Version 1.0 Montag, 31. Dezember 2018

Chaos Communication Congress 35C3 in Leipzig vom 27.12.2018 - 30.12.2018. - Eine Vortragsauswahl.

Alle ca. 169 Vorträge sind unter https://media.ccc.de/c/35c3 abrufbar. Sprache kann umgeschaltet werden. Zum Umschalten im Video = Klick auf das Zahnrad 

- Opening Event - Refreshing Memories
  - https://media.ccc.de/v/35c3-9985-opening_event

- Mind the Trap: Die Netzpolitik der AFD im Bundestag
  - https://media.ccc.de/v/35c3-9513-mind_the_trap_die_netzpolitik_der_afd_im_bundestag

- Hackerethik - eine Einführung
  - https://media.ccc.de/v/35c3-10011-hackerethik_-_eine_einfuhrung

    Die Hackerethik ist die Grundlage für den Umgang mit den diversen ethischen Problemen, die sich beim schöpferisch-kritischen Umgang mit Technologie (auch "hacking" genannt) stellen. Sie bietet Anhaltspunkte für die alltäglichen Fragestellungen und Probleme, die aufkommen, wenn man Technologie anders benutzt, als der Hersteller es sich gedacht hat, wenn man Lücken in Systemen findet und ausnutzt oder über Berge von persönlichen Daten stolpert. Dieser Talk gibt eine Einführung in die verschiedenen Aspekte der Hackerethik und regt zum Nachdenken über die ethischen Fragen an, die sich Menschen mit speziellen Fähigkeiten und Fertigkeiten stellen, wenn sie ihren Neigungen nachgehen.

- All Your Gesundheitsakten Are belong to us
  - https://media.ccc.de/v/35c3-9992-all_your_gesundheitsakten_are_belong_to_us

    Plötzlich geht alles ganz schnell: Online-Behandlungen und elektronische Gesundheitsakten sind dieses Jahr für Millionen Krankenversicherte Wirklichkeit geworden. Zu einem hohen Preis: Bereits einfache Angriffe lassen das Sicherheitskonzept der Apps und Plattformen zusammenbrechen. Warum das so ist, welche kritischen Fehler Vivy & Co. gemacht haben und wie das möglicherweise verhindert werden kann, das soll dieser Vortrag zeigen - denn in spätestens drei Jahren sollen auch die Gesundheitsdaten aller übrigen Versicherten zentral gespeichert und online abrufbar sein.
    Die elektronische Gesundheitskarte ist gescheitert. Stattdessen kommt jetzt die elektronische Patientenakte: In spätestens drei Jahren sollen die Befunde, Diagnosen, Röntgenbilder und Rezepte aller gesetzlich Krankenversicherten online und zentral gespeichert verfügbar sein. Schon heute können Millionen Versicherte eine solche Lösung nutzen und, wie Gesundheitsminister Jens Spahn fordert, "auch auf Tablets und Smartphones auf ihre elektronische Patientenakte zugreifen". Zeitgleich zur elektronischen Patientenakte steht die Onlinebehandlung vor der Tür: Das Fernbehandlungsverbot wurde vor wenigen Monaten gekippt, und schon heute können sich Millionen Versicherte ausschließlich online behandeln lassen.

    Nach Jahren des Wartens geht dabei alles ganz schnell. "Diese Maßnahmen dulden keinen Aufschub", sagt Spahn. Und macht uns alle damit zu Beta-Testern in Sachen Gesundheit. Mit fatalen Folgen: Unsere streng vertraulichen Gesundheitsdaten liegen für alle sichtbar im Netz.
    In diesem Vortrag zeige ich an fünf konkreten Beispielen, welche fahrlässigen Entscheidungen die Online-Plattformen und Apps der Anbieter aus dem Bereich Gesundheitsakte und Telemedizin so angreifbar machen und demonstriere, wie einfach der massenhafte Zugriff auf unsere vertraulichen Gesundheitsdaten gelang. Zur Debatte steht, was angesichts dieser neuen alten Erkenntnisse zu tun ist - und was wir besser bleiben lassen.

- Venenerkennung hacken
  - https://media.ccc.de/v/35c3-9545-venenerkennung_hacken
  - Vom Fall der letzten Bastion biometrischer Systeme
    Die Venenerkennung ist eine der letzten Bastionen biometrischer Systeme, die sich bisher der Eroberung durch Hacker widersetzt hat. Dabei ist sie ein lohnendes Ziel, schützt sie doch Bankautomaten und Hochsicherheitsbereiche. In diesem Talk machen wir die Verteidigungsanlagen dem Erdboden gleich.
    Seit Jahrzehnten vor allem im asiatischen Raum eingesetzt sind bisher keine ernsthaften Versuche bekannt Venenerkennungssysteme zu überwinden. Neben dem Mythos der Hochsicherheit sind vor allem die, unsichtbar im Körper gelegenen Merkmale dafür verantwortlich. In diesem Talk werden wir zeigen, mit welch geringem Aufwand man an die "versteckten" Venenbilder gelangen kann und wie, auf Grundlage dieser, Attrappen gebaut werden können, welche die Systeme der beider grosser Hersteller überwinden.

- "The" Social Credit System
  - https://media.ccc.de/v/35c3-9904-the_social_credit_system
  - Why It's Both Better and Worse Than We can Imagine

- How does the Internet work?
  - https://media.ccc.de/v/35c3-10005-how_does_the_internet_work
  - An explanation of Inter-Net and everyday protocols

- What The Fax?!
  - https://media.ccc.de/v/35c3-9462-what_the_fax#t=1

- Schweiz: Netzpolitik zwischen Bodensee und Matterhorn
  - https://media.ccc.de/v/35c3-9590-schweiz_netzpolitik_zwischen_bodensee_und_matterhorn
    Datenreichtum, E-Voting, Massenüberwachung und andere netzpolitische Schauplätze in der Schweiz
    Der Kampf um die Freiheit im digitalen Raum wird auch in der Schweiz intensiver. Wir blicken auf das netzpolitische Jahr 2018 in der Schweiz zwischen Bodensee und Matterhorn zurück. Wir behandeln jene Themen, die relevant waren und relevant bleiben. Weiter zeigen wir, was von der Digitalen Gesellschaft in der Schweiz im neuen Jahr zu erwarten ist.
    Massenüberwachung: Kabelaufklärung und Vorratsdatenspeicherung sowie die Beschwerden, welche die Digitale Gesellschaft in der Schweiz führt.
    E-Voting: Abstimmungen und Wahlen im Internet sowie der Kampf für das Vertrauen in die Direkte Demokratie in der Schweiz.
    Netzsperren: Die Zensur im schweizerischen Internet begann mit «Denkt denn niemand an die Kinder?» und geht nun mit Geldspielen im Internet weiter …
    Urheberrecht: Wie die USA im «Piratenstaat» Schweiz ihre Forderungen durchsetzen, unter anderem mit Massenabmahnungen gegen Filesharing.
    Datenschutz: Wo war in der Schweiz besonders viel «Datenreichtum» zu beobachten?
    Digitale Gesellschaft in der Schweiz: Razzia am «Hort der Linksextremen», Winterkongress und andere Aktivitäten.

- Polizeigesetze
  - https://media.ccc.de/v/35c3-10015-polizeigesetze

  Heimatminister Horst Seehofer und seine Amtskollegen in den Ländern erweitern die Rechte der Polizeien und planen ein „Musterpolizeigesetz“. Damit handelten sie sich die größten Proteste gegen Überwachungsvorhaben seit Jahren ein. Wir geben nicht nur einen Überblick über die zahlreichen Neuregelungen der Polizeigesetze in den Bundesländern, sondern berichten auch aus den Anhörungen in den Landtagen und von den Stellungnahmen. Wir erklären, was in den neuen Gesetzen steht und welche rechtlichen und technischen Grenzüberschreitungen wir zu kritisieren haben. Und wir haben ein paar Forderungen.

- Jahresrückblick des CCC 2018
- https://media.ccc.de/v/35c3-9975-jahresruckblick_des_ccc_2018

  Biometrische Videoüberwachung, Hausdurchsuchungen, Polizeiaufgabengesetze, Staatstrojaner und ganz viel Cyber: Wir geben einen Überblick über die Themen, die den Chaos Computer Club 2018 beschäftigt haben.
  Neben der Zusammenfassung und der Rückschau auf das vergangene Jahr wollen wir aber auch über zukünftige Projekte und anstehende Diskussionen reden.

- G10, BND-Gesetz und der effektive Schutz vor Grundrechten
  - Die strategische Fernmeldeüberwachung des BND vor dem Bundesverfassungsgericht
  - https://media.ccc.de/v/35c3-10016-g10_bnd-gesetz_und_der_effektive_schutz_vor_grundrechten

  Der Vortrag behandelt die Klage des **Internetknotens DE-CIX** gegen die strategische Fernmeldeüberwachung des BND vor dem Bundesverwaltungsgericht in Leipzig, was wir aus dem Urteil über den Rechtsschutz der Bürger lernen können und wieso der Fall nun das Bundesverfassungsgericht in Karlsruhe beschäftigt.

- How Facebook tracks you on Android
  - (even if you don´t have an Facebook account)
  - https://media.ccc.de/v/35c3-9941-how_facebook_tracks_you_on_android
  - https://privacyinternational.org/types-abuse/facebook
  - https://privacyinternational.org
  - https://privacyintyqcroe.onion

  In this talk, we’re looking at third party tracking on Android. We’ve captured and decrypted data in transit between our own devices and Facebook servers. It turns out that some apps routinely send Facebook information about your device and usage patterns - the second the app is opened. We’ll walk you through the technical part of our analysis and end with a call to action: We believe that both Facebook and developers can do more to avoid oversharing, profiling and damaging the privacy of their users.

- Smart Home - Smart Hack
  - https://media.ccc.de/v/35c3-9723-smart_home_-_smart_hack
    - Weitere Infos und Downloads https://www.vtrust.de/35c3

  Wie der Weg ins digitale Zuhause zum Spaziergang wird.
  Mehr als 10.000 unterschiedliche Device-Hersteller aus aller Welt verwenden die Basis-Plattform (WIFI-Modul, Cloud, App) eines einzigen Unternehmens zur technischen Umsetzung ihrer Smart-Home-Produkte.
  Die Analyse dieser Basis zeigt **erhebliche Sicherheitsmängel** auch konzeptioneller Natur und somit **diverse Angriffspunkte**, von denen mehrere Millionen Smart Devices betroffen sind.
  Der Vortrag stellt die Funktionsweise smarter Geräte im Zusammenhang mit der genannten Basis-Plattform dar, zeigt das Ausmaß der Sicherheitslücken anhand diverser Angriffsszenarien und bietet der Community eine Lösung für die sichere Nutzung der betroffenen Geräte.

- Mehr schlecht als Recht: Grauzone Sicherheitsforschung
  - https://media.ccc.de/v/35c3-9898-mehr_schlecht_als_recht_grauzone_sicherheitsforschung

  Reverse Engineering zum Aufspüren von Schwachstellen ist gängige Praxis. Umso überraschender kam für 2 Forschungsteams die Abmahnung durch Rechtsanwälte eines Herstellers. Sie hatten Schwachstellen aufgedeckt und damit, so der Hersteller, seine Rechte verletzt. Vorwurf? Vom Verstoß gegen das Urheberrecht bis zum Verrat von Geschäftsgeheimnissen war alles dabei.
  Nach hunderten Seiten an Schriftsätzen, einem zurückgehaltenen Paper sowie 7 Stunden Marathon-Prozess konnte ein Vergleich geschlossen werden, bei dem wir mit einer Verpflichtung zum Responsible Disclosure davon kamen - die Kernfragen bleiben jedoch offen: Welche Teile des Reverse Engineering sind rechtswidrig? Verstößt Reversing auch zum Zwecke der IT-Sicherheitsforschung gegen das Urheberrechtsgesetz? Was schützt in Zukunft Sicherheitsforscher vor rechtlichen Schritten des Herstellers? Wie können sich Unternehmen verhalten und welche Abwägungen müssen vor der Veröffentlichung getroffen werden?
  Wir berichten vom Ablauf eines solchen Prozesses inklusive Anekdoten, weisen auf die Unklarheiten in geltendem Recht hin und schaffen ein Bewusstsein für die Problematik.

- wallet.fail
  - Hacking the most popular cryptocurrency hardware wallets
  - https://media.ccc.de/v/35c3-9563-wallet_fail#t=1

  In this presentation we will take a look at how to break the most popular cryptocurrency hardware wallets. We will uncover architectural, physical, hardware, software and firmware vulnerabilities we found including issues that could allow a malicious attacker to gain access to the funds of the wallet. The attacks that we perform against the hardware wallets range from breaking the proprietary bootloader protection, to breaking the web interfaces used to interact with wallets, up to physical attacks including glitching to bypass the security implemented in the IC of the wallet. Our broad look into several wallets demonstrates systemic and recurring issues. We provide some insight into what needs to change to build more resilient hardware wallets.
  Hardware wallets are becoming increasingly popular and are used to store a significant percentage of the world's cryptocurrency. Many traders, hedge funds, ICOs and blockchain projects store the entirety of their cryptocurrency on one or very few wallets. This means that users of hardware wallets store tens of millions of euros of cryptocurrency on small USB peripherals that costs only a few euros to manufacture. Moreover, many users that trade and speculate in cryptocurrency interact, update, and generate transactions using their hardware wallets on a daily basis.
  In this talk we look at the good, the bad and the ugly of hardware wallet security: We will walk through the different architectures of the wallets, look at the different attack vectors and talk about the challenges of building secure hardware before diving in deep finding vulnerabilities in the different wallets.
  The vulnerabilities we will present range from vulnerabilities that can be fixed in a firmware upgrade, to bugs that will require a new hardware revision, up to attacks on the microcontrollers themselves, requiring new silicon to be fixed.
  Some of the (most entertaining) vulnerabilities will be demonstrated live on stage.