit anderen an einem bestimmten Softwareprojekt zusammenzuarbeiten“, erklärt der CISPA-Forscher. Zur Durchführung entwickelte er ein mehrstufiges Verfahren, um veraltete Codeschnipsel-Versionen in GitHub-Projekten zu entdecken und zu überprüfen, ob bei diesen Codeschnipseln sicherheitsrelevante Updates durchgeführt wurden oder nicht.

Fehlende Updates von Codeschnipseln führen zu Sicherheitslücken

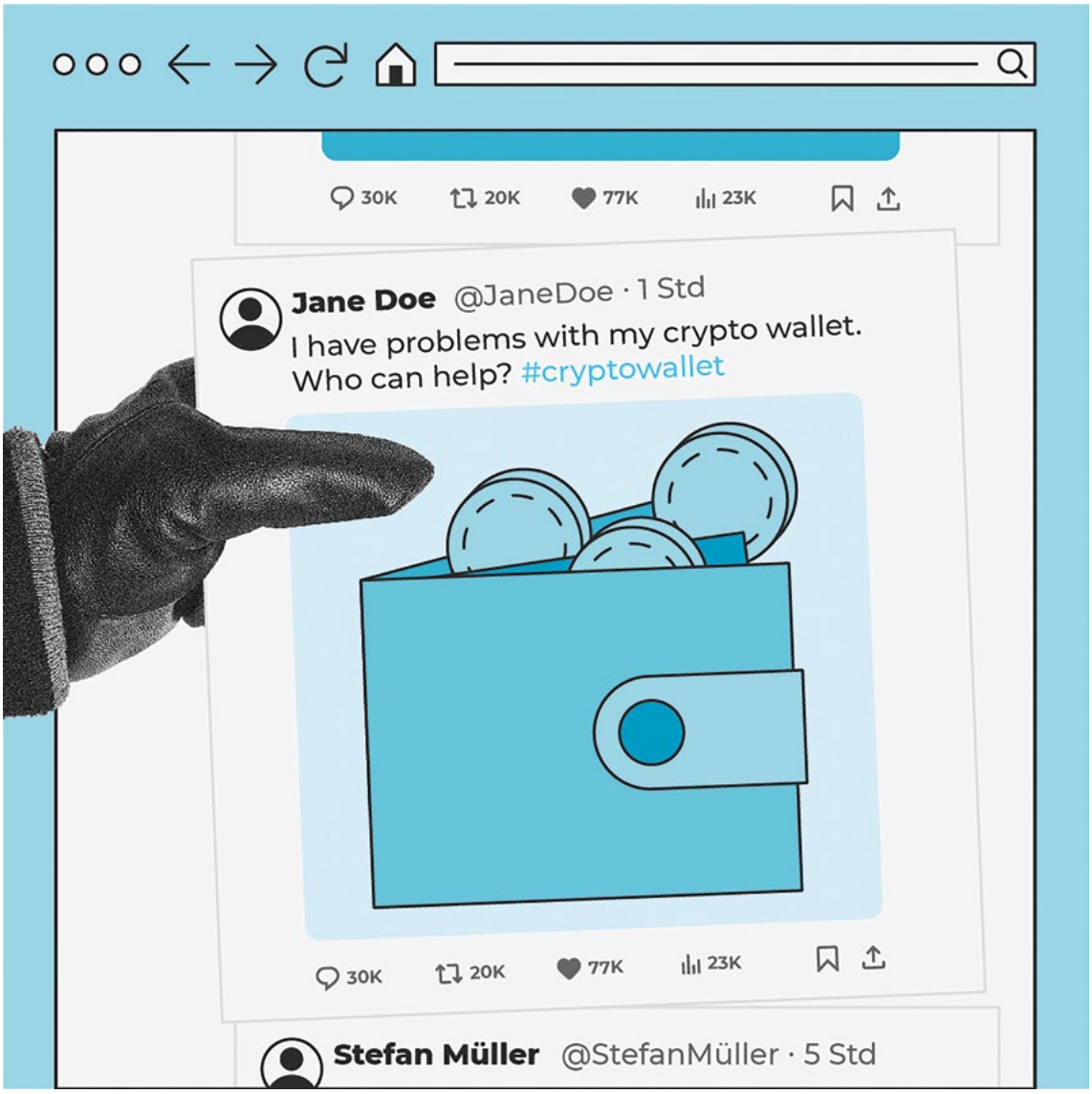
In ihrer Untersuchung von knapp 11.500 GitHub-Projekten kamen Jallow und seine Kollegen zu dem Ergebnis, dass jeder zweite wiederverwendete Codeschnipsel veraltet ist, unabhängig von der verwendeten Programmiersprache. Sie fanden keine Hinweise darauf, dass die GitHub-Entwickler:innen Updates der Codeschnipsel auf Stack Overflow in ihre Projekte übernommen haben. Die mit den Ergebnissen einhergehenden Gefahren liegen laut Jallow in den fast unbegrenzten Verbreitungszirkeln von Software. „Wenn man einen Codeschnipsel aus Stack Overflow kopiert, der die Privatsphäre des Nutzers verletzen kann, und jemand die App auf seinem Handy installiert hat das eine Menge gesellschaftlicher Auswirkungen. Wenn die Verletzung der Privatsphäre von einem Codeschnipsel von Stack Overflow ausgeht, ist das wirklich ein großes Problem“, ist er überzeugt. Jallow und seine Kollegen ziehen aus ihren Ergebnissen das Fazit, dass „die Entwickler:innen die von Stack Overflow kopierten Snippets nicht auf Änderungen überprüfen, oder sich nicht bewusst sind, dass der von ihnen wiederverwendete Code auf Stack Overflow diskutiert und aktualisiert oder gefixt wird.“

Fehlendes Tool ist ein Auftrag für die Zukunft

Für Entwickler:innen hat Jallow im Moment vor allem eine Empfehlung: „Seid vorsichtig, wenn ihr einen Codeschnipsel von Stack Overflow verwendet. Und wenn ihr welche verwendet, findet einen Weg, um euch diesen zu merken.“ Da es bisher noch kein automatisiertes Tool gibt, bleibt Entwickler:innen nur, selbst immer wieder zu überprüfen, ob es zu den von ihnen verwendeten Codeschnipseln ein Update auf Stack Overflow gibt. Genau das spornt Jallow an, wie er im Gespräch erzählt: „Um diese Lücke zu schließen, würde ich gerne ein Tool entwickeln. Wenn das nicht mehr während meiner Doktorarbeit klappt, dann in einer späteren Karrierephase. Das CISPA hat dieses wirklich tolle Ökosystem, in dem Forschungsergebnisse in die Industrie transportiert werden und Ausgründungen und Startups gefördert werden. Den großen Vorteil, dass es dieses Angebot am CISPA gibt, würde ich gerne nutzen.“

»Seid vorsichtig, wenn ihr einen Codeschnipsel von Stack Overflow verwendet. Und wenn ihr welche verwendet, findet einen Weg, um euch diesen zu merken.«

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



Die zunehmende Beliebtheit von Kryptowährungen hat die sozialen Medien zu einem zentralen Ort gemacht, an dem Nutzer:innen nach Hilfe suchen, wenn sie Probleme mit ihrer Krypto-Wallet oder ihrem privaten Schlüssel haben. Diesen Umstand machen sich Betrüger:innen zunutze, um mit vorgespielten Hilfsangeboten Kasse zu machen oder um zu versuchen, Zugang zu den Wallets oder den Schlüsseln zu erhalten. CISPA-Forscher Dr. Bhupendra Acharya hat die erste breit angelegte Studie darüber vorgelegt, wie die Betrugsmaschen ablaufen und eine End-to-End-Analyse der Betrugsoperationen auf X (ehemals Twitter) erstellt. Die Ergebnisse hat er auf dem IEEE Symposium on Security and Privacy 2024 (S&P) vorgestellt.

Die Suche nach Hilfe in sozialen Medien bei Problemen mit Krypto-Wallets kann Betrüger anlocken

Bhupendra Acharya

Aufgrund ihres dezentralen Charakters und der Anonymität, die sie ihren Nutzer:innen gewähren, gewinnen Kryptowährungen wie Bitcoin oder Ethereum zunehmend an Akzeptanz. Um Kryptowährungen zu verwalten und zu verkaufen, brauchen die Nutzer:innen sogenannte Krypto-Wallets, eine Art digitale Geldbörse für Kryptowährungen. Die bekanntesten Wallets sind Metamask, Coinbase und Trust. Um auf die Wallets zugreifen zu können, ist ein privater Schlüssel nötig. Alle, die Zugang zu den privaten Schlüsseln haben, können die Krypto-Wallets verwalten oder darauf zugreifen. Bei Verlust des privaten Schlüssels ist kein Zugriff auf die Krypto-Wallets mehr möglich.

„Wir haben beobachtet, dass in dem Maße, wie Kryptowährungen immer beliebter geworden sind, die Menschen sich darüber auch in den sozialen Medien austauschen. Dies umfasst auch technische Probleme, etwa wenn kein Zugriff auf die Wallet möglich, der private Schlüssel verloren ist oder ähnliches. Das lockt Betrüger:innen an, die sich als offizieller Technik-Support ausgeben“, erklärt CISPA-Forscher Bhupendra Acharya. Viele Menschen ziehen es vor, in einer Chat-Gruppe oder über einen Tweet Hilfe zu suchen, anstatt sich direkt an die offiziellen Support-Kanäle der jeweiligen Krypto-Wallet-Anbieter zu wenden. „Mit unserer Studie wollen wir aufdecken, wie genau sich Betrüger:innen die sozialen Medien zunutze machen, um mithilfe von fingierten technischen Supportangeboten Zugriff auf Krypto-Wallets zu erhalten“, so Acharya.

Den Betrüger:innen mit Honey Tweet auf der Spur

Um zu untersuchen, wie der Support-Betrug in den sozialen Medien konkret abläuft, haben Acharya und seine Kolleg:innen ein Tool namens HoneyTweet entwickelt. „HoneyTweet verschickt automatisiert einzigartige Tweets mit Schlüsselwörtern für technische Supportanfragen, um damit die Betrüger:innen in die Falle zu locken“, erklärt Acharya. „Betrüger:innen, die gefälschten Support anbieten, werden dann über das Tool kontak-

tiert, um die für den Betrug genutzten Zahlungsmethoden oder den Modus Operandi der Betrüger:innen zu erkennen“, fährt er fort. Teil des Modus Operandi ist das Unterbreiten verschiedener Scheinangebote wie etwa des Software-Tools „Zeus“, mit dem gegen Zahlung angeblich der Zugriff auf die Brieftasche wiederhergestellt werden kann. Häufig werden die Nutzer:innen während des Vorgangs auch auf externe Kommunikationskanäle umgeleitet, um zu vermeiden, dass der Betrug auf der ursprünglichen Plattform entdeckt wird. Mit Hilfe von HoneyTweet haben Acharya und seine Kolleg:innen in drei Monaten über 9.000 Betrüger:innen angelockt und ihre Spuren auf sechs Social-Media-Plattformen verfolgt, sowie auf PayPal- und Kryptowährungsadressen, die als Zahlungsmittel von den Betrüger:innen angegeben wurden.

Die wichtigsten Ergebnisse der Studie

Acharya und seine Kolleg:innen konnten mit ihrer Studie nachweisen, dass Support-Betrug für Krypto-Wallets ein weit verbreitetes Phänomen in sozialen Medien wie X ist. „Wir haben festgestellt, dass die sozialen Medien noch viel Arbeit vor sich haben, um diese Betrügereien zu beenden“, so Acharya. „Und wir fanden auch heraus, dass Betrüger:innen oft mehrere Social-Media-Plattformen für ihre Betrugsversuche nutzen. Zusätzlich zum Austausch auf der Plattform X bitten die Betrüger:innen darum, über Direktnachrichten auf Instagram, Facebook, Telegram, WhatsApp oder anderen Plattformen kontaktiert zu werden.“ Im Grunde genommen arbeiten sie in einer Art Betrugskette, die mehrere soziale Medien miteinander verbindet.

Während des Betrugsprozesses versuchen die Betrüger:innen zunächst, Vertrauen aufzubauen. Später versuchen sie dann ihr Gegenüber gezielt zu manipulieren. Vermeintlich um technische Hilfe leisten zu können, fordern sie ihre Opfer auf, ihre privaten Schlüssel zur Wallet preiszugeben. Eine andere Masche ist es, sich für die angebliche Hilfeleistung bezahlen zu lassen. Das Problem gelöst, wurde dabei natürlich nicht. Durch die Zusammenarbeit mit PayPal und die Weitergabe der entdeckten Betrugskonten an den Zahlungsdienstleister waren die Forscher in der Lage, die finanziellen Auswirkungen des Betrugs zu bestätigen.

Take-Aways für Unternehmen und Nutzer:innen

„Es gibt zwei Gruppen, für die unsere Ergebnisse interessant sind“, erzählt Acharya. „Die erste sind beteiligte Dienste wie zum Beispiel die Anbieter der Krypto-Wallets. Sie sollten alle Aktivitäten überwachen, die direkt mit ihren Markennamen verbunden sind, und einschreiten, wenn Betrüger:innen versuchen, in ihrem Namen zu kommunizieren. Die zweite Gruppe sind soziale Medien wie X, Instagram, Facebook oder Telegram. Es ist wichtig,

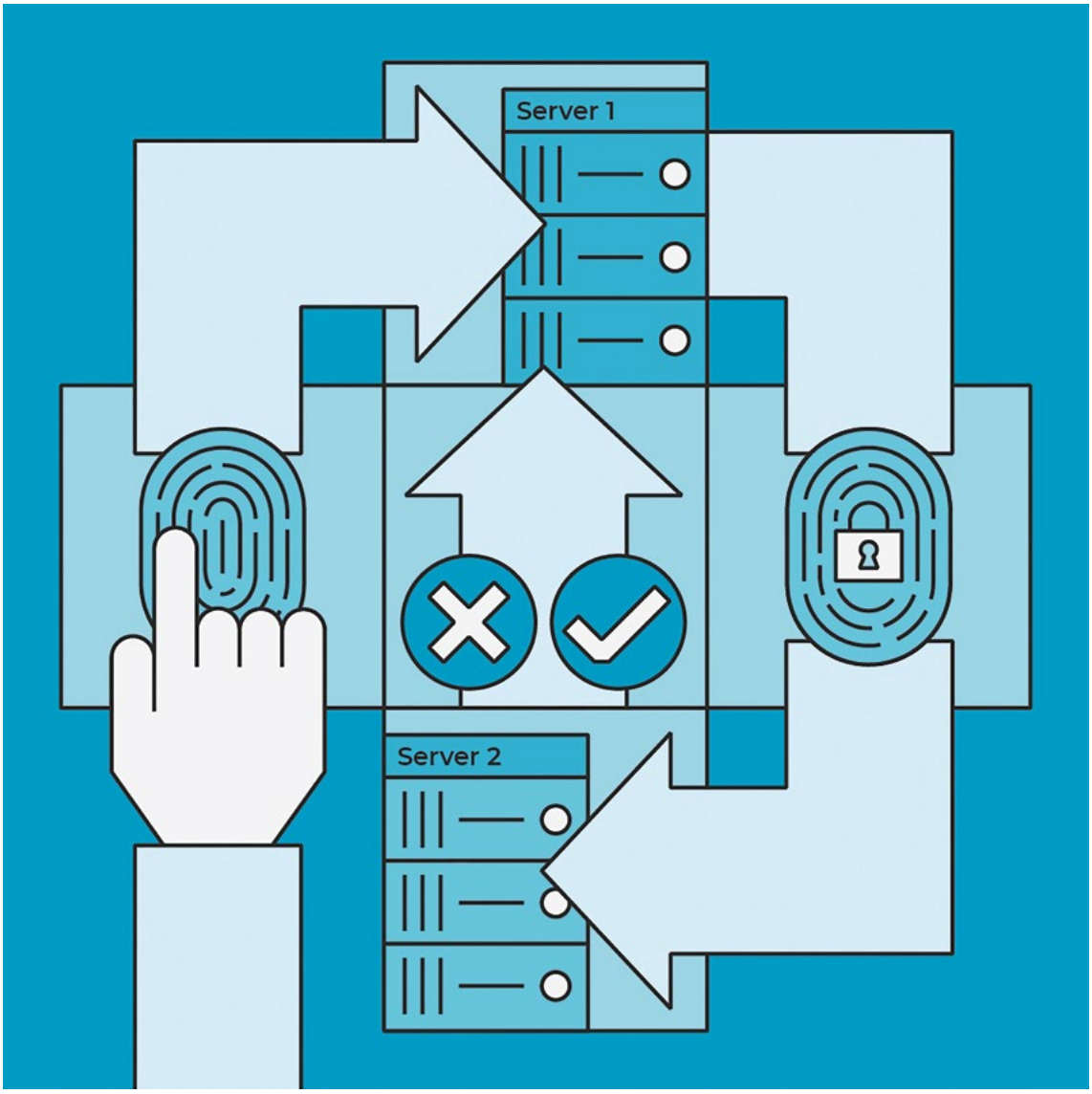
dass diese gemeinsam überwachen, was in den Betrugsketten vor sich geht, da der Betrug nicht unbedingt auf der Plattform stattfindet, auf der der Chat begonnen hat. Der endgültige Betrug kann am Ende der Kette, das heißt auf einer anderen Plattform, stattfinden. Um diese Ketten zu bekämpfen, ist die Zusammenarbeit zwischen den Diensten immens wichtig."

Aber auch Nutzer:innen von Krypto-Wallets können aktiv werden. Acharya empfiehlt, sicherzugehen, immer nur mit den offiziellen Anbieter:innen von Krypto-Wallets in Kontakt zu treten und sehr vorsichtig mit allen inoffiziellen Kanälen zu sein. Und auf keinen Fall sollten Informationen über Google-Forms oder ähnliche Plattformen geteilt werden. „Krypto-Wallets oder mit diesen verbundene offizielle Social-Media-Accounts fragen die Nutzer:innen nie nach ihren privaten Schlüsseln", so der CISPA-Forscher abschließend.

Die Zukunft gehört den (sicheren) Digitalwährungen

Acharya, der sich im Gespräch als großer Fan von Digitalwährungen und Kryptowährungsnutzer outet, sieht viel Potential in Kryptowährungen. „Ich glaube, dass digitale Währungen wie Kryptowährungen die nächste Generation von Zahlungsmitteln sind und bestehende Währungen in Zukunft ersetzen werden", ist er überzeugt. „Was wir jedoch brauchen, ist ein System, das sicher genug ist, um eine digitale Währung zu schaffen, beziehungsweise zu betreiben." Dafür will er als Forscher auch in Zukunft einen Beitrag leisten. „Ein Projekt ist, dass wir ChatGPT einsetzen, um mit den Betrüger:innen auf der Grundlage von HoneyTweet zu chatten. Dabei konzentrieren wir uns auch auf andere Betrugskategorien, wie etwa die vermeintliche Kontowiederherstellung", erklärt der CISPA-Forscher. „In einer weiteren Folgestudie werden wir eine auf Deepfake basierende Methode verwenden, um mit den Betrüger:innen über Zoom-Video und Telefon zu kommunizieren, um weitere Betrugsmechanismen zu identifizieren." Es bleibt also spannend, was noch alles an Betrugsmaschen im Bereich Kryptowährungen von Acharya und seinen Kolleg:innen aufgedeckt wird.

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



Millionen von Menschen weltweit sind auf humanitäre Hilfe angewiesen. Eine Herausforderung bei der Verteilung ist, dass die Ressourcen fast immer sehr knapp sind. Aus diesem Grund wollen humanitäre Organisationen sicherstellen, dass Menschen sich nur einmal registrieren können. CISPA-Faculty Dr. Wouter Lueks und seine Kolleg:innen vom EPFL in Lausanne haben jetzt in Kooperation mit dem Internationalen Komitee des Roten Kreuzes (IKRK) ein Tool entwickelt, das es Organisationen ermöglicht, diese Herausforderung durch die sichere Nutzung biometrischer Daten zu bewältigen. Das Paper „Janus: Safe Biometric Deduplication for Humanitarian Aid Distribution“ wurde auf dem IEEE Symposium on Security and Privacy 2024 (S&P) vorgestellt.

JANUS: Vermeidung von Mehrfachregistrierungen in der humanitären Hilfe dank Biometrie

Wouter Lueks

Das Risiko, dass sich Menschen mehrfach für humanitäre Hilfsprogramme registrieren, schwebt wie ein Damoklesschwert über den Programmen. „Hilfsorganisationen versuchen, so vielen Menschen wie möglich zu helfen“, erklärt CISPA-Faculty Dr. Wouter Lueks. „Und bei der Verwirklichung dieses Ziels wollen sie sicherstellen, dass sie Empfänger:innen nicht zweimal Hilfe gewähren. Denn dann kann jemand anderes keine Hilfe erhalten.“ Lueks suchte nach einem Ansatz, um die doppelte Ausgabe humanitärer Hilfe zu verhindern. Da in Regionen mit humanitären Krisen der Rückgriff auf Ausweisdokumente meist nicht möglich oder mit Risiken verbunden ist, sind biometrische Daten das Mittel der Wahl. „Kern der von uns designten Lösung ist, dass wir diese Daten nur für einen Zweck verwenden wollen: Wir wollen in der Lage sein, zu entscheiden, ob die biometrischen Daten der Person, die wir vor uns haben, bereits registriert wurden“, erklärt Lueks.

Hashfunktionen als Sicherheitsgarant

Aber wie läuft das Verfahren nun konkret ab? „Wenn eine Person zu einer Registrierungsstelle kommt und um Registrierung bittet, werden biometrische Daten von ihr genommen, zum Beispiel ein Fingerabdruck“, erklärt Lueks. Dafür braucht es ein an einen Computer angeschlossenes Lesegerät und eine Internetverbindung. „Dann wird ein so genanntes kryptografisches Protokoll zwischen dem Computer in der Registrierungsstation und einem zweiten Computer an einem anderen Ort ausgeführt, in unserem Fall in der IKRK-Zentrale in Genf“, fährt Lueks fort. „Das Ergebnis dieses Protokolls ist eine Ja-Nein-Entscheidung. Ja, ich habe die biometrischen Daten in der Datenbank gefunden oder Nein, ich habe sie nicht gefunden. In diesem Fall können die Daten des Empfängers hinzugefügt werden“. Auf dem lokalen Computer werden die Daten nur für den Moment der Datenaufnahme gespeichert und dann wieder gelöscht.

Sicherheit des Verfahrens

„Die Tatsache, dass biometrische Daten nicht veränderbar sind, macht ihre Speicherung in Datenbanken jedoch sehr riskant“, so der CISPA-Forscher. „Sie hinterlassen Spuren von Informationen darüber, dass bestimmte Personen hier waren, dass sie sich registriert haben und so weiter. Wir haben in der Vergangenheit etwa nach dem Abzug der USA aus Afghanistan gesehen, dass die einfache Tatsache, dass Menschen sich für ein bestimmtes Programm angemeldet haben, sehr weitreichende Folgen für ihr zukünftiges Leben haben und ihre Sicherheit bedrohen kann.“ Aus diesem Grund haben Lueks und seine Kolleg:innen verschiedene Sicherheitsmechanismen in ihr Verfahren eingebaut. „Entscheidend ist, dass die beiden Computer zusammenarbeiten müssen, um diese Ja/Nein-Entscheidung zu treffen“, erklärt Lueks. „Wenn einer der beiden Computer die Kooperation verweigert, oder konkreter gesagt, wenn jemand in Genf beschließt, das System abzuschalten, werden keine weiteren Informationen aus dem System herausgegeben.“ Nicht einmal der physische Zugriff auf einen der beiden Computer wird die biometrischen Daten der Hilfsempfänger:innen preisgeben: Das System ist so konzipiert, dass der Zugriff auf die Daten verhindert wird.

»Die Tatsache, dass biometrische Daten nicht veränderbar sind, macht ihre Speicherung in Datenbanken jedoch sehr riskant.«

Einbettung der Registrierung in die Verteilung humanitärer Hilfe

Das Verfahren, das Lueks und seine Kolleg:innen in ihrem aktuellen Paper vorstellen, zielt auf den Registrierungsprozess ab. Dieser ist jedoch nur ein Teil des komplexen Prozesses zur Verteilung humanitärer Hilfe. Ein weiterer wichtiger Teil ist die tatsächliche Ausgabe von Gütern. Auch hier gilt es zu verhindern, dass Menschen mehr als einmal Hilfe empfangen. Um dies zu verhindern, entwickelten die Forscher:innen bereits im vergangenen Jahr ein Token-basiertes System zur Verteilung humanitärer Hilfe. Konkret würde dies bedeuten, dass Hilfe-Empfänger:innen nach der erfolgreichen Registrierung einen Token etwa in Form einer Smart-Card bekommen, mit der sie die ihnen zustehenden Güter abholen können. Das Design des Tokens verhindert dabei, das pro Ausgaberunde mehr als eine Ausgabe pro Person erfolgen kann. Obwohl die damalige Lösung sich auf Haushalte, nicht auf Einzelpersonen bezog, ließe sich der Ansatz problemlos mit dem jetzt entwickelten Verfahren kombinieren. Für die Zukunft kann Lueks sich vorstellen, einen Prototyp für die Anwendung beider Verfahren zu entwickeln. Seitens seiner Kooperationspartner vom IKRK besteht daran auf jeden Fall Interesse.

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 einer im Sommer beim USENIX Security Symposium 2024 vorgestellten Studie mit dem Titel „Prompt Stealing Attacks Against Text-to-Image Generation Models“ weist CISPA-Forscherin Xinyue Shen nach, dass Reverse Engineering auch bei KI-generierten Bildern erfolgreich sein kann. Mit Hilfe eines von ihr entwickelten Tools namens PromptStealer gelang es Shen und ihren Kolleg:innen, aus KI-generierten Bildern den ursprünglichen Prompt zu extrahieren. Damit deckt sie ein neues Angriffsszenario für Text-zu-Bild-Generatoren auf und liefert mit PromptShield zugleich auch einen Schutzmechanismus mit.

Prompt Stealing: CISPA-Forscherin entdeckt neues Angriffsszenario für Text-zu-Bild-Generatoren

Xinyue Shen

Aufgrund des immensens Qualitätssprung der generierten Ergebnisse erfreuen sich KI-Bildgeneratoren zuletzt großer Beliebtheit. Die meisten Bildgeneratoren wie Stable Diffussion oder DALL-E sind Text-zu-Bild-Generatoren. Ein entscheidender Faktor, um ein perfektes Bild generieren zu können, sind präzise Texteingaben, die sogenannten Prompts. Da dafür ein sehr spezialisiertes Wissen erforderlich ist, hat sich mit den Prompt Engineers ein eigener Berufszweig entwickelt. Bei KI-Bildern gibt es jedoch eine weitere Besonderheit, erklärt CISPA-Forscherin Xinyue Shen: „Um ein Bild in einem bestimmten Stil zu bekommen, braucht es neben einer präzisen Beschreibung noch einen sogenannten Modifier, der den Bildstil beschreibt. Ohne diesen sind die Ergebnisse eher willkürlich“.

Der Begriff „unsichere Bilder“

Aber noch etwas anderes erregte Shens Aufmerksamkeit: „Mir fiel auf, dass aufgrund der Bedeutung von Prompts ein eigener Markt hierfür entstanden ist“, so Shen. „Auf Plattformen wie Promptbase verkaufen Prompt-Engineers ihre Texteingaben zur Generierung von KI-Bildern.“ Interessent:innen können mit wenigen Klicks und wenigen Euro-Investition einen Prompt für ein bestimmtes Bild erwerben und ersparen sich damit zeitraubendes Ausprobieren. Aber mit neuen digitalen Marktplätzen sind oft auch neue Angriffsszenarien verbunden. „Wir wollten herausfinden, ob es eine Möglichkeit gibt, die Prompts zu bekommen, ohne dafür zu bezahlen“, erzählt Shen. „Dieses Szenario haben wir Prompt Stealing genannt“. Die Forscher verstehen darunter die Extraktion des Prompts aus einem KI-generierten Bild ohne Einwilligung des Prompt Engineers, was Plattformen wie Promptbase die ökonomische Grundlage entziehen würde.

»Um ein Bild in einem bestimmten Stil zu bekommen, braucht es neben einer präzisen Beschreibung noch einen sogenannten Modifier, der den Bildstil beschreibt. Ohne diesen sind die Ergebnisse eher willkürlich.«

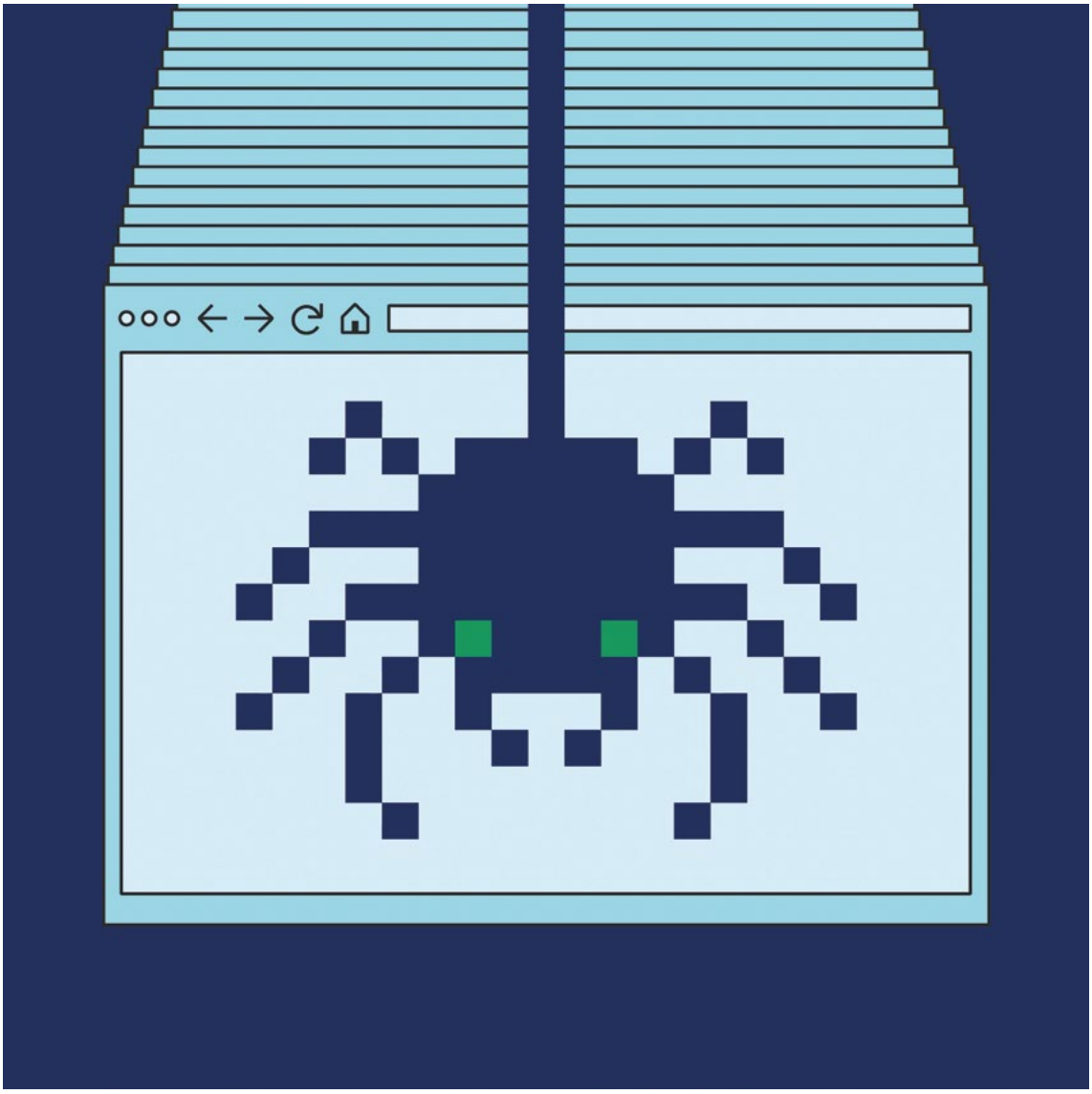
Ein neues Tool namens PromptStealer

Da erste Versuche, den Prompt über einen Text-Decoder zu generieren, nicht zu den gewünschten Ergebnissen führten, machte sich Shen an die Entwicklung eines eigenen Tools. Grundlegend war ihre Erkenntnis, dass für einen präzisen Prompt sowohl die Bildbeschreibung als auch ein spezifischer Modifier entscheidend sind. „Wir haben der neuen Methode den Namen PromptStealer gegeben“, erzählt Shen. „Da sowohl das Motiv als auch die Modifikatoren wichtig sind, lösen wir das Problem in unserem Tool Schritt für Schritt. Zunächst verwenden wir einen Motivgenerator, um das im Bild dargestellte Motiv zu erhalten. Dann verwenden wir einen Detektor für die Modifier, um diese ebenfalls präzise vorherzusagen.“ Über eine quantitative und qualitative Analyse konnte die CISPA-Forscherin nachweisen, dass PromptStealer bessere Ergebnisse liefert, als andere Methoden wie Image Captioning oder CLIP Interrogator. So waren die mithilfe der Prompts aus dem PromptStealer generierten KI-Bilder dem Originalbild am ähnlichsten.

PromptShield zur Verhinderung von Attacken

Als Cybersicherheitforscher:innen haben sich Shen und ihre Kolleg:innen auch Gedanken darüber gemacht, wie sich Prompt-Stealing-Attacken verhindern lassen. „Eine naheliegende Idee war zu überlegen, wie wir die Leistung der Machine-Learning-Modelle verringern können“, erklärt die CISPA-Forscherin. „Damit wollten wir verhindern, dass Modelle wie PromptStealer den benutzten Modifier erkennen können. Denn das Erkennen der exakten Modifier ist entscheidend für einen präzisen Prompt.“ Dies zu verhindern gelang ihr über das Hinzufügen von Störungen zum KI-generierten Bild. Wie relevant das von Shen entdeckte Angriffs-Szenario ist, zeigt sich daran, dass es bereits vom Softwarekonzern Microsoft in die Vulnerability Severity Classification for AI Systems aufgenommen wurde. Die Daten ihrer Studie stellt die CISPA-Forscherin im Internet frei zur Verfügung. Dazu zählt zum einen ein kuratiertes Datenset mit 61.467 KI-generierten Bildern von der Plattform Lexica, als auch der Code ihres Tools 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

CISPA-Forscher Aleksei Stafeev legt zum ersten Mal eine Studie vor, in der das Wissen über Tools zur automatisierten Analyse von Websites, sogenannte Webcrawler, im Bereich der Web-Sicherheitsmessung systematisiert wird. Dafür untersuchte er hunderte Paper, die in den letzten zwölf Jahren bei den wichtigsten internationalen Konferenzen publiziert wurden. Es zeigte sich, dass viele Paper die Crawler nur unzureichend beschreiben und dass randomisierte Algorithmen bei der Navigation der Crawler auf den Websites am besten abschneiden. Die vollständigen Ergebnisse sind im Paper „SoK: State of the Krawlers – Evaluating the Effectiveness of Crawling Algorithms for Web Security Measurements“ veröffentlicht, dass Stafeev im August auf dem USENIX Security Symposium 2024 präsentierte. Das Paper entstand im Rahmen des Projekts TESTABLE von CISPA-Faculty Dr. Giancarlo Pellegrino.

Untersuchung von Web-crawlern legt Defizite offen

Aleksei Stafeev

Studien zur Messung der Websicherheit etwa in Bezug auf die Umsetzung von Datenschutzmaßnahmen oder der Sicherheit von Websites erfreuen sich in der Cybersicherheitsforschung großer Beliebtheit. Für deren Umsetzung sind Crawler das Mittel der Wahl. „Ziel von Crawlern ist es, die Datenerfassung auf einer Website zu automatisieren“, erklärt CISPA-Forscher Aleksei Stafeev. Ihnen zu Grunde liegt ein Algorithmus, der steuert, wie der Crawler automatisiert über eine Website läuft, verschiedene Seiten besucht und von diesen Daten sammelt. „Aber Webcrawling ist nicht so einfach, wie es klingt“, so Stafeev weiter. „Theoretisch besuchen die Tools einfach nur Websites. Aber in Wirklichkeit ist das Internet sehr komplex: Auf jeder Website gibt es eine Vielzahl verschiedener Schaltflächen und jede davon führt möglicherweise zu einer anderen Seite. Man hat ein exponentielles Wachstum verschiedener Seiten und muss herausfinden, welche man tatsächlich besuchen muss, um die für die eigene Forschungsfrage relevanten Daten zu erhalten.“ Trotz der großen Bedeutung von Webcrawlern wurde deren Leistung bisher nur sehr begrenzt untersucht. Diese Lücke schließt Stafeev nun mit seiner Studie.

Dabei ist der CISPA-Forscher zweischrittig vorgegangen. „Zunächst haben wir eine Übersicht über die aktuellen Arbeiten zu Web-Messungen durchgeführt, die Crawler verwenden“, erzählt Stafeev. Ergebnis war ein Datenkorpus von 407 Papern, die zwischen 2010 und 2022 publiziert worden waren. „Wir haben versucht, daraus die Informationen zu extrahieren, welche Crawler wie verwendet werden, um ein allgemeines Bild davon bekommen, was bei Web-Messungen verwendet wird“, so der CISPA-Forscher. Für den zweiten Teil richtete Stafeev den Blick auf Paper der letzten drei Jahre, die neue Crawler vorschlagen. „Wir haben die Crawler im Hinblick darauf bewertet, welche Daten sie für den Zweck der Web-Sicherheitsmessung sammeln“, führt Stafeev weiter aus. Um die Crawler hinsichtlich der Code-Abdeckung, der Quellen-Abdeckung und der JavaScript-Sammlung untersuchen zu können, entwickelte Stafeev ein experimentelles Setup namens Arachnarium.

Unzureichende Beschreibungen und das Randomisierungs-Paradox

Eines der zentralen Ergebnisse des ersten Teils der Studie war, dass in den meisten Papern nur unzureichende Beschreibungen der Webcrawler zu finden waren. „Es war wirklich schwierig, die Informationen darüber, welche Technologie sie zum Crawlen verwenden und welche Techniken sie einsetzen, zu extrahieren und zu verstehen. Und es gab meist nicht genügend Details zu verwendeten Codes und Algorithmen. Oft hieß es nur ‚Wir verwenden Crawling' und das war's. Dass wir das als Community besser machen können, indem wir mehr Informationen über die von uns verwendeten Crawler und deren Konfiguration bereitstellen, war eine der wichtigsten Erkenntnisse." Wichtig ist dies vor allem, um die Reproduzierbarkeit von Studien garantieren zu können, was ein zentrales Kriterium wissenschaftlicher Qualität darstellt.

Ein erstaunliches Ergebnis förderte auch der zweite Teil der Studie zu Tage. „Nach unseren Daten scheinen Webcrawler, die randomisierte Algorithmen nutzen, am besten abzuschneiden", erklärt Stafeev. „Das ist eigentlich ziemlich überraschend, bedeutet es doch, dass wir, egal was wir an Navigationsstrategien entwickelt haben, immer noch keine bessere Lösung gefunden haben, als einfach nur zufällig auf Dinge zu klicken." Der CISPA-Forscher testete Crawler mit verschiedenen Metriken. Dabei hat er festgestellt, dass es bei all diesen drei Metriken keinen einzigen Gewinner unter den Crawlern gibt. „Wir können also keine einheitliche Empfehlung für alle geben, die besagt: ‚Jeder sollte diesen Crawler verwenden' ", so der CISPA-Forscher weiter. Es hängt also entscheidend vom Kontext und der genauen Zielsetzung ab, welcher Crawler passend ist.

Take-Aways und der weitere Umgang mit den Forschungsdaten

Um die Studie umsetzen zu können, hat Stafeev einen riesigen Datensatz erstellt. „Wir glauben, dass wir noch viel mehr daraus lernen können", erzählt er. „Und es wäre wirklich schön, wenn andere mehr Erkenntnisse aus den von uns gesammelten Daten gewinnen könnten." Aus diesem Grund hat Stafeev den kompletten Datensatz online frei zugänglich gemacht. Er selbst will sich in Zukunft wieder seiner eigentlichen Leidenschaft widmen: der Entwicklung neuer Crawler. Denn ursprünglich hatte Stafeev gar nicht geplant, eine so große Studie durchzuführen. Er wollte eigentlich nur seinen eigenen Crawler verbessern und sich dafür anschauen, wie andere mit dem Problem umgegangen waren. „Die Systematisierung von Wissen, wie sie dieser Studie zu Grunde liegt, ist ein ziemliche großes Unterfangen", erzählt er. „Aber ich habe bei diesem Projekt extrem viel gelernt, wie man solche Experimente durchführt und mit so großen Datensätzen arbeitet. Dieses Wissen werde ich mir bei meiner künftigen Arbeit zunutze machen", so der CISPA-Forscher abschließend.

»Webcrawling ist nicht so einfach, wie es klingt. Theoretisch besuchen die Tools einfach nur Websites. Aber in Wirklichkeit ist das Internet sehr komplex: Auf jeder Website gibt es eine Vielzahl verschiedener Schaltflächen und jede davon führt möglicherweise zu einer anderen Seite.«

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

Vom heimischen Rechner aus über den Webbrowser Zugang zu virtuellen Welten erhalten und dabei sicher und mit viel Privatsphäre mit anderen interagieren können: das ist das Versprechen von Metaverse-Plattformen. CISPA-Forscher Andrea Mengascini hat dieses Versprechen einem Realitätscheck unterzogen und erhebliche Risiken hinsichtlich mangelnden Privatsphäreschutzes sowie der Gefahr von Cyberangriffen gefunden. Seine Studie „The Big Brother's New Playground. Unmasking the Illusion of Privacy in Web Metaverses from a Malicious User's Perspective" hat er im Herbst 2024 auf der renommierten Conference on Computer and Communications Security (CCS) vorgestellt.

Studie zeigt Anfälligkeit von Metaverse-Plattformen für Cyberangriffe

Andrea Mengascini

„Virtual Reality und Onlinespiele haben mich schon immer interessiert“, erzählt CISPA-Forscher Andrea Mengascini. Als er und sein Forschungsgruppenleiter CISPA Faculty Dr. Giancarlo Pellegrino anfingen, sich mit der Sicherheit von VR-Headsets zu beschäftigen, machten sie eine interessante Entdeckung: „Uns wurde bewusst, dass dieselbe Technologie aus Onlinespielen auch in Metaversen Verwendung findet“, so Mengascini. Ein Metaverse definiert er als einen „virtuellen sozialen Raum, in dem Menschen nach Regeln interagieren können, die in gewisser Weise die der physischen Welt widerspiegeln“. Während die Sicherheit von Online-Spielen zum einen erforscht und zum anderen Schutzmechanismen umgesetzt sind, war dies bezogen auf Metaverse-Plattformen eine ungeklärte Frage. Dies weckte Mengascinis Interesse.

„Der Zugang zu einem Metaverse ist in den letzten Jahren viel einfacher geworden“, erklärt Mengascini. „Heute reicht ein normaler Webbrowser aus, um diese Räume zu betreten. Dank der WebXR-API-Schnittstelle kann dabei auch ein VR-Headset genutzt werden.“ Im Metaverse finden die Menschen eine Art digitale Kopie der realen Welt: Es gibt Räume, um sich privat zum Austausch zu treffen, große oder kleinere öffentliche Events, Spaß und Unterhaltung. „Diese Plattformen werden als webbasierte Clients ausgeführt und verwenden JavaScript, um komplexe 3D-Umgebungen, die Avatare der Benutzer:innen und Echtzeitinteraktionen zu verwalten. All das ist nicht nur entscheidend für den reibungslosen Betrieb des Metaverse, sondern spielt auch eine große Rolle für dessen Sicherheit“, so der CISPA-Forscher. Herauszufinden, ob es beim Zugang zum Metaverse über Webbrowser Sicherheitslücken gibt, war Mengascinis Ziel.

Die Fragen und das Vorgehen des Forschers

Für seine Studie stellte sich Mengascini drei konkrete Fragen: 1. Welche Entitäten, also etwa User und Objekte sind in Metaversen vorhanden und welche Attribute wie etwa Position oder Aussehen werden diesen zugeordnet? 2. Wo werden diese Elemente im Speicher abgelegt und welchen Zugriff können Angreifer:innen auf den Speicher erlangen? 3. Wie kann der Speicher für Angriffe ausgenutzt werden? Über eine Google-Suche identifizierte der CISPA-Forscher zunächst 27 Metaverse-Plattformen, die die WebXR-API-Schnittstelle nutzen. Im nächsten Schritt untersuchte er drei davon näher, die hinsichtlich Popularität, Nutzeraktivität, Internetverkehr und der Berichterstattung über reale Ereignisse am besten abschnitten. Die Methode, die Mengascini dafür wählte, war das Erstellen sogenannter Memory Snapshots, eine Momentaufnahme der Objekte im Speicher. Die Snapshots wurden vor und nach dem Ausführen einer bestimmen Aktion, wie der Bewegung eines Avatars von A nach B, aufgenommen. Danach wurde mithilfe eines Algorithmus überprüft, ob es Veränderungen gab und ob sich Informationen darüber aus dem Speicher des Webbrowsers auslesen lassen.

Speicher sind sehr einfach zugänglich

„Die wichtigste Erkenntnis ist, dass es diesen Plattformen an einfachsten Sicherheitsmechanismen mangelt“, erklärt Mengascini. „Das Problem ist, dass vor allem der Speicher der Browser viel zu einfach zugänglich ist.“ Selbst ein Laie könne mit etwas Übung sowohl auf den Quellcode als auch auf die eigentlichen Objekte im Speicher zugreifen. „Darüber hinaus haben wir herausgefunden, dass diese Plattformen eigentlich normale Praktiken des guten Programmierens bei der Entwicklung von Webanwendungen vermasselt haben“, so der Forscher weiter. „Die Entwickler:innen der Plattformen haben übersehen, dass durch eine Mischung aus nicht überprüften clientseitigen Informationen und einer übermäßigen Weitergabe von Informationen an den Client Angriffe möglich sind.“

Was all dies konkret bedeutet, erläutert Mengascini an einem Beispiel: „Nehmen wir mal an, es gäbe ein CISPA-Metaverse mit einem exakten Nachbau unseres Gebäudes. Was ich geschildert habe, würde bedeuten, dass die Computer eines jeden Users alle Information darüber bekommen, was am CISPA gerade passiert: Wer mit wem in welchem Raum spricht, wo sich einzelne Personen befinden und wie sie sich bewegen, inklusive der genauen Positionen der Wände. Daraus errechnet mein Computer die virtuelle Umgebung und sorgt etwa dafür, dass eine Wand verhindert, dass ich Gespräche im Büro des Direktors mithören kann. Gleichwohl hat der Browser aber die Information, was in dem Raum gesprochen wird. Und das ist schlecht. Auch wenn man mit einem normalen Client nicht mithören kann,

können diese Informationen von Angreifer:innen recht einfach extrahiert werden. Deswegen ist es wichtig, nicht zu viele Informationen zu teilen."

Mögliche Angriffsszenarien

Aus dieser Sicherheitslücke ergeben sich laut Mengascini eine Reihe möglicher Angriffsszenarien. Grundlegend ist die Erkenntnis, dass es für Angreifer:innen möglich ist, die Avatar- und die Kamera-Position von Angreifer:innen und Opfern sowie deren Aussehen unabhängig voneinander anzusteuern. Angreifer:innen können zum Beispiel ihre Kamera unabhängig von ihrem Avatar bewegen, erklärt Mengascini. „Damit können sich Angreifer:innen ungesehen im Raum positionieren und mithören", so Mengascini weiter. Eine andere Möglichkeit ist, dass Angreifer:innen ohne Wissen der Nutzer:innen deren Kamera-Inhalte sehen können. „Das ist als würden sich Angreifer:innen die VR-Brille des Nutzers aufsetzen, ohne dass dieser es merkt", erklärt der Forscher. Damit dies nicht passiert, müssten möglichst viele Informationen auf Seite des Servers verbleiben, was dort jedoch zu einer erhöhten Rechenleistung führen würde. Genau dies ist laut Mengascini auch einer der Gründe, warum die Metaverse-Plattformen so stark auf die Webbrowser setzen.

Neue Forschungsfragen als Take-Away

Wie in der Cybersicherheitsforschung üblich, wurden die drei Plattformen über die Sicherheitslücken informiert und ihnen Zeit gegeben, diese zu schließen. Umgesetzt hat dies bisher keine der drei Plattformen, weshalb deren Namen im veröffentlichten Paper weiter anonymisiert sind. „Aus Forschersicht bin ich auf der einen Seite natürlich besorgt darüber, dass die Plattformen sich nicht auf die Sicherheit konzentrieren wollen oder dazu nicht die Manpower haben", erzählt Mengascini. „Auf der anderen Seite vertrete ich den Standpunkt, dass wir als Forscher jetzt eine offene Forschungsfrage haben. Vielleicht ist es an der Zeit, dass wir Sicherheitsmechanismen vorschlagen, wie Angriffe verhindert oder zumindest erschwert werden können." Ideen, welche Schutzmechanismen implementiert werden könnten, hat er bereits. Dabei denkt er vor allem daran, das Wissen aus der Entwicklung von Onlinespielen zu nutzen und auf Metaversen zu übertragen. Wobei Mengascini bewusst ist, dass viele der Ansätze immer auch Nachteile mit sich bringen und noch ausführlich zu testen sind. Dieser Herausforderung will er sich jedoch in nächster Zeit stellen.

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

ÜBER DAS CISPA

Das CISPA Helmholtz-Zentrum für Informationssicherheit ist eine Großforschungseinrichtung des Bundes innerhalb der Helmholtz-Gemeinschaft. CISPA-Wissenschaftler:innen erforschen die Informationssicherheit in all ihren Facetten. Sie betreiben modernste Grundlagenforschung sowie innovative anwendungsorientierte Forschung und arbeiten an den drängenden Herausforderungen der Cybersicherheit, der künstlichen Intelligenz und des Datenschutzes. CISPA-Forschungsergebnisse finden Einzug in industrielle Anwendungen und Produkte, die weltweit verfügbar sind. Damit stärkt das CISPA die Konkurrenzfähigkeit Deutschlands und Europas.

Das CISPA bietet ein Forschungsumfeld von Weltrang und stellt einer großen Zahl an Forscher:innen umfangreiche Ressourcen zur Verfügung. Darüberhinaus fördert das CISPA in besonderem Maße auch die grundständige und postgraduale Bildung von Cybersicherheitsstudierenden. Das Zentrum hat sich zum Ziel gesetzt, eine Kaderschmiede für die nächste Generation an Cybersicherheitsexpert:innen und wissenschaftlichen Führungskräften in diesem Bereich zu werden. Das CISPA ist in Saarbrücken und St. Ingbert situiert. Die Lage des Zentrums in direkter Nachbarschaft zu Frankreich und Luxemburg ist ideal für grenzüberschreitende Kollaborationen mit anderen Forschungsinstitutionen.

Aktuell konzentriert sich unsere Forschung auf die folgenden sechs Forschungsbereiche:

Algorithmische Grundlagen und Kryptographie

Vertrauenswürdige Informationsverarbeitung

Verlässliche Sicherheitsgarantien

Erkennung und Vermeidung von Cyberangriffen

Sichere vernetzte und mobile Systeme

Empirische und verhaltensorientierte Sicherheit

IMPRESSUM

CISPA – Helmholtz-Zentrum
für Informationssicherheit gGmbH
Stuhlsatzenhaus 5
66123 Saarbrücken, Deutschland

Herausgeber

Sebastian Klöckner

Verantwortliche Redaktion

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

Redaktion

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

Illustration

Alexandra Goweiler,
Chiara Schwarz

Gestaltung

Tobias Ebelshäuser

Fotografie

Januar 2025

Stand des Impressums

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

Kontakt Corporate Communications

CISPA
HELMHOLTZ-ZENTRUM FÜR INFORMATIONSSICHERHEIT

Neue Nutzerstudie zeigt, worin Passwortmanager besser werden müssen

Das Beispiel Tor und VPN: Cybersicherheit zwischen Tatsachen und Erzählungen

Sicherheitslücken bei Browserweiterungen im Chrome Web Store

Dieser Artikel wird Ihr Leben verändern! – Clickbait-PDFs sind die neueste Phishing-Masche

Neuer Ansatz, um den Prozess der Zwei-Faktor-Authentifizierung auf Websites zu vergleichen

Schleifen ohne Ende: Neuer Denial-of-Service-Angriff gefährdet Protokolle auf der Anwendungsschicht

Manuelles Transkribieren schlägt (noch) KI: Eine vergleichende Studie über Transkriptionsservices

CISPA-Forscher entwickeln neues Sicherheitskonzept für Zoom-Gruppen

Neue Ergebnisse aus der KI-Forschung: Menschen können KI-generierte Medien kaum erkennen

Anmeldebenachrichtigungen: Ein wichtiger Sicherheitsfaktor aus Nutzerperspektive

Kritische Sicherheitslücken in Voice over WiFi aufgedeckt

Sicherheitslücke „GhostWrite“ untergräbt Integrität der RISC-V-CPU „XuanTie C910“ von T-Head

Veraltete Codeschnipsel von Stack Overflow gefährden Softwaresicherheit

Die Suche nach Hilfe in sozialen Medien bei Problemen mit Krypto-Wallets kann Betrüger anlocken

JANUS: Vermeidung von Mehrfachregistrierungen in der humanitären Hilfe dank Biometrie

Prompt Stealing: CISPA-Forscherin entdeckt neues Angriffsszenario für Text-zu-Bild-Generatoren

Untersuchung von Webcrawlern legt Defizite offen

Studie zeigt Anfälligkeit von Metaverse-Plattformen für Cyberangriffe