MONTHLY SECURITY SUMMARY

)SCIP(

AUSGABE JULI 2022
AREA41 UND HTTP/2 REQUEST SMUGGLING

RÜCKBLICK ZUR AREA41 IN ZÜRICH

Die bekannte Information Security Conference in Zürich konnte endlich wieder durchgeführt werden. Unsere Berichterstattung diskutiert die spannendsten Vorträge des Events.

HTTP/2 REQUEST SMUGGLING IM DETAIL

Das Umsetzen von HTTP/2 Request Smuggling bedarf eines zusätzlichen Verständnisses für die eingesetzten Technologien. Das Vorgehen wird in unserem Beitrag detailliert besprochen.

Juli 2022: Software-Update für Waffen

Deutschland hat der Ukraine als Unterstützung vier *Raketenwerfer* versprochen. Geliefert werden können jedoch nur drei. Der Grund: Den Geräten fehlt ein *Software-Update*, weshalb ein Grossteil der aktuellen Munition nicht verschossen werden kann.

Solche Meldungen lesen sich wie Satire, denn Zeitschriften wie *Titanic* oder *The Onion* könnten die Realität nicht besser persiflieren. Den Leuten in der Ukraine ist aber definitiv nicht zum Lachen zumute. Eine ballistische Waffe, die nicht schiessen kann, taugt nur noch als Briefbeschwerer oder Türstopper.

Da erscheint der Unmut der Steuerzahlen zuerst fehlplatziert. Denn auch die werden sich natürlich unmittelbar fragen, ob und inwiefern ihre abgelieferten finanziellen Mittel richtig eingesetzt werden. Wenn es schon beim Update von Raketenwerfern scheitert, möchte man gar nicht wissen, wo es im riesigen Verwaltungsapparat sonst noch hapert.

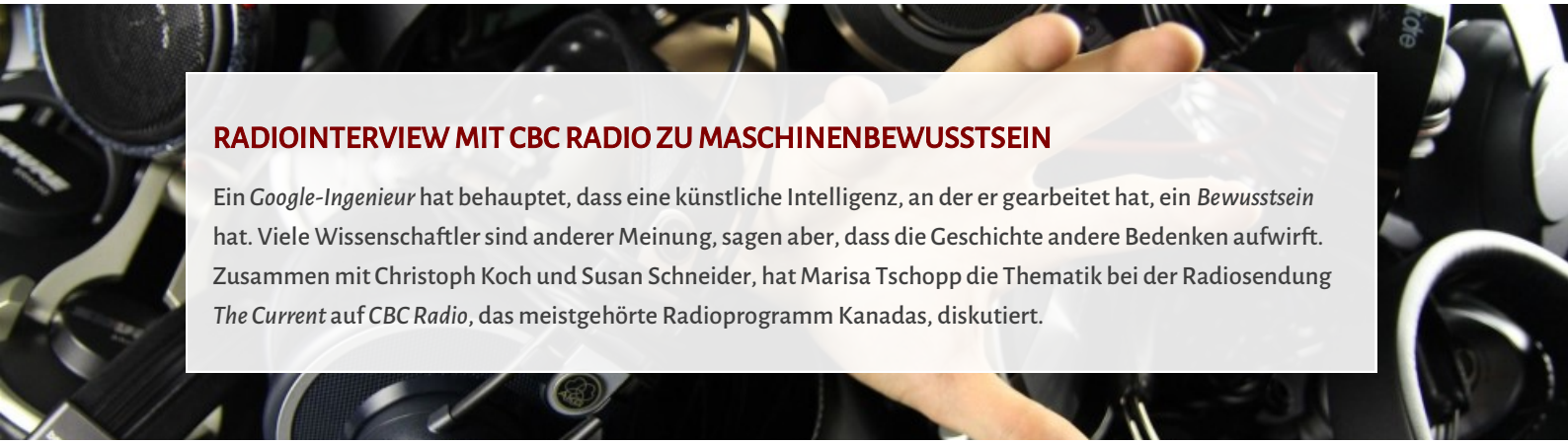
Marc Ruef
Head of Research

NEWS

WAS IST BEI UNS PASSIERT?

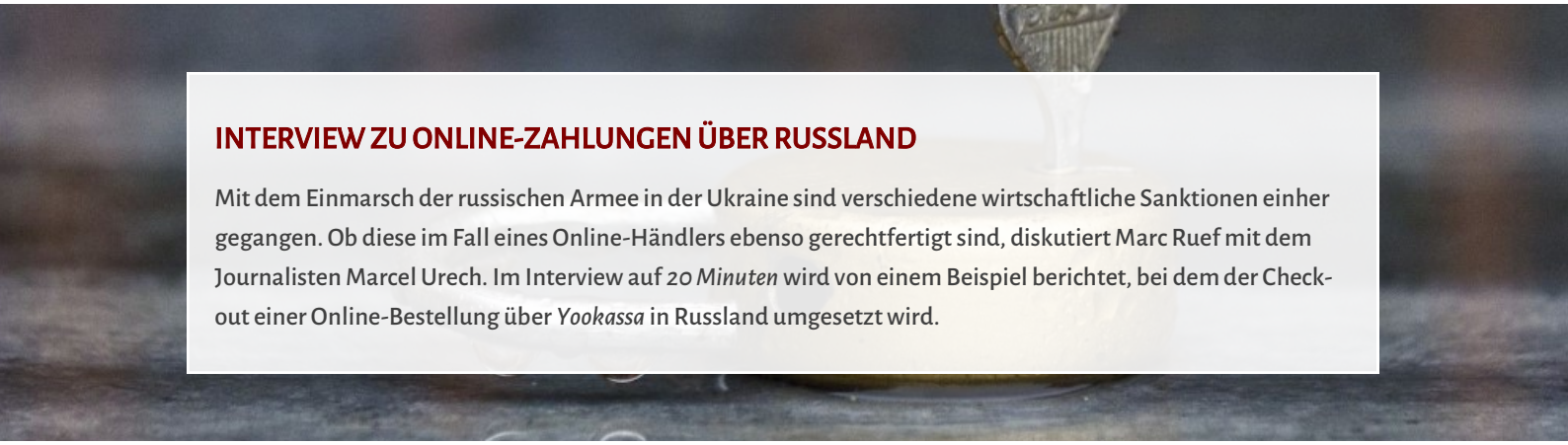
PODIUMSDISKUSSION ZU APPROPRIATE TRUST IN HUMAN-AI INTERACTIONS

An der 20. *European Conference on Computer-Supported Cooperative Work* (ECSCW) findet am 27. Juli ein Workshop zum Thema *angemessenes Vertrauen in der Mensch-KI Interaktion* statt. Marisa Tschopp wurde zur *Podiumsdiskussion* eingeladen, welche die die Grenzen und Unterschiede zwischen Vertrauen, Transparenz, Erklärbarkeit, Rechenschaftspflicht und Verantwortung in der KI kritisch beleuchten soll.



RADIOINTERVIEW MIT CBC RADIO ZU MASCHINENBEWUSSTSEIN

Ein *Google-Ingenieur* hat behauptet, dass eine künstliche Intelligenz, an der er gearbeitet hat, ein *Bewusstsein* hat. Viele Wissenschaftler sind anderer Meinung, sagen aber, dass die Geschichte andere Bedenken aufwirft. Zusammen mit Christoph Koch und Susan Schneider, hat Marisa Tschopp die Thematik bei der Radiosendung *The Current* auf *CBC Radio*, das meistgehörte Radioprogramm Kanadas, diskutiert.



INTERVIEW ZU ONLINE-ZAHLUNGEN ÜBER RUSSLAND

Mit dem Einmarsch der russischen Armee in der Ukraine sind verschiedene wirtschaftliche Sanktionen einher gegangen. Ob diese im Fall eines Online-Händlers ebenso gerechtfertigt sind, diskutiert Marc Ruef mit dem Journalisten Marcel Urech. Im Interview auf *20 Minuten* wird von einem Beispiel berichtet, bei dem der Checkout einer Online-Bestellung über *Yookassa* in Russland umgesetzt wird.

Weitere News zu unserem Unternehmen finden Sie auf unserer Webseite.

SCIP BUCHREIHE

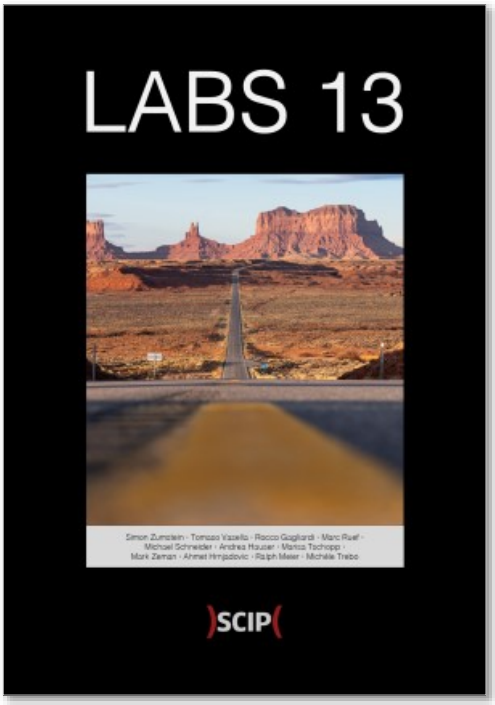
UNSER NEUES JAHRBUCH

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]

BEWAHREN SIE STETS EINEN KÜHLEN KOPF

Bildquelle: https://pixabay.com/images/id-6724514/

LENA CSOMOR, ANDREA HAUSER, MICHAEL SCHNEIDER

AREA41 2022 EIN RÜCKBLICK

Die diesjährige Area41 findet im bekannten Zürcher Nachtklub Kaufleuten statt. Nach zwei Jahren Zwangspause herrschen gute Laune und rege Gespräche. Die Besucher sind offensichtlich erfreut, ihre Netzwerke in Person wieder aufleben zu lassen.

BEGRÜSSUNG

Bereits am Eingang erhalten die Besucher den ersten Swag des Tages: Der Badge ist ein goldener Coin mit verborgener Challenge im Design. Mit Goodie-Bag in der Hand geht es gleich weiter zum Sponsoren- und Networkingbereich wo Gipfeli und Kaffee auf die treuen Jünger der 3-2-1-Regel (3 Stunden Schlaf, 2 Mahlzeiten, 1 Mal Duschen) warten. Ein Gong lädt die Teilnehmer ein, im Präsentationssaal Platz zu nehmen. Die bereits leicht schwitzende Meute stellt erleichtert fest, dass dieser gut klimatisiert und mit ausreichend Wasserflaschen versehen ist. Dann wird die lang ersehnte Konferenz von Candid Wüst, Stefan Friedli und Adrian Wiesmann eröffnet. Wir erfahren, dass das leuchtende LED-Armband aus dem Swag-Bag über 433 MHz kontrolliert werden kann, was prompt zu einer aufgeregten Blinkerei der über 300 Armbändern im Saal führt.

John Salomon: It's All About Risk

Der erste Talk wird von John Salomon gehalten, einem offensichtlich erfahrenen und charmanten Schnellsprecher. Er erklärt, wie man auf C-Level dem Management klar macht, weshalb Security Budget braucht und was ohne dieses passiert. Mit einer klugen CYA-Strategie kann sich der Security-Experte auf vorhandene Gesetze und Policies stützen, um ein Modell zu kreieren, welches die Konsequenzen unter verschiedenen (Budget-)Inputs aufzeigt. Die Diskussion lässt sich damit auf ein regulatorisches Problem reduzieren, welches nota bene nicht mehr Sache der Techies ist und so erfolgreich an ein hoffentlich verhandlungssicheres Legal-Team abgeschoben ist. Er erwähnt jedoch auch, dass ein gewisses Minimum an technischem Verständnis im zuständigen C-Level (meistens wohl der CISO) heutzutage unabdinglich ist. Dem kann man sich nur anschliessen.

Florian Egloff: Pirates, privateers, and mercantile companies in cybersecurity

Nach einer Kaffeepause folgt Florian Egloff mit einer Vorstellung seines Buches über "Semi-State Actors in Cyber Security". Nach einem Exkurs über Hochsee-

politik und -sicherheit in der Kolonialzeit erklärt uns der "Head of Cyber" die Ähnlichkeiten zwischen Söldnern, Piraten, Händlern und Hackern, organisiertem digitalen Verbrechen und den gigantischen Tech-Firmen. Die Gemeinsamkeiten bilden sich aus den riesigen und verteilten Ressourcen in privater Hand, gegen die sich der öffentliche Sektor mit seiner grossen Angriffsfläche kaum verteidigen kann. Das führt dazu, dass der öffentliche Sektor genau jene Ressourcen anheuern muss, um sich zu helfen, denn die benötigten Skillsets befinden sich hauptsächlich im höchstens halbstaatlichen Bereich. Der Hauptunterschied findet sich wohl darin, dass hacken meistens um einiges bequemer ist als kämpfen auf hoher See, sowie sich die gefragten Skills vom Muskelgedächtnis zu deklarativen Prozessen gewandelt hat.

Desiree Sacher-Boldewin: The Intelligent Process Lifecycle of Cyber Defenders – The Extended Version

Das erste, was wir über Desiree erfahren, ist dass sie falschpositive Ergebnisse hasst und eine grosse Freude an KPIs hat. Sie bietet uns ein interessantes Framework zur erfolgreichen, nachhaltigen Sicherheit an, welches durch intelligente Prozesse, effiziente Workflows und Erkennungsmechanismen weit verbreitete Schwierigkeiten in dem Gebiet lösen soll. Sie führt uns durch Prozesse für die Einschätzung von Gefahren, Verwundbarkeiten, Aktionen und mehr. Ein wichtiges Take-Away ist ihre Einteilung von möglichen Aktionen im Falle eines Angriffs oder einer entdeckten Verwundbarkeit. Sie unterteilt dabei in aktive und passive Aktionen. Dabei sind die aktiven "deny, degrade, disrupt, deceive, destroy" und die passiven "detection, discover" gut zu merken und ziemlich selbsterklärend.

Lunch

Die Aussicht auf Futter führt zu einer leichten Aufregung im Saal, und man geht mit knurrendem Magen gesittet zum Ausgang.

Tobias Ospelt: Improving Web Application Scanning

Ein in der lokalen Branche bekannter Retter diverser Pentests und Pentester präsentiert uns seine neueste Extension für Burp Suite, welches bestimmte Requests bzw. Veränderungen an denselben möglich macht. Nach Tobias hat der eingebaute Scanner von Burp Suite einige Problemzonen, die sich auch mit

geschickten Konfigurieren nicht umgehen lassen. Er führt uns durch seinen Arbeits- und Implementationsprozess, seine Kompatibilitätsschwierigkeiten mit Burp Suite, die Wichtigkeit von Wiederholbarkeit von Requests und vieles mehr. Die abschliessende Demo zeigt nochmal mit Nachdruck wie beeindruckend seine Arbeit ist und wie wichtig die neue Extension PentagridScanController für Pentester werden könnte.

Tamas Jos: Hacking from the Browser

Ein Highlight jagt das nächste: Tamas zeigt sein selbstkreiertes Tool OctoPwn, welches einem viele wichtige Anwendungen für Pentesting direkt in einem Browser zur Verfügung stellt. Nur ein winzig kleines Binary muss lokal ausgeführt werden. OctoPwn begeistert das Publikum: Tamas hat einige bekannte Anwendungen wie Bloodhound komplett nochmals selbst implementiert, um sie im Browser anzubieten. In einer Demo zeigt er, dass er sogar den ganzen RDP Stack im Browser zur Verfügung hat, und damit sogar einen visuellen Zugriff auf ein fremdes Gerät zur Verfügung stellen kann. Sehr zum Leidwesen des benachbarten Tesla-Stores beweist Tamas zusätzlich, dass das schlanke OctoPwn sogar auf dem Display eines Autos funktioniert.

Daniel Fabian: Building a Red Team – The Best Defense is a Good Offense

Als letzter vor dem nächsten Koffeinschub folgt Daniel Fabian von Google. Er präsentiert die Qualitäten von internen Red Teams und ihre Aufgabenbereiche, wie sie sich vorbereiten, zusammensetzen und worauf als Manager eines solchen Teams zu achten ist. Eine besondere Schwierigkeit ist, dass Red und Blue Teams einander vertrauen und kollaborieren, ohne dass durch die wiederholten Angriffe Frustration entsteht. Daniel erwähnt auch wiederholt, dass frische, diverse Inputs wichtig sind, um beim Angreifen gut bekannter Systeme neue Angriffsvektoren zu finden. Google rotiert deshalb regelmässig Mitarbeiter zwischen den Security Teams. Während ein “Attacker Mindset” zwar eine wichtige Grundlage für einen Red Teamer ist, kreiert dieses alleine keinen Mehrwert für die Firma – Daniel betont, wie wichtig gutes Reporting und Aufarbeitung der Angriffe ist, sowohl während wie auch nach dem Angriff.

Coffee Break

Obwohl anfangs Vorbehalte gegenüber der "neuen" verfügbaren Mate-Sorte zu vernehmen waren, scheint sich Entzug schnell genug über persönliche Präferenzen gestellt zu haben, um den Mate-Kühlschrank unterdessen zu leeren. Nur schnelle Refills durch das unermüdliche und grossartige Service-Personal vermögen drohende Katastrophen abzuwenden. Was eine solche Menge an Zuckerzufuhr mit Bauchspeicheldrüsen und Arterien anstellt, mag man sich an dieser Stelle lieber nicht vorstellen.

Frank Boldewin: Subverting ProBase security for fun and profit – A sophisticated ATM blackboxing case

Der aufmerksame Leser möchte nun sicher gerne wissen, wie aufwändig es wohl ist, einen Geldautomaten zu knacken (nein, nicht sprengen). Der Talk von Frank wurde nicht aufgezeichnet, weshalb wir hier auch keine weiteren Details verraten werden. Es sei aber gesagt – die Attacke ist enorm aufwändig und ziemlich kurzlebig. Es gibt diverse einfachere und risikoärmere Arten von Diebstahl.

Security Content Creator Panel

Im Panel befinden sich Robbe van Roey, Carl Svensson und Thomas Roth. Sie alle kreieren "content", in ihrem Fall Videos und Streams, im Internet. Das Panel ist eine lebendige Diskussion, an der sich auch das Publikum mit reichlich Fragen beteiligt. Die Vor- und Nachteile der jeweiligen Videoformate werden besprochen, ebenso der bewegten Bilder über Text. Die drei jungen Männer sind ausserdem mit unterschiedlichen Ausmassen an Internethass konfrontiert: Sie sind sich einig, dass dieser durch den sehr technischen Inhalt ihrer Formate und ihrem männlichen Geschlecht jedoch eher schwach ausgeprägt ist – Robbes Freundin, die einen ASMR Channel betreibt, habe trotz geringerer Reichweite mit einem ungleich höherem Ausmass an Hass und Belästigung zu kämpfen, erwähnt Robbe. Die Diskussion entwickelt sich dann in Richtung Geld und Gesetz. Thomas erwähnt, dass er jeweils sehr genau überlegen muss, welche Geräte er im Internet auseinandernimmt. Die Gefahr, von einer Marke verklagt zu werden, ist hoch. Umgekehrt müssen sich alle drei genauso gut überlegen, von welchen Firmen sie Sponsorships annehmen wollen und ob und welche Werbung sie machen möchten. Sie sind sich einig, dass Content

Creation mehr Spass macht, wenn man nicht von Einnahmen abhängig ist und sich seine Inhalte selbst aussuchen kann. Sie debattieren aber auch, dass sie sehr überlegt Zielgruppen ansprechen wollen und müssen, um nicht aus Versehen Inhalte hochzuladen, die aus Sicht der Plattform gefährlich sind und darum gesperrt werden. Zuletzt stellt jeder seine nächsten hochinteressanten Projekte vor. Es bleibt spannend!

BBQ

Zum Abschluss des Tages folgt das von Candid angekündigte BBQ, angeboten vom beliebten Sternengrill aus Zürich.

AREA41 TAG 2

Der zweite Tag beginnt ein wenig später als der erste, und entsprechend fit wirken die Teilnehmer. Erneut wird reichlich Kaffee und Gipfeli gereicht und auch der Mate-Kühlschrank ist wieder gut gefüllt, mit einer wiederum anderen Sorte. Die Mate-Kenner haben ihre Scheu wohl abgelegt und die Neugier hat gesiegt, denn der Bestand reduziert sich rasch.

Dobin Rutishauer: Develop your own RAT – EDR + AV defense

Der Freitag präsentiert sich von Anfang an technisch. Dobin schlägt sich trotz Wackelkontakten souverän und führt uns durch den Entwicklungsprozess seines Remote Access Tools antium, welches er zur Übersicht erst mal in der Killchain einordnet. Er erklärt die Wahl der Programmiersprache und des Kommunikationschannels und präsentiert Teile seiner Architektur. Dabei fällt auf, wie systematisch und geordnet er vorgeht: Sein Testing-Cycle wirkt durchdacht und von seiner Sorgfalt könnte wohl mancher eine Scheibe abschneiden. Dann geht Dobin dazu über, seine AV-Evasion zu präsentieren: Signature Scanning, Detect-On-Load und weiteres werden von ihm an- und umgangen. Die abschliessende Frage, die er sich selbst im Prozess wohl häufig gestellt hat: “Ist es wert, sowas selber zu machen?” Gemäss Dobin nur, wenn man es auch aus Passion tut.

Dagmawi Mulugeta: Command & Control Freak: Cloud Edition

Als nächstes folgt Dagmawi mit einer sehr modernen Attacke: C&C via Missbrauch von Cloud-

Anwendungen wie Google Drive, Dropbox oder sogar Messengers wie Slack und Telegram. Gemäss Dagmawi sind solche Attacken mit minimalem Setup machbar, und es gibt mehrere Subtechniken, die uni- und bidirektionale Kommunikation oder einen sogenannten Dead Drop Resolver benutzen. In den letzten 2 Jahren wurden 23 solche Attacken entdeckt, aber man darf von einer Dunkelziffer ausgehen. Es zeigen sich klare Trends bezüglich der bevorzugten Cloud-Anwendung hin zu Dropbox und Google Drive. Was die Attacke mitunter so effektiv macht, ist das der verursachte Traffic gut im regulären Traffic zu verbergen ist, vorausgesetzt das Opfer benutzt diese Anwendung, oder es ist zumindest wahrscheinlich, dass sie benutzt wird. Dagmawi begeistert das Publikum mit gleich zwei Demos, einmal via Dropbox und einmal via Slack. Besonders die Attacke via Slack ist faszinierend, da man sie auf dem Chat Client live verfolgen kann über die Nachrichten, welche die Parteien einander schicken.

Stephan Gerling: Into the Dark – switching off renewable power from everywhere

Wie aus einem Apokalypsen-Film präsentiert sich Stephans Attacke gegen Solarstromanlagen. Er fand eine Schwachstelle in Solar Power Inverters die ihm eine RCE auf den Geräten ermöglichte. Mit Shodan stellte er fest, dass er mit dieser Schwachstelle 16'000 Solaranlagen angreifen konnte, was einen Verlust von 2.8 GW Strom in Deutschland bedeuten würde. Die Schwachstelle ist unterdessen bekannt und ein Patch ist vorhanden, allerdings scheint es viele Systeme zu geben, die nicht regelmässig gepatcht werden. Da das deutsche Stromnetz über genügend Backup-Power verfügt reichen die von ihm kontrollierten 2.8 GW noch nicht für ein Blackout. Von dem liess sich Stephan nicht beirren und suchte einen zweiten Vektor, um die Attacke zu verstärken. Die meisten Anlagen von Elektrokonsumenten verfügen über Load-Shedding. Dies erlaubt den Elektroproduzenten in einem Notfall das schrittweise herunterfahren von den grössten Stromfressern. Durch die unverschlüsselte Kommunikation auf einer spezifischen Frequenz mit einem öffentlichen Protokoll kann sich jedoch jeder Hobby-Bastler für 300 Euro an dem Spass des Load-Sheddings beteiligen und in die Kommunikation reinfunken. Licht aus, Vorhang zu.

Lunch

Candid verkündet, dass der Lunch-Prozess ein Update erhalten hat und nun sogar zwei Buffets zur Verfügung stehen, damit sich keine Ungeduld breit macht. Wir werden gut versorgt und gönnen uns reichlich Nachspeise in Form von Küchlein, Früchten und Glace.

Niklas Brymko, Simon Scannell, Carl Smith: Counter-Strike: Global Offsets – A Journey into Exploiting the Source Engine

Die drei Männer präsentieren ihr Pandemieprojekt, für welches sie 15'000 Franken Bug Bounty erhalten haben: Sie hacken die Kommunikation vom Server zum Client in Counter-Strike. Zur Hilfe nehmen sie veralteten, geleakten Source Code und stellen fest, dass Counter-Strike sehr viel Legacy Code mit sich herumschleppt. Sie finden einen Weg, ein Feature, bei dem Spieler Maps on-demand herunterladen, auszunutzen indem sie den Parser des Content-Length Headers austricksen, um ASLR zu umgehen. In einer Demo zeigen sie, wie sie mit dem Exploit den Taschenrechner auf einem Client öffnen. Ehemalige und aktuelle Counter-Strike Spiele geraten bei diesem Anblick wohl ein wenig ins Schwitzen.

Philipp Mao: No Passwords more Problems

Philipp hat sich die Anwendungen von Drittanbietern zum passwortfreien Einloggen in Windows vorgenommen. Er zeigt, dass eine der kritischsten Designentscheidungen das Cachen von Logindaten ist – und zwar ob, wann, wo und wie. Auch die angebotenen Funktionalitäten lassen auf mehr oder weniger Sicherheitsprobleme schliessen. Besonders wenn die Funktion "Run as different user" für Windows mit der Anwendung möglich ist, gibt es ein Problem, denn dann sind die heiklen Daten auch von einem normalen Benutzerprozess erreichbar. Philipp demonstriert uns sein erworbenes Wissen an drei Produkten, Veridium AD, Thales SafeNet und Hypr. Beide weisen wesentliche Schwachstellen auf. Speziell bei Hypr, wo eine Nonce die Nutzung eines gestohlenen Client-Zertifikates verhindern sollte, lässt sich diese mit etwas Geschick und Geduld wiederholen. Dazu kommen statische Diffie-Hellman Parameter, und Philipp hat freies Spiel.

Coffee Break

Es folgt die letzte Coffee Break des Tages, aber mit den Highlights ist es noch nicht vorbei!

Michael von Tessin, Alexander Maksyagin: A proprietary security protocol for hearing aids

Michael und Alexander haben sich einem ganz besonderen Problem gewidmet: sie müssen die Kommunikation zwischen smarten Hörgeräten und gekoppelten Computern beziehungsweise Smartphones sichern. Da die Geräte mehr können und brauchen als BLE, aber zu wenig Power für schwere kryptographische Operationen haben, muss ein neues Protokoll her. Die beiden präsentieren ein ausgehöhltes TLS Protokoll, bei dem sie alle Features, die sie nicht brauchen, rausgestrichen haben. Damit sie ihre Nutzer nicht gefährden, lassen sie das Protokoll zudem von der ETH mit dem Tamarin Prover formal verifizieren. Wer das Äffchen kennt, weiss aber auch um seine Limitierungen – insbesondere muss derjenige hinter dem Computer genau wissen, welche Eigenschaften das Protokoll aufweisen muss, bevor Tamarin diese verifizieren kann. Ausserdem kommen kritische Stimmen aus dem Publikum, die darauf hinweisen, dass die Implementierung des Protokolls ein mindestens genauso grosses Problem darstellen kann. Michael und Alexander scheinen aber sehr reflektiert mit dem Thema umzugehen und anerkennen die Probleme. Auch wirkt ihr Vorgehen strategisch und sorgfältig – was man von den Entwicklern der attackierten Software im nächsten Talk definitiv nicht behaupten kann.

Max Moser: How a smart conferencing device turned into a security nightmare

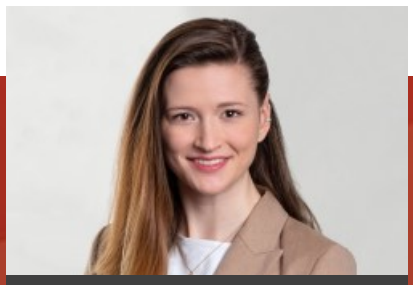
Der letzte Talk bringt noch einmal einige Lacher ins Publikum. Max hat sich die beliebte Meeting Owl vorgeknöpft, die sich mit so ziemlich allem irgendwie verbinden lässt. Zwar sind gewisse Funktionen durch einen Passcode geschützt, aber Max findet sowohl einen Weg, diesen zu umgehen, wie auch eine Backdoor, welche ihm vom Support prompt selbst mitgeteilt wurde. Was folgt, macht schon etwas mulmig: Innert kürzester Zeit findet Max Wege, Leute zu belauschen, ihnen zuzuschauen, sie zu lokalisieren und ihre Netzwerke zu infiltrieren. Die Meeting Owl präsentiert sich als Spion für jedermann. Max gibt die Probleme an die Firma weiter, doch diese reagiert sehr zögerlich. Erst, als Max die Ergeb-

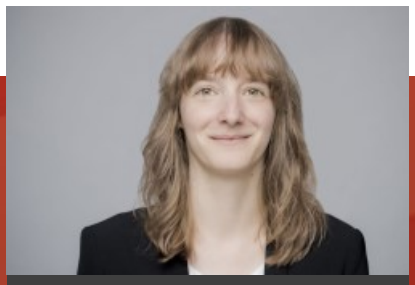
nisse veröffentlicht, kommen erste Fixes von allerdings fragwürdiger Qualität. Bis auf weiteres eignet sich das Gerät darum mehr für Lauschangriffe als für eigene Businessmeetings.

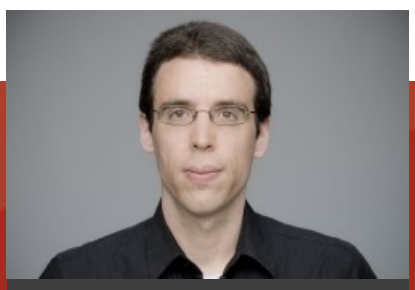
Closing Ceremony

Der Tag neigt sich dem Ende zu und Candid spricht Danksagungen an die fleissigen Helfer, Sponsoren und das Personal des Kaufleuten. Auch das Rätsel um den Badge wird aufgelöst, sowie einige Gutscheine verlost. Die Organisatoren gehen auch auf erhaltenes Feedback ein, welches sich hauptsächlich um Futter dreht – Schlange zu lang, zu wenig Mate (trinkt hier auch jemand Wasser?), am BBQ zu wenig Auswahl, ausserdem hat der Badge offenbar nicht genug geblinkt. Nach all der Arbeit kann einem das Organisationsteam an diesem Punkt ein wenig leidtun, das Publikum scheint wirklich anspruchsvoll zu sein. Das Team gelobt Besserung – falls es ein Area41 2024 geben sollte.

Wir finden, der Event ist sehr gelungen, trotz der Hitze blieb das Klima drinnen immer angenehm, wir wurden grosszügig ver- und umsorgt und haben viel gehört, gelernt und geschwatzt. Danke, Defcon Switzerland!

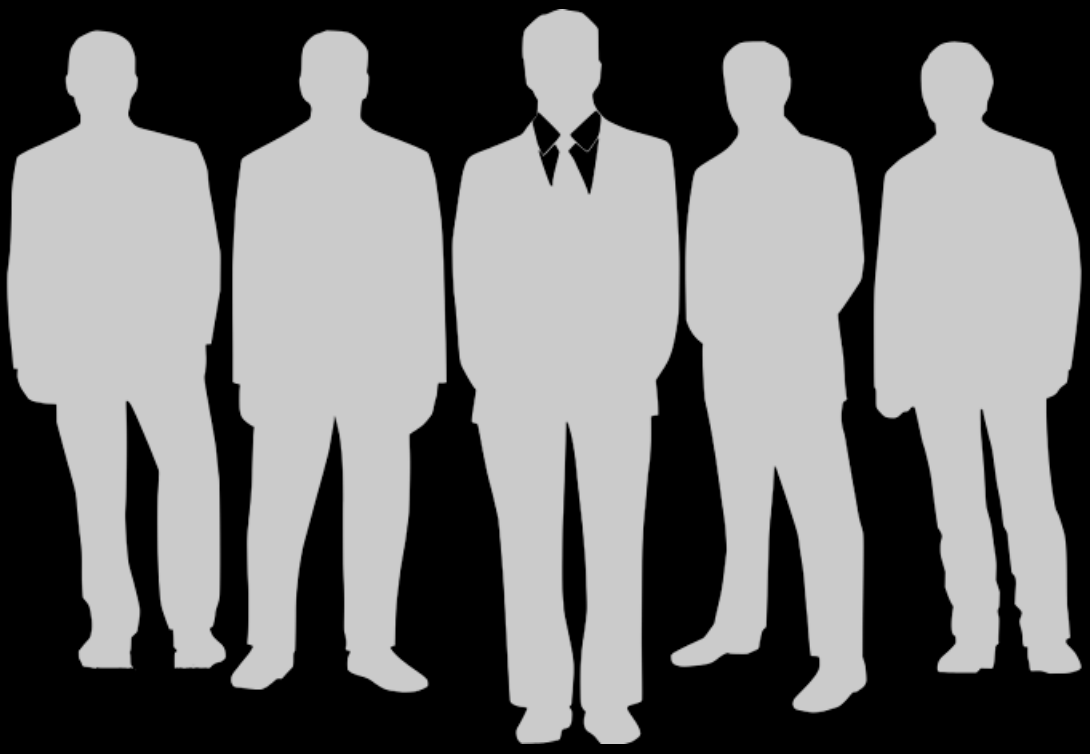

Lena Csomor


Andrea Hauser


Michael Schneider

next gen vulnerability intelligence

VulDB



Werden Sie Teil der Community

Welche Schwachstellen betreffen die bei Ihnen eingesetzten Software-Produkte? Welches Risiko geht von ihnen aus? Muss man diese adressieren? Und falls ja, wie? Die mehrsprachige Verwundbarkeitsdatenbank VulDB wird durch eine aktive Community unterstützt, die neue Schwachstellen dokumentiert und bestehende Einträge aktualisiert. Seien Sie einen Schritt voraus!

)SCIP(
official data provider

> https://vuldb.com

ANDREA HAUSER

HTTP/2 REQUEST SMUGGLING EINFÜHRUNG

Im vorhergehenden Artikel wurden die Grundlagen des *Request Smugglings* erklärt. Diese werden für die nachfolgenden Erklärungen notwendig sein, wer Request Smuggling noch nicht kennt, sollte also zuerst den Artikel zu Request Smuggling – Beschreibung und Vorgehen beim Testen lesen.

HTTP/2 ist ein *binäres Protokoll*. Dabei werden HTTP/2-Nachrichten in einem, bis mehreren Frames versandt und jeder Frame hat eine explizite Länge, die dem Server vorgibt, wie viele Bytes gelesen werden sollen. Die Länge einer HTTP/2-Nachricht wird dementsprechend berechnet in dem die Länge aller Frames aufsummiert wird. Diese Länge kann *nicht manipuliert* werden. Nun stellt sich die Frage, wie in HTTP/2 dennoch Request Smuggling entstehen kann, wenn die Länge der Frames nicht manipuliert werden kann, da diese Manipulation der Länge bei HTTP/1.1-Anfragen die Voraussetzung für das Request Smuggling war. Grundsätzlich entsteht HTTP/2 Request Smuggling nur dann, wenn das Front-End HTTP/2 spricht, das Back-End allerdings nicht. Dann muss das Front-End die HTTP/2-Anfrage für das Back-End *in eine HTTP/1.1-Anfrage umwandeln*. Hier entstehen dann neue Möglichkeiten für Manipulationen.

Da HTTP/2 ein binäres Protokoll ist, werden hier abstrahierte und vereinfachte Darstellungen verwendet, um die Konzepte aufzuzeigen. Die einzelnen Frames werden *nicht* aufgezeigt. In HTTP/2 existieren sogenannte *Pseudoheader*. Diese werden für den weiteren Verlauf des Artikels wie folgt definiert und mit einem Doppelpunkt vor dem Namen als solche gekennzeichnet:

- :method — Entspricht der Request Methode.
- :path — Entspricht dem Request Pfad inklusive möglichen Parametern.
- :authority — Entspricht ungefähr dem Host Header.
- :scheme — Entspricht dem Request Schema und ist im Normalfall http oder https.
- :status — Entspricht dem Response Status Code und wird in Requests nicht verwendet.

Am einfachsten ist es diese Header im Einsatz zu sehen im Vergleich zur gleichen Anfrage in HTTP/1.1 und HTTP/2.

HTTP/1.1 Request

```
POST /test HTTP/1.1\r\n
Host: example.com\r\n
User-Agent: test\r\n
Content-Length: 3\r\n
\r\n
x=1
```

HTTP/2 Request

```
:method POST
:path /test
:authority example.com
:scheme https
user-agent test
x=1
```

Mit den Grundlagen abgedeckt können nun die HTTP/2 Request Smuggling-Schwachstellen angegangen werden.

H2.CL Schwachstelle

Diese Schwachstelle funktioniert vom Prinzip her ähnlich wie die TE.CL Schwachstelle aus dem letzten Artikel, allerdings verwendet das Front-End HTTP/2, *ignoriert* den *Content-Length* Header und gibt ihn unverändert an das Back-End weiter. Das Back-End verwendet HTTP/1.1 und interpretiert daher den *Content-Length* Header. In einem Beispiel sieht der Angriff wie folgt aus.

```
:method POST
:path /test
:authority example.com
content-type application/x-www-form-urlencoded
content-length 0
Injected
```

Da das Back-End die Verarbeitung der Anfrage aufgrund der *Content-Length* von 0 früher beendet, als das Front-End geschickt hat, bleibt der *Rest* der Anfrage *in der Pipeline* zwischen Front-End und Back-End bestehen. Sobald eine nächste Anfrage eintrifft, wird der noch in der Pipeline vorhandene Rest der vorherigen Anfrage vor dieser neuen Anfrage hinzugefügt. Eine neue Anfrage würde im Back-End also wie folgt aussehen.

```
InjectedGET /user-requested HTTP/1.1
Host: example.com
H2.TE Schwachstelle
```

Ähnlich wie bei der oben beschriebenen Schwachstelle verwendet das Front-End HTTP/2, *ignoriert* den

Transfer-Encoding Header und gibt ihn unverändert an das Back-End weiter. Das *Back-End* verwendet HTTP/1.1 und *interpretiert* daher den *Transfer-Encoding* Header. In einem Beispiel sieht der Angriff wie folgt aus.

```
:method POST
:path /test
:authority example.com
content-type application/x-www-form-urlencoded
transfer-encoding chunked
0

GET /admin HTTP/1.1
Host: example.com
Foo: Injected
```

Da das Back-End die Verarbeitung der Anfrage aufgrund des Transfer-Encoding von 0 früher beendet, als das Front-End geschickt hat, bleibt der Rest der Anfrage in der Pipeline zwischen Front-End und Back-End bestehen. Sobald eine nächste Anfrage eintrifft, wird der noch in der Pipeline vorhandene Rest der vorherigen Anfrage vor dieser neuen Anfrage hinzugefügt. Eine neue Anfrage würde im Back-End also wie folgt aussehen.

```
POST /test HTTP/1.1
Host: example.com
Content-Type: application/x-www-form-urlencoded
Transfer-Encoding: chunked

0
--> Anfrage eins endet hier
GET /admin HTTP/1.1
Host: example.com
Foo: InjectedGET /user-requested HTTP/1.1
```

Request Smuggling mit CRLF-Injektion

Da HTTP/2 und HTTP/1.1 nicht auf der gleichen Basis interpretiert werden, da *HTTP/2* ein *binäres Protokoll* ist und *HTTP/1.1 String-basiert* ist, können diese Unterschiede ausgenutzt werden. In einem HTTP/2 Header können zum Beispiel problemlos *Zeilenumbrüche* genutzt werden, da diese nicht speziell interpretiert werden. Das heisst aus einem im Front-End als ein Header interpretierten Header können im Back-End mehrere Header werden. Zum Beispiel wäre

```
Testheader: Test\n\rInjected
```

im Front-End ein Header, würde im Back-End allerdings wie folgt aussehen

```
Testheader: Test
Injected
```

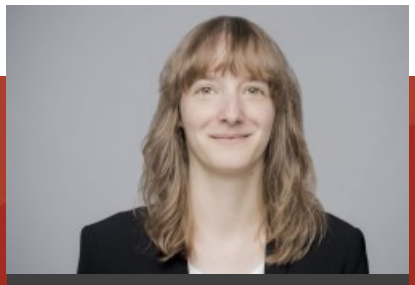
Danke der ausgezeichneten Forschung von James Kettel können die oben beschriebenen Angriffe in der Web Security Academy nachgespielt werden.

GEGENMASSNAHMEN

Diese Schwachstelle kann, wie zu Beginn bereits angedeutet, am einfachsten verhindert werden, in dem *durchgehend HTTP/2 eingesetzt* wird. Falls dies nicht möglich ist, muss darauf geachtet werden, dass bei der Umwandlung in einen HTTP/1.1 Request keine Header wie Content-Length oder Transfer-Encoding und keine Spezialzeichen wie \r\n und : übernommen werden.

FAZIT

Bei der Umstellung auf HTTP/2 im Front-End Server kann *unbewusst* eine *weitreichende Schwachstelle* eingeführt werden, wenn sich die HTTP/2 und die HTTP/1.1 sprechenden Server nicht einig sind, wo die Grenze des Requests sind. Die Auswirkungen von Request Smuggling könne das unberechtigte Lesen von Responses von anderen Benutzern, das Einfügen von beliebigem JavaScript in beliebige Responses von Benutzern, sowie das vollständige Stören eines normalen Betriebs einer Webseite sein. Die Behebung ist vergleichsweise einfach, wenn der Back-End Server ebenfalls auf HTTP/2 umgestellt werden kann. Ansonsten benötigt es eine sorgfältige Umwandlung der Requests, um keine Schwachstellen einzuführen.



Andrea Hauser

HERAUSFORDERUNGEN WERDEN STETS AUCH ZU CHANCEN

Bildquelle: https://pixabay.com/images/id-6917552/

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

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.

scip AG
Badenerstrasse 623
8048 Zürich
Schweiz

+41 44 404 13 13
www.scip.ch