MONTHLY SECURITY SUMMARY

AUSGABE MÄRZ 2023
FLIPPER ZERO UND TEDX IN BOSTON

ANGRIFFE AUF KABELLOSE PERIPHERIE

Mit Flipper Zero wird es verhältnismässig einfach möglich, kabellose Peripherie anzugreifen. Unser Beitrag diskutiert die Möglichkeiten solcher Attacken.

HINTERGRUNDINFOS ZU TEDX IN BOSTON

Wir haben einen Vortrag an TEDx in Boston gehalten und erklären in unserem Artikel, wie ein Event dieses Ausmasses ausgerichtet wird.

März 2023: Kriminelle Einfältigkeit

Wir werden immer wieder für Analysen und Aufklärungen im *Darknet* herbeigezogen. Dabei ist es nicht untypisch, dass hochgradig kriminelle Akteure am Werk sind, die das schnelle Geld machen wollen.

Nicht selten offenbart sich relativ schnell, dass diese nur die Grundlagen von Sicherheit und Privatsphäre verstanden haben. Sie sind da, um sich zu bereichern. Und nicht, um ein Verständnis für Technologien und Vorgehensweisen aufzubauen. Doch dieses wird eigentlich vorausgesetzt, um überhaupt über längere Zeit sein kriminelles Geschäftsmodell ausüben zu können.

Aus diesem Grund machen sie über kurz oder lang Fehler, die zu einer Deanonymisierung, Enttarnung und Identifizierung führen können. Für uns ist es wichtig, dass solche Fehler im Idealfall provoziert werden können. Manchmal passieren sie aber halt auch einfach von selbst. In diesen Situationen liegt es an uns, den Fehler zu bemerken und zu unserem Vorteil zu nutzen.

Bisher haben wir noch niemanden gesehen, der nicht früher oder später einen Fehler macht. Jeder Kriminelle, der das Gefühl hat, dass ein solcher ihm nicht passieren wird, zelebriert ironischerweise nur seine kriminelle Einfältigkeit. Und wir zelebrieren am Schluss mit ihm.

Marc Ruef
Head of Research

NEWS

WAS IST BEI UNS PASSIERT?

VORTRAG AN TEDXBOSTON

Am 6. März fand die jährliche *TEDxBoston* Veranstaltung statt, die unter dem diesjährigen Motto *Countdown to Artificial General Intelligence* stand. Diese Veranstaltung befasste sich mit den jüngsten Fortschritten bei generativen und multimodalen Modellen, wie *ChatGPT* und *Gato*. Marisa Tschopp wurde eingeladen, einen Vortrag über unsere Forschung in Zusammenarbeit mit dem *Leibniz Institut für Wissensmedien* (IWM) im Bereich der *Mensch-Maschine-Beziehungen* zu halten.

RADIOINTERVIEW ZU ANGRIFFE GEGEN UNIVERSITÄT ZÜRICH

Die weitreichenden Angriffe gegen die *Universität Zürich* beschäftigen die Schweizer Medienlandschaft. Hierzu hat Tomaso Vasella ein Radiointerview mit *TOP-Medien* geführt. In diesem geht er auf die etwaigen Hintergründe der Angriffe ein und wie man sich gegen diese schützen kann.

BEITRAG ZU KI UND DISKRIMINIERUNG

In einem Beitrag im *Handelsblatt*, hat Frau Daniela Kluckert, parlamentarische Staatssekretärin beim *Bundesminister für Digitales und Verkehr*, über das Thema *Diskriminierung und KI* geschrieben. Die Bundesregierung fördert früh Frauen in Forschung und Entwicklung. In einer Zusammenarbeit mit Marisa Tschopp wurde das Thema im Vorhinein diskutiert und nun ebenfalls in einem ausführlicheren Artikel veröffentlicht.

Weitere News zu unserem Unternehmen finden Sie auf unserer Webseite.

SCIP BUCHREIHE

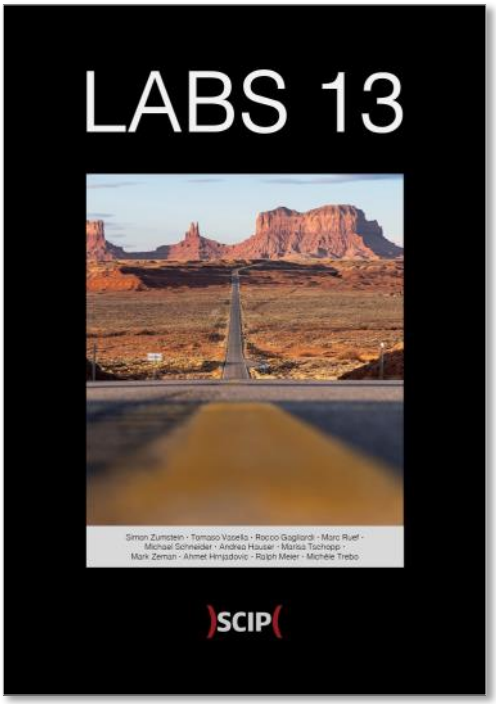
UNSER AKTUELLES JAHRBUCH

Erneut veröffentlichen wir die aktuelle Ausgabe unseres Jahrbuchs. Bereits zum 13ten Mal fassen wir in diesem die Fachbeiträge von einem Jahr Forschung im Bereich Cybersecurity zusammen.

Das Buch ist wiederum sowohl in deutscher (ISBN 978-3-907109-30-4) als auch in englischer Sprache (ISBN 978-3-907109-31-1) verfügbar. Das Vorwort wurde von Dr. iur. David Vasella verfasst und setzt sich mit den rechtlichen Rahmenbedingungen der Informationssicherheit auseinander.

In unserem Katalog finden sich ebenfalls themenspezifische Bücher zu Künstlicher Intelligenz (ISBN 978-3-907109-14-4) und Sicherheit in der Hotellerie (978-3-907109-16-8).

Weitere Informationen auf unserer Webseite.



ISBN 978-3-907109-30-4 [de]
ISBN 978-3-907109-31-1 [en]

JEDE SCHWACHSTELLE IST EINZIGARTIG

Bildquelle: https://pixabay.com/images/id-7838638/

RALPH MEIER

FLIPPER ZERO FÜR ANGRIFFE AUF KABELLOSE PERIPHERIE

In diesem Artikel geht es um ein praktisches Beispiel, wie kabellose Peripheriegeräte wie Mäuse oder Tastaturen angegriffen werden können, als Beispiel dient die Logitech Unify-Technologie. Für ein Grundverständnis und um einen Überblick über die verschiedenen Module und Funktionen des Flipper Zeros zu erhalten, sollte folgender Artikel Flipper Zero – Was kann das kleine Hacking Tamagotchi zuerst gelesen werden. Die Inspiration zur Auseinandersetzung mit dem Thema Angriff auf kabellose Peripheriegeräte kam durch ein Video.

Der Einsatz von kabellosen Tastaturen bringt eine erhöhte Angriffsfläche mit sich und je nach System sind öffentlich bekannte Schwachstellen vorhanden, wie CVE-2019-13055. Darin geht es um die Aufzeichnung des AES-Schlüsselmaterials bei der Erstkopplung eines Logitech Unify-Geräts mit einem Unify-Adapter und die Entschlüsselung der anschliessend getippten Zeichen.

MOUSEJACK

MouseJack ist eine Sammlung von Schwachstellen, welche das Injizieren von Tastatureingaben und das Umgehen von Verschlüsselung beinhaltet. Offiziell wird MouseJack als CVE-2016-10761 gelistet. Eine Vielzahl von kabellosen Tastaturen und Mäusen, die über die Frequenz 2.4GHz kommunizieren, sind davon betroffen. Peripheriegeräte, die ausschliesslich über Bluetooth kommunizieren sind davon ausgeschlossen. Die Schwachstelle wurde von der Firma Bastille im Jahr 2016 entdeckt, sie listet auf ihrer Webseite auch betroffene Geräte mit Hersteller Statements und eine Behebung der Schwachstelle, wo es möglich ist, auf.

Funktionsweise

Bei kabelloser Peripherie, wie Mäuse oder Tastaturen gibt es keine proprietären Protokolle, welche auf der Frequenz 2.4GHz operieren. Demnach ist jeder Hersteller selbst für die Kommunikation und die eingesetzte Security zuständig. Bei einer Mausbewegung oder während dem Tippen werden die getätigten Bewegungen beziehungsweise Anschläge mittels Pakete, die genaue Umsetzung ist wie bereits erwähnt Hersteller abhängig, an den Wireless Empfänger am Computer übermittelt. Im Normalfall werden die getätigten Eingaben des Benutzers verschlüsselt Übertragen. Der Schlüssel wird dabei beim initialen Pairing zwischen Eingabegerät und

Wireless Empfänger festgelegt. Die Verschlüsselte Übertragung verhindert das einfache Abhören von fremden Eingaben.

Injizieren von Tastatureingaben

Die getesteten Unify-Adapter, welche von der MouseJack Schwachstelle betroffen waren, wurden zwar initial gepairt geliefert, konnten aber selbständig mit neuen Mäusen oder Tastaturen verbunden werden. Demnach machte es keinen Unterschied, ob der Unify-Adapter ausschliesslich mit einer Maus, einer Tastatur oder mit beiden gepairt war. Dies lässt daraus schliessen, dass beim ausschliesslichen Einsatz einer Maus nicht überprüft wird, ob die erhaltenen Befehle auch ausschliesslich Mausbewegungen oder das Betätigen von Maustasten sind. Daher ist es auch möglich beim Einsatz einer Funkmaus ungewollte Tastatureingaben auf dem Zielsystem vorzunehmen.

Bei der ursprünglichen Entdeckung der MouseJack Schwachstelle von Bastille wurde festgehalten, dass die meisten Hersteller die getätigten Tastatureingaben verschlüsseln, die Unify-Adapter jedoch nicht überprüfen, ob alle empfangen Benutzereingaben verschlüsselt sind. Beziehungsweise die Eingaben auch in unverschlüsselter Form entgegengenommen werden. Dies vereinfacht den Vorgang für Angreifer enorm, da sie sich nicht um den eingesetzten Schlüssel kümmern müssen, sondern lediglich die genaue Unify-Adapter-Adresse benötigten, um den gewünschten Payload zu versenden.

ANGRIFF AUF KABELLOSE PERIPHERIEGERÄTE MIT FLIPPER ZERO

Da im Inspirationsvideo, welches zu diesem Artikel führte, ein Flipper Zero eingesetzt wurde, war das Ziel diesen Angriff nachzubauen.

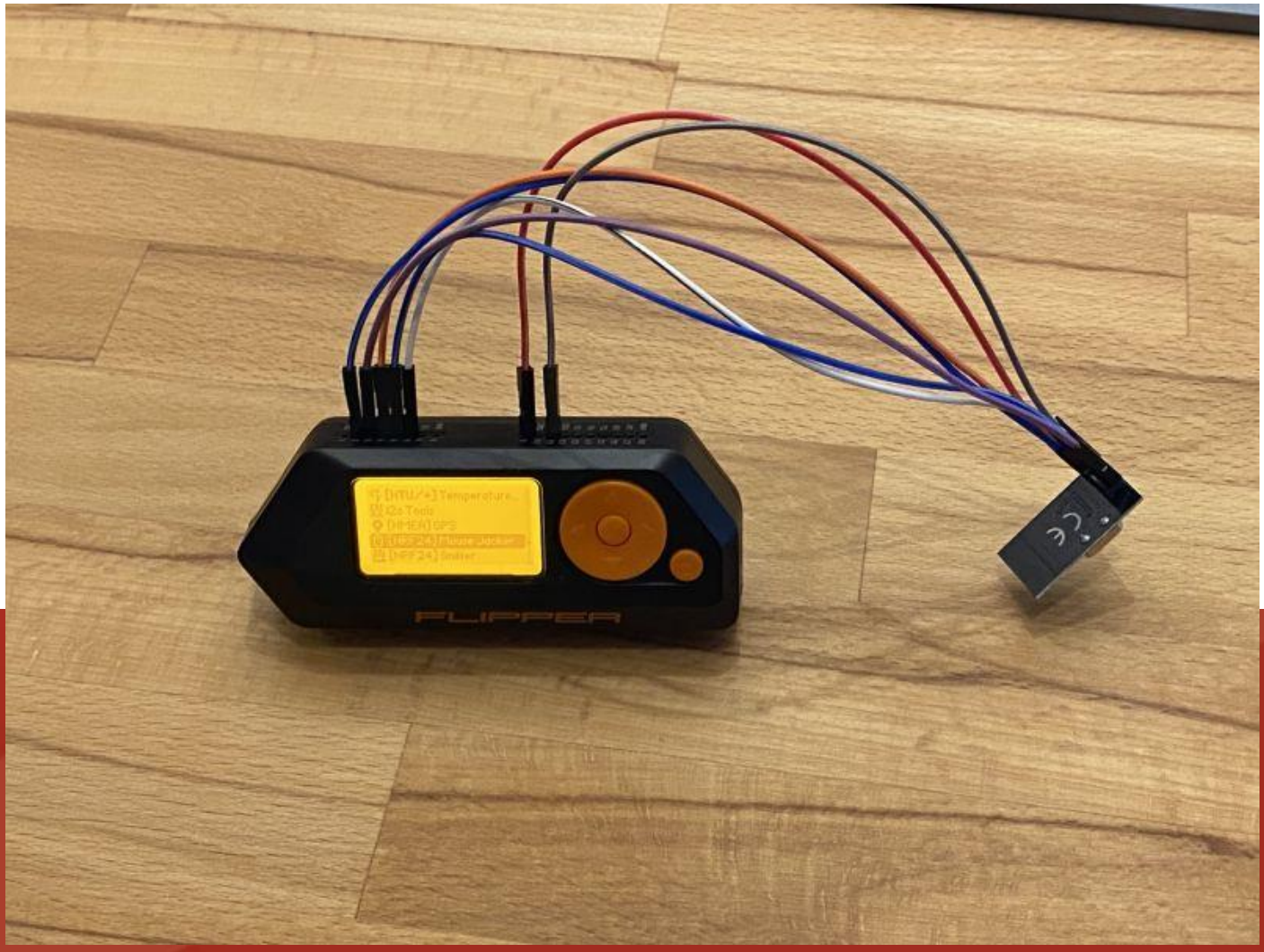
Testsetup

Als Testsetup wurde ein Windows Notebook mit einem Logitech Unify-Adapter und einer Logitech M525 Maus sowie später einer Logitech K800 Tastatur eingesetzt. Um den Angriff auszuführen, wurde ein Flipper Zero mit einem NRF24L01+ WLAN-Funkmodul, das via GPIO-Pins verbunden war, eingesetzt. Als Firmware auf dem Flipper Zero kam ein Fork der Flipper Firmware von RogueMaster zum Einsatz, dies weil da die notwendigen Scripts für den

Betrieb des NRF24L01+ WLAN-Funkmoduls über die GPIO-Pins bereits vorhanden sind.

Die Verkabelung zwischen Flipper Zero und NRF24L01+ WLAN-Funkmodul wurde nach dem verlinkten Schema umgesetzt. Nach der Verkabelung sah dies wie in der Darstellung abgebildet aus.

Nach dem Verbinden über die GPIO-Pins kann die Adresse des Unify-Adapters mit dem NRF24 Sniffer Script herausgefunden werden und danach mit dem NRF24 MouseJack Script angegriffen werden. Das MouseJack Script fragt beim Start um ein Ducky Script als Payload, welches ausgeführt wird und die Tastatureingaben unverschlüsselt an den Unfiy-Adapter schickt.



Es kann zum Beispiel folgendes Ducky Script verwendet werden:

```
DELAY 1000
GUI r
DELAY 500
STRING firefox.exe
DELAY 500
ENTER
DELAY 1500
CTRL l
DELAY 500
STRING www.scip.ch
DELAY 500
ENTER
```

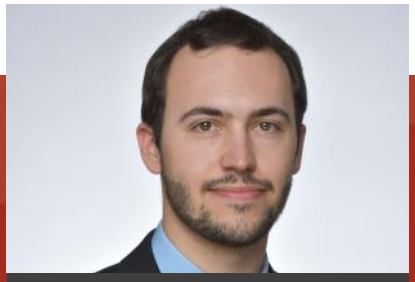
Ducky Scripts werden im Artikel Angriffe über Peripheriegeräte genauer erläutert.

EINFLUSS VON FLIPPER ZERO IN KOMBINATION MIT MOUSEJACK

Durch die geringe Grösse des Flipper Zeros ist ein Angriff auf kabellose Peripheriegeräte oder andere Ziele, welche eine gewisse physische Nähe benötigen, einiges einfacher umzusetzen. Der Flipper Zero passt nämlich auch mit Zusatzmodul oder dem oben gezeigten WLAN-Funkmodul problemlos in eine Jacken- oder Umhängetasche. Dadurch ist er bei einem Angriff mit physischer Nähe deutlich unauffälliger. In einem Grossraumbüro, in welchem mehrere Personen kabellose Peripherie einsetzen, die von der MouseJack Schwachstelle betroffen sind, ist die Wahrscheinlichkeit für einen unscheinbarer, erfolgreichen Angriff sehr hoch.

FAZIT

Kabellose Geräte bringen eine höhere Angriffsfläche mit sich, sollten daher stehts auf dem aktuellen Firmwarestand gehalten werden und in sensitiven Bereichen sollte für den Dauerbetrieb eine kabelgebundene Tastatur und Maus vorgezogen werden. Die MouseJack Schwachstelle ist zur Zeit dieses Artikels bereits über sieben Jahre alt und bei der Prüfung von Geräten im eigenen Umfeld stehts präsent und ausnutzbar. Durch den geringen Formfaktor des Flipper Zeros und die Unterstützung einer Vielzahl von Funkfrequenzen, sowie der einfachen Erweiterbarkeit über die GPIO-Pins, eignet sich das Gerät perfekt für Angriffe auf kabellose Ziele mit notwendiger physischer Nähe zum Zielgerät.


Ralph Meier

next gen vulnerability intelligence

VulDB

Den Gegner verstehen

Tägliche Dokumentation neuer Schwachstellen, detaillierte Analyse der technischen Hintergründe, exklusive Details zu Exploiting und Gegenmassnahmen. Mit vuldb.com erhalten Sie ein durchschlagskräftiges Werkzeug in die Hand!

SCIP
official data provider

https://vuldb.com

MARISA TSCHOPP

EINBLICK IN TEDX IN BOSTON

TEDx-Events sind unabhängig organisierte Veranstaltungen, die sich an den grösseren TED-Konferenzen (Technology, Entertainment, Design) orientieren. Dabei handelt es sich um globale Veranstaltungen mit Vorträgen von Experten und Innovatoren aus verschiedenen Bereichen. Arisa Tschopp war eine der eingeladenen Rednerinnen und hielt einen Vortrag über unsere Forschung zu Beziehungen zwischen Mensch und KI.

TEDx-Veranstaltungen werden in der Regel zu einem bestimmten Thema organisiert und umfassen eine Reihe von Rednern, die Experten auf ihrem Gebiet sind oder eine inspirierende Geschichte zu erzählen haben. Die Vorträge sind in der Regel 18 Minuten lang und sollen zum Dialog und zum Handeln anregen und bieten den Zuhörern oft die Möglichkeit, sich mit den Rednern und untereinander auszutauschen. Es gibt eine Playlist der beliebtesten TED Talks aller Zeiten mit Bill Gates, Elon Musk oder Brene Brown. Sir Ken Robinsons TED-Talk aus dem Jahr 2006 wurde über 74 Millionen Mal angesehen.

ÜBER TEDXBOSTON

Die TEDxBoston ist nach Angaben von John Werner eine der grössten und erfolgreichsten TEDx Veranstaltungen weltweit. Die jüngste Veranstaltung fand am 6. März im Quin House im Zentrum Bostons statt und war eine Sonderausgabe zum Thema Künstliche Intelligenz. Unter dem provokanten Titel Countdown to Artificial Intelligence traten 61 Redner auf, von denen jeder 5 Minuten Zeit hatte, um über sein spezielles Thema zu sprechen: Von technologischen Entwicklungen, über Geschäftsmöglichkeiten bis hin zu gesellschaftlichen Auswirkungen. Das neue Format ist eine Herausforderung und zugleich eine Chance, eine grössere Vielfalt an Themen und Rednern zu präsentieren, aber auch ein breiteres Publikum anzusprechen, wo jeder um die Aufmerksamkeit der “swiping tik-tok” Generation kämpft.

Abstract: 2022 war ein bahnbrechendes Jahr für den Fortschritt in der Künstlichen Intelligenz (KI). Zu den diesjährigen Fortschritten bei generativen Modellen gehören grosse Sprachmodelle wie GPT-3.5 und ChatGPT, modusübergreifende Modelle wie DALL-E 2 und Stable Diffusion sowie multimodale Modelle wie Gato. Die Schätzung der Metaculus-

Gemeinschaft für das Ankunftsdatum der "Weak AGI" ist von 2042 auf 2027 gesunken. Im Jahr 2023, an der Schwelle zu einem Wendepunkt in den Fähigkeiten der KI, stehen wir auf den Schultern dieser sich beschleunigenden Technologien und sind bereit, jeden Teil der menschlichen Gesellschaft zu beeinflussen. Wir kommen zusammen, um zu diskutieren, wie diese Zukunft aussehen könnte – wie wir die noch ausstehenden Herausforderungen im Bereich des Deep Learning und der KI bewältigen und unsere eigene menschliche Intelligenz auf ein neues Niveau heben können. Wir haben kuratierte Ideen/ Visionen, wie diese Zukunft aussehen könnte.

THEMEN BEI TEDXBOSTON

Die Vielfalt der Themen war immens: KI für Smart Homes, Spieleentwicklung oder Programmierung. Forscher und Praktiker teilten ihre Ideen oder Startups. Das Gesundheitswesen war ein sehr prominentes Thema in der Hoffnung, Krebs zu bekämpfen, CT-Scans zu verbessern oder klinische Studien zu beschleunigen. Auch die Themen Vertrauenswürdigkeit und erklärbare KI waren immer wieder präsent. Es war auch faszinierend zu sehen, wie Menschen mit indogenen Hintergründen_ ihren Gemeinden helfen, auf dem neuesten Stand zu bleiben und Kindern das Programmieren beizubringen. Die vollständige Liste der Themen (die Arbeitstitel sind) kann online gefunden werden und die jeweiligen Vorträge werden in den nächsten 2-3 Monaten online sein (Youtube oder TED-Website).

ÜBERBLICK ÜBER UNSEREN VORTRAG BEI TEDXBOSTON

Marisa Tschopp wurde eingeladen, am Nachmittag einen Vortrag über unsere Forschung zu human-AI relationships zu halten, hier ist eine Zusammenfassung davon:

Jeden Tag drücken 19.000 Menschen ihren Sprachassistenten ihre Liebe aus und 6.000 Menschen in Indien machen ihnen sogar einen Heiratsantrag. In den Medien wird oft auf diese nicht ganz so seriösen Studien hingewiesen, wie z. B. eine Studie, die ergab, dass 14 % der männlichen Nutzer von Smart-Home-Lautsprechern im Vereinigten Königreich eine sexuelle Beziehung mit ihren Systemen wünschen. Dies heizt den öffentlichen Diskurs darüber an, wie die Menschen wirklich über diese sprechenden Maschi-

nen denken, die im Grunde genommen nur Hard- und Software sind.

Trotz der Tatsache, dass diese Maschinen nicht menschlich sind, hat eine Fülle empirischer Untersuchungen gezeigt, dass Menschen dazu neigen, sie zu vermenschlichen und sie als soziale Akteure zu behandeln. Aber nur weil jemand sagt, dass er sein KI-System liebt, bedeutet das, dass er es wirklich so liebt, wie er es bei einem anderen Menschen tun würde? Wenn die Menschen ihren Sprachassistenten also nicht wirklich lieben, ihn aber auch nicht einfach nur als Werkzeug sehen, wie nehmen sie dann ihre Beziehung zur KI wahr? Und was können wir aus einem besseren Verständnis der Beziehungen zwischen Mensch und KI lernen?

Um diese Fragen zu beantworten, haben wir eine mehrdimensionale Beziehungstheorie aus der Psychologie verwendet und sie auf den Kontext der Beziehungen zwischen Mensch und KI angewandt. Wir untersuchten etwa 1000 KI-Nutzer und fanden heraus, dass sie auf drei Arten mit ihren KI-Systemen in Beziehung treten: Die traditionelle Herr-Diener-Beziehung, eine rationale Beziehung ohne Hierarchien und eine freundschaftliche, emotionale Beziehung. Nur wenige charakterisieren ihre Beziehung als freundschaftliche, emotionale Beziehung. Es

überrascht nicht, dass die meisten Nutzer die Beziehung zu ihrem Sprachassistenten als eine traditionelle Herr-Diener-Beziehung wahrnehmen. Überraschend war, dass die nicht-hierarchische Beziehung fast genauso beliebt war wie die Herr-Diener-Beziehung.

Dieses Ergebnis könnte für die Entwickler von Sprachschnittstellen interessant sein, denn wie viel Befugnis die Nutzer einem System zuschreiben, kann sich darauf auswirken, wie sie es nutzen oder wofür sie den Sprachassistenten einsetzen. Nehmen wir eine einfache Aufgabe wie das Stellen eines Weckers. Sie erfordert wenig Engagement, nur kurze, einfache Interaktionen. Eine komplexe Aufgabe, wie z. B. das Online-Shopping mit einem Sprachassistenten, erfordert mehr Engagement. Dazu gehören beispielsweise Dialoge mit mehreren Abzweigungen und potenziell mehr Datenaustausch und finanzielle Risiken. Anders ausgedrückt: Mehr "geteilte" Verantwortung. Wenn wir also digitale Assistenten auch für komplexere Aufgaben einsetzen wollen, wäre es sinnvoll, sie mehr als Entscheidungspartner zu sehen oder zu gestalten, statt als blosse Befehlsempfänger. Bedeutet das, dass die Rolle der digitalen Assistenten als unsere Diener irgendwie aus der Mode kommen wird?

Wir sind dieser Frage nachgegangen, indem wir Einkaufsentscheidungen per Sprache untersucht haben. Konkret wollten wir wissen, ob die Art und Weise, wie Menschen sich zu ihrem Sprachassistenten verhalten, die Art der Produkte beeinflusst, die sie über ihren Sprachassistenten kaufen. Die Forschung zeigte, dass die Betrachtung des Sprachassistenten als Freund oder Diener den Kauf von billigen und einfachen Produkten per Sprache fördert. Überraschenderweise fanden wir aber auch heraus, dass die Wahrnehmung des Sprachassistentin als Freund am wichtigsten ist, wenn es um den Kauf von teuren und komplexen Produkten geht. Mit anderen Worten: Friendship sells!

Es gibt jedoch moralische Bedenken, die sehr dagegen sprechen, Entwicklern von Sprachbenutzerschnittstellen zu empfehlen, ihre Schnittstellen als AI Friends zu gestalten, um den Umsatz zu steigern. Die Vermenschlichung von Maschinen kann negative Folgen haben, z. B. die Weitergabe von persönlichen Daten oder das Verleiten von Menschen zu Entscheidungen, die nicht in ihrem Interesse liegen. Darüber

hinaus wurden Fälle aufgedeckt, in denen Nutzer über Symptome von Depressionen berichteten, nachdem sie die Verbindung zu einem Chatbot verloren hatten. Was tun wir, wenn unsere Bindung an diese Technologien zu einer pathologischen Sucht wird oder sich zu einer Unfähigkeit entwickelt, mit echten Menschen im wirklichen Leben umzugehen?

FAZIT

Marisa Tschopp schloss ihren Vortrag mit dem Hinweis auf die Notwendigkeit, die Beziehung zwischen Mensch und KI besser zu verstehen. Denn die Art und Weise, wie wir uns zu diesen Systemen verhalten, kann das Nutzerverhalten in einer Weise beeinflussen, die wir noch nicht vollständig verstehen. Und diese psychologischen Mechanismen können viel zu leicht ausgenutzt oder in Weisen manipuliert werden, die schwer zu kontrollieren sein werden. Der Vortrag wird demnächst online verfügbar sein.

Ziel der TEDxBoston-Veranstaltung war es, aktuelle Herausforderungen zu erforschen und neue Einsichten in die menschliche Intelligenz zu gewinnen, und zwar mit einer gut ausgewählten Reihe von 5-Minuten-Vorträgen, die von angesehenen Rednern zu Themen wie den Auswirkungen von AGI auf Ethik, Kreativität, Intelligenzsteigerung, die Zukunft von Arbeit und Bildung und Innovation im Gesundheitswesen gehalten wurden, um nur einige zu nennen. Unserer Meinung nach waren die Themen gut ausgewählt, ebenso wie die Redner, von Newcomern bis hin zu erfahrenen Experten auf diesem Gebiet. Besonders beeindruckt waren wir von der hervorragenden Zusammenstellung der Heterogenität der Referenten hinsichtlich ihrer Herkunft und Kultur. Diese Bereicherung ist immens wertvoll für einen sinnvollen Austausch, um den eigenen Horizont zu erweitern und, kurz gesagt, um bessere KI für eine bessere Zukunft zu schaffen.

Marisa Tschopp

EIN AUSBLICK IN DIE ZUKUNFT IST IN JEDEM FALL HILFREICH

Bildquelle:https://pixabay.com/images/id-7781669/

SCIP MONTHLY SECURITY SUMMARY

IMPRESSUM

ÜBER DEN SMSS

Das *scip Monthly Security Summary* erscheint monatlich und ist kostenlos.

Anmeldung: smss-subscribe@scip.ch
Abmeldung: smss-unsubscribe@scip.ch

Informationen zum Datenschutz.

Verantwortlich für diese Ausgabe:
Marc Ruef

Eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch die Redaktion des Herausgebers, den Redaktoren und Autoren nicht übernommen werden. Die geltenden gesetzlichen und postalischen Bestimmungen bei Erwerb, Errichtung und Inbetriebnahme von elektronischen Geräten sowie Sende- und Empfangseinrichtungen sind zu beachten.

ÜBER SCIP AG

Wir überzeugen durch unsere Leistungen. Die scip AG wurde im Jahr 2002 gegründet. Innovation, Nachhaltigkeit, Transparenz und Freude am Themengebiet sind unsere treibenden Faktoren. Dank der vollständigen Eigenfinanzierung sehen wir uns in der sehr komfortablen Lage, vollumfänglich herstellerunabhängig und neutral agieren zu können und setzen dies auch gewissenhaft um. Durch die Fokussierung auf den Bereich Information Security und die stetige Weiterbildung vermögen unsere Mitarbeiter mit hochspezialisiertem Expertenwissen aufzuwarten.

Weder Unternehmen noch Redaktion erwähnen Namen von Personen und Firmen sowie Marken von fremden Produkten zu Werbezwecken. Werbung wird explizit als solche gekennzeichnet.

scip AG
Badenerstrasse 623
8048 Zürich
Schweiz

+41 44 404 13 13
www.scip.ch