<?xml version='1.0' encoding='utf-8' ?>

<schedule>

<version>1.5 To shine in a bright light</version>

<conference>

<acronym>31c3</acronym>

<title>31. Chaos Communication Congress</title>

<start>2014-12-27</start>

<end>2014-12-31</end>

<days>4</days>

<timeslot\_duration>00:05</timeslot\_duration>

</conference>

<day date="2014-12-27" end="2014-12-28T04:00:00+01:00" index="1" start="2014-12-27T11:00:00+01:00">

<room name="Saal 1">

<event guid="29aecfd7-2e44-4f49-ab86-29b5e0877325" id="6561">

<date>2014-12-27T11:00:00+01:00</date>

<start>11:00</start>

<duration>00:30</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6561\_-\_en\_-\_saal\_1\_-\_201412271100\_-\_31c3\_opening\_event\_-\_erdgeist\_-\_geraldine\_de\_bastion</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>31C3 Opening Event</title>

<subtitle/>

<track>CCC</track>

<type>lecture</type>

<language>en</language>

<abstract/>

<description/>

<persons>

<person id="1544">erdgeist</person>

<person id="3874">Geraldine de Bastion</person>

</persons>

<links/>

</event>

<event guid="8c4e647f-813e-41ef-b05b-65469dd841c3" id="6571">

<date>2014-12-27T11:30:00+01:00</date>

<start>11:30</start>

<duration>01:00</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6571\_-\_en\_-\_saal\_1\_-\_201412271130\_-\_31c3\_keynote\_-\_alecempire</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>31C3 Keynote</title>

<subtitle>A New Dawn</subtitle>

<track>CCC</track>

<type>lecture</type>

<language>en</language>

<abstract>The 31C3 Keynote</abstract>

<description>A New Dawn</description>

<persons>

<person id="5309">alecempire</person>

</persons>

<links/>

</event>

<event guid="HOqeNIb6G7M4hYFKFRkCmQ" id="6264">

<date>2014-12-27T12:45:00+01:00</date>

<start>12:45</start>

<duration>01:00</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6264\_-\_de\_-\_saal\_1\_-\_201412271245\_-\_wir\_beteiligen\_uns\_aktiv\_an\_den\_diskussionen\_-\_martin\_haase\_maha</slug>

<recording>

<license>cc-by-sa</license>

<optout>false</optout>

</recording>

<title>„Wir beteiligen uns aktiv an den Diskussionen“</title>

<subtitle>Die digitale „Agenda“ der Bundesregierung aus inhaltlicher, philologischer und linguistischer Perspektive</subtitle>

<track>Ethics, Society &amp; Politics</track>

<type>lecture</type>

<language>de</language>

<abstract>Im Sommer 2014 wurde die sogenannte Digitale „Agenda“ vorgestellt, die als „netzpolitisches Regierungsprogramm“ bezeichnet wurde. Aus texttypologischer Sicht handelt es sich aber eher um einen PR-Text, der so aussieht, als sei er ein Auszug aus einer Wahlkampfbroschüre. Der Vortrag analysiert den Text zunächst inhaltlich, um zu zeigen, worum es im Einzelnen geht und wo Widersprüche auftauchen, dann aus textkritischer und aus linguistischer Perspektive. Insbesondere werden bestimmte Interessen der Bundesregierung und anderer Akteure deutlich, die weniger offen thematisiert werden, aber doch sprachlich zu Tage treten.</abstract>

<description>Am 20. August 2014 wurde in Berlin die so genannte Digitale „Agenda“ der Bundesregierung vorgestellt. Das „netzpolitische Regierungsprogramm“ wurde begrüßt, aber viele Kritiker qualifizierten es als „zu wenig, zu spät“. Dabei ist wenigen aufgefallen, dass es sich in Bezug auf die Textsorte um einen PR-Text handelt, der wenig Ähnlichkeiten mit einem Regierungsprogramm hat, sondern eher so aussieht, als stamme er aus einer Wahlkampfbroschüre. Eine textkritische und eine linguistische Analyse ergeben, dass von einer „Agenda“ wenig zu spüren ist, obwohl das Wort „aktiv“ sehr häufig verwendet wird, allerdings in Kontexten, die nichts mit Aktivitäten zu tun haben. Das ist nicht der einzige Widerspruch. Es zeigt sich wieder einmal, dass die Sprache des Textes auch versteckte Interessen an den Tag bringt. </description>

<persons>

<person id="4085">Martin Haase/maha</person>

</persons>

<links>

<link href="http://breitband.deutschlandradiokultur.de/brb140823/">Maha kurz bei Breitband zu diesem Thema</link>

</links>

</event>

<event guid="OQzXwQcnHSLD9Qd7Iu7Rqw" id="6010">

<date>2014-12-27T14:00:00+01:00</date>

<start>14:00</start>

<duration>01:00</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6010\_-\_en\_-\_saal\_1\_-\_201412271400\_-\_scada\_strangelove\_too\_smart\_grid\_in\_da\_cloud\_-\_sergey\_gordeychik\_-\_aleksandr\_timorin</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>SCADA StrangeLove: Too Smart Grid in da Cloud</title>

<subtitle/>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>For two years SCADA StrangeLove speaks about Industrial Control Systems and nuclear plants. This year we want to discuss Green Energy. Our hackers' vision of Green Energy, SmartGrids and Cloud IoT technology.

We will also speak about the security problems of traditional &quot;heavy&quot; industrial solutions, about the things that Zurich Airport and Large Hadron Collider have in common

On top of it you will learn about our new releases, some funny and not so funny stories about discovery and fixing of vulnerabilities and the latest news from the front struggling for the Purity of Essence.​</abstract>

<description>Our latest research was devoted to the analysis of the architecture and implementation of the most wide spread platforms for wind and solar energy generation which produce many gigawatts of it.

It may seem (not) surprising but the systems which manage huge turbine towers and household PhotoVoltaic plants are not only connected to the internet but also prone to many well known vulnerabilities and low-hanging 0-days. Even if these systems cannot be found via Shodan, fancy cloud technologies leave no chances for security.

We will also speak about the security problems of traditional &quot;heavy&quot; industrial solutions, about the things that Zurich Airport and Large Hadron Collider have in common and why one should not develop brand new web server.

Specially for the specialists on the other side of the fences, we will show by example of one industry the link between information security and industrial safety and will also demonstrate how a root access gained in a few minutes can bring to nought all the years of efforts that were devoted to the improvement of fail-safety and reliability of the ICS system.

On top of it you will learn about our new releases, some funny and not so funny stories about discovery and fixing of vulnerabilities and the latest news from the front struggling for the Purity of Essence.​</description>

<persons>

<person id="3530">Sergey Gordeychik</person>

<person id="5274">Aleksandr Timorin</person>

</persons>

<links>

<link href="http://www.scadasl.org">SCADA StrangeLove</link>

<link href="https://twitter.com/scadasl">Twitter</link>

</links>

</event>

<event guid="J9UXjl3ggsIGnkIJSxSxmw" id="6120">

<date>2014-12-27T16:00:00+01:00</date>

<start>16:00</start>

<duration>01:00</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6120\_-\_en\_-\_saal\_1\_-\_201412271600\_-\_practical\_emv\_pin\_interception\_and\_fraud\_detection\_-\_andrea\_barisani</slug>

<recording>

<license>CC-BY-3.0</license>

<optout>false</optout>

</recording>

<title>Practical EMV PIN interception and fraud detection</title>

<subtitle/>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>This talks follows our previous EMV research uncovering new findings as well as a detailed analysis of Chip &amp; PIN fraud markers in order to benefit cardholders, as well as issuing banks, in preventing wrongful liability for fraudulent charges.</abstract>

<description>The EMV global standard for electronic payments is widely used for

inter-operation between chip equipped credit/debit cards, Point of Sales devices and ATMs.

In 2011, our &quot;Chip &amp; PIN is definitely broken&quot; presentation uncovered an EMV design flaw that, by means of chip skimmers, allows for arbitrary PIN harvesting.

Since then, by consulting on EMV implementations and their behaviour under effective attacks, Inverse Path has assisted issuing banks, as well as cardholders, with successful resolution of cases involving wrongful liability for fraudulent charges.

Our updated research effort identifies and verifies new interactions between previous EMV attacks, which even further affect the protection, or lack of, that EMV provides for the PIN.

This presentation aims to fully empower both cardholders and issuers with an understanding of all applicable attacks, while also illustrating the relevant EMV fraud detection markers.

Such information is vital to enable cardholders to request the correct and relevant information necessary to claim fraudulent charges and to enable issuers and processors to prevent fraud in the first place.</description>

<persons>

<person id="4941">Andrea Barisani</person>

</persons>

<links>

<link href="http://dev.inversepath.com/download/emv/emv\_2014.pdf">Slides - Practical EMV PIN interception and fraud detection</link>

</links>

</event>

<event guid="-n9QScyDLXMEwkqrCHASYw" id="6249">

<date>2014-12-27T17:15:00+01:00</date>

<start>17:15</start>

<duration>01:00</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6249\_-\_en\_-\_saal\_1\_-\_201412271715\_-\_ss7\_locate\_track\_manipulate\_-\_tobias\_engel</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>SS7: Locate. Track. Manipulate.</title>

<subtitle>You have a tracking device in your pocket</subtitle>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>Companies are now selling the ability to track your phone number whereever you go. With a precision of up to 50 meters, detailed movement profiles can be compiled by somebody from the other side of the world without you ever knowing about it. But that is just the tip of the iceberg.</abstract>

<description>SS7 is the global telecommunications backbone network. You use it every time you make a call, receive a text message or use the mobile network's internet access. But to be reachable, the network has to know your location. And access to the SS7 network is getting easier and easier, without the security measures keeping up.

As a follow-up to 25C3's &quot;Locating Mobile Phones using SS7&quot; this talk will offer a look at what has changed in the last six years. I will show how easy it is for intelligence services and criminals to circumvent the network's defenses to get the data they want, just based on your phone number.

</description>

<persons>

<person id="1848">Tobias Engel</person>

</persons>

<links>

<link href="http://www.washingtonpost.com/business/technology/for-sale-systems-that-can-secretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8a-f003-11e3-bf76-447a5df6411f\_story.html">Overview of the subject in the Washington Post</link>

</links>

</event>

<event guid="szHEwO2pazLIG7w8wQTa1w" id="6122">

<date>2014-12-27T18:30:00+01:00</date>

<start>18:30</start>

<duration>01:00</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6122\_-\_en\_-\_saal\_1\_-\_201412271830\_-\_mobile\_self-defense\_-\_karsten\_nohl</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Mobile self-defense</title>

<subtitle/>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>We know that mobile networks can — and do — attack us on many fronts. As this talk will show, even 3G is attackable. It’s high time that we upgrade from complaining to self-defense.</abstract>

<description>Modern phones include all components necessary to block — or at least make visible — a large range of attacks including IMSI catchers, SIM exploits, and SMS attacks. The possibility of other attacks, such as passive intercept, can be inferred from measurements that normally remain hidden in a phone’s baseband.

This talk details how these secrets were unlocked through reverse-engineering of the most widely deployed baseband family. We release tools that block or alert users to many common attacks.

We also introduce and demonstrate new attack scenarios — hybrids between local and interconnect abuse — including the passive intercept and decryption of 3G traffic.</description>

<persons>

<person id="1741">Karsten Nohl</person>

</persons>

<links/>

</event>

<event guid="A8xVpIjX1oKQOQcWMt\_49Q" id="6450">

<date>2014-12-27T20:30:00+01:00</date>

<start>20:30</start>

<duration>01:00</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6450\_-\_de\_-\_saal\_1\_-\_201412272030\_-\_ich\_sehe\_also\_bin\_ich\_du\_-\_starbug</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Ich sehe, also bin ich ... Du</title>

<subtitle>Gefahren von Kameras für (biometrische) Authentifizierungsverfahren</subtitle>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>de</language>

<abstract>Bei der Passworteingabe über die Schultern schauen? Die Mateflasche klauen, um an Fingerabdrücke zu kommen? Alles Technik von gestern. Der Vortrag zeigt, wie man heutzutage an Daten kommt, um Authentifizierungsmethoden zu überwinden.</abstract>

<description>Dass man Menschen bei der Passworteingabe über die Schulter gucken kann, ist bekannt. Und auch, dass man bestimmte biometrische Merkmale mit einer Kamera fotografieren kann oder Spuren der Merkmale an Gegenständen findet. Bisher ging man davon aus, dass man sich für solche Angriffe in der unmittelbaren Nähe der auszuspähenden Person befinden musste. Der Vortrag soll klar machen, dass dem nicht so ist. Wir stellen Ergebnisse von Untersuchungen vor, die zeigen, dass biometrische Merkmale und Passworteingaben auch aus großer Entfernung oder remote durch Kameras in Mobiltelefonen direkt oder indirekt (durch Reflexionen im Auge) ausgespäht werden können. </description>

<persons>

<person id="1623">starbug</person>

</persons>

<links/>

</event>

<event guid="7G4FQIXg2eb7D6F\_jNwuxA" id="6369">

<date>2014-12-27T21:45:00+01:00</date>

<start>21:45</start>

<duration>01:00</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6369\_-\_en\_-\_saal\_1\_-\_201412272145\_-\_ecchacks\_-\_djb\_-\_tanja\_lange</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>ECCHacks</title>

<subtitle>A gentle introduction to elliptic-curve cryptography</subtitle>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>This talk will explain how to work with elliptic curves constructively to obtain secure and efficient implementations, and will highlight pitfalls that must be avoided when implementing elliptic-curve crypto (ECC). The talk will also explain what all the buzz in curve choices for TLS is about. This talk does not require any prior exposure to ECC.</abstract>

<description>ECC is rapidly becoming the public-key technology of choice for Internet protocols. ECC was introduced in 1985 and has a much stronger security record than RSA. ECC research has found new ways of attacking implementations but has also found nicer curves that avoid such attacks.

As a followup to the Snowden revelations, the TLS working group of the IETF has recently asked the crypto research group (CFRG) to suggest new curves for use in TLS, and NIST has publicly announced that they are considering new curves.

This talk gives a hands-on description of how to compute with elliptic curves. It shows different ways to write elliptic curves and the consequences of this representation for secure and efficient implementation. Algorithms will be presented as Python code snippets and will already be online before the talk at http://ecchacks.cr.yp.to.

The talk will be given as a joint presentation by Daniel J. Bernstein and Tanja Lange.</description>

<persons>

<person id="3538">djb</person>

<person id="3714">Tanja Lange</person>

</persons>

<links/>

</event>

<event guid="MghFmvDBS-J7T2ZOkNXUKA" id="6154">

<date>2014-12-27T23:00:00+01:00</date>

<start>23:00</start>

<duration>01:00</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6154\_-\_en\_-\_saal\_1\_-\_201412272300\_-\_crypto\_tales\_from\_the\_trenches\_-\_nadia\_heninger\_-\_julia\_angwin\_-\_laura\_poitras\_-\_jack\_gillum</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Crypto Tales from the Trenches</title>

<subtitle/>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>Julia Angwin, Jack Gillum, and Laura Poitras will tell us stories about how they use crypto and privacy-enhancing technologies as high-profile journalists, and rant in an entertaining way about how these tools have failed or are horribly inadequate for their needs. They will also talk about their rare crypto successes.</abstract>

<description>Cryptography and privacy-enhancing technologies are increasingly part of a modern journalist's spycraft. But what does it look like when a reporter actually tries to protect herself and her sources with the best tools that the hacker/academic/activist/cipherpunk/technologist communities have produced? Disaster, chaos, crashes, and UI-sponsored opsec fails.

In this talk, Julia Angwin, Jack Gillum, and Laura Poitras will tell us highly entertaining and disturbing war stories of using crypto in the field as high-risk targets, and excoriate the crypto and developer communities for failing to meet their needs while claiming success and security for all. We will hear how the crypto-nerd's utopia of

deniable poker over the phone with an honest-but-curious adversary becomes a set of barely usable implementations and user expectation mismatches.

We hope to provide some clarity on what works and what doesn't for those who develop or aspire to develop secure applications, and also a rough guide to usable opsec right now for sources, journalists, and

other nontechnical users worried about sophisticated adversaries.</description>

<persons>

<person id="4131">Nadia Heninger</person>

<person id="4993">Julia Angwin</person>

<person id="3669">Laura Poitras</person>

<person id="5345">Jack Gillum</person>

</persons>

<links/>

</event>

<event guid="77aea78c-f2d2-461a-92b3-82929a79d598" id="6581">

<date>2014-12-28T00:00:00+01:00</date>

<start>00:00</start>

<duration>02:15</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6581\_-\_en\_-\_saal\_1\_-\_201412280000\_-\_citizenfour\_-\_laura\_poitras</slug>

<recording>

<license/>

<optout>true</optout>

</recording>

<title>Citizenfour</title>

<subtitle/>

<track>Entertainment</track>

<type>other</type>

<language>en</language>

<abstract>&quot;Citizenfour&quot; is Laura Poitras' documentary and a closeup view about blowing the whistle on the spooks at the NSA.</abstract>

<description>A portrait of Edward Snowden in the weeks he chooses to change our understanding of what governments know about us.</description>

<persons>

<person id="5258">Laura Poitras</person>

</persons>

<links/>

</event>

</room>

<room name="Saal 2">

<event guid="mzNAGavKy2KOcwOjGqC8pw" id="6443">

<date>2014-12-27T12:45:00+01:00</date>

<start>12:45</start>

<duration>01:00</duration>

<room>Saal 2</room>

<slug>31c3\_-\_6443\_-\_en\_-\_saal\_2\_-\_201412271245\_-\_trustworthy\_secure\_modular\_operating\_system\_engineering\_-\_hannes\_-\_david\_kaloper</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Trustworthy secure modular operating system engineering</title>

<subtitle>fun(ctional) operating system and security protocol engineering</subtitle>

<track>Science</track>

<type>lecture</type>

<language>en</language>

<abstract>We present Mirage OS, a modular library operating system developed from scratch in the functional programming language OCaml. Each service, called unikernel, is an OCaml application using libraries such as a TCP/IP stack, DNS. It is either compiled to a Xen virtual machine image or to a Unix binary (for development). State in 2014 is that it runs on x86 and arm, we implemented a clean-slate TLS (1.0, 1.1, 1.2), X.509, ASN.1 stack, crypto primitives, Off-the-record. We also have TCP/IP, HTTP, a persistent branchable store (similar to git) - all implemented in OCaml. A virtual machine serving data via https is roughly 2MB in size - no libc inside :)</abstract>

<description>Mirage OS is a (BSD-licensed) research project at University of Cambridge and released in December 2013 a 1.0 version. In 2014, 2.0 got released with full support on arm, a clean-slate TLS implementation, and the branchable data store Irmin. We (Hannes and David) developed a TLS stack from scratch (including cryptographic primitives, X.509, ASN.1), which we will present.

We intentionally breaks with the UNIX philosophy. Instead of using a programming language designed to replace platform-specific assembly code we use the functional programming language OCaml with higher-order functions, a composable module system, pattern matching, a sophisticated type system. Our developed TLS stack separates side effects, such as mutable memory, network input and output, etc., clearly from the pure functional core. This separation is not enforced on a language level, but by convention.

A mirage unikernel runs either as a Xen guest or as native Unix application. Each unikernel runs in a single address space, and does not include layers over layers of abstraction (kernel, user space, file system, processes, language runtime, threads, ...). The performance is not too bad (see link below). Each unikernel only uses those libraries it really needs - e.g. a name server does not depend on a file system or user accounts. A common unikernel is rather small in binary size: a web server, including TCP/IP stack and the data to be served, is less than a megabyte in size, including the OCaml runtime. There is no libc included :)

Modularity is the key for Mirage OS: the same application code can be compiled as a UNIX executable using the POSIX socket API, or as UNIX program using the userspace tun/tap interface and the TCP/IP stack written in OCaml, or as a Xen domU. This eases development, testing, debugging, and deployment.

Our target platform is the cubieboard2, a small board with a dual-core ARM A7 CPU and ethernet (and various other unused interfaces).

Code reviews, comments, contributions are always welcome.</description>

<persons>

<person id="1626">hannes</person>

<person id="4273">David Kaloper</person>

</persons>

<links>

<link href="http://www.openmirage.org">Mirage OS</link>

<link href="http://roscidus.com/blog/blog/2014/08/15/optimising-the-unikernel/">Performance: optimising the unikernel</link>

<link href="https://tls.openmirage.org">TLS demonstration server</link>

<link href="https://github.com/mirleft/ocaml-tls">OCaml-TLS source code</link>

<link href="http://openmirage.org/blog/announcing-mirage-20-release">Mirage 2.0 release</link>

<link href="http://openmirage.org/blog/introducing-ocaml-tls">Blog entry about OCaml-TLS</link>

<link href="http://docs.cubieboard.org/products/start">Cubieboard 2</link>

<link href="https://github.com/mirleft">Mirleft source code</link>

</links>

</event>

<event guid="419d4f7e-7506-4d46-8700-e47e164a8e32" id="6584">

<date>2014-12-27T14:00:00+01:00</date>

<start>14:00</start>

<duration>01:00</duration>

<room>Saal 2</room>

<slug>31c3\_-\_6584\_-\_de\_-\_saal\_2\_-\_201412271400\_-\_mit\_kunst\_die\_gesellschaft\_hacken\_-\_stefan\_pelzer\_-\_philipp\_ruch</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Mit Kunst die Gesellschaft hacken</title>

<subtitle>Das Zentrum für politische Schönheit</subtitle>

<track>Ethics, Society &amp; Politics</track>

<type>lecture</type>

<language>de</language>

<abstract>Ein Mahnmal gegen die Vereinten Nationen, 25.000 Euro Kopfgeld auf eine

deutsche Waffenhändlerfamilie, eine falsche Kampagne für das

Familienministerium oder die Flucht der &quot;Mauerkreuze&quot; vom Reichstagsufer

an die EU-Außengrenzen: wenn das Zentrum für Politische Schönheit (ZPS)

das Kriegsbeil ausgräbt, ist eine kontroverse Debatte garantiert.</abstract>

<description>Die Reaktionen reichen von Begeisterung bis Entsetzen. Das Feuilleton

jauchzt, die Springer-Presse heult, die CDU ist tief erschüttert, der

Bundestag debattiert und Griechenland mobilisiert Spezialeinheiten der

Polizei.

Eins ist sicher: Das Thema schlägt mit aller Wucht auf der Agenda ein

und wird bundesweit diskutiert.

Wie kann Kunst die Gesellschaft hacken?

Wie trifft man immer wieder den empfindlichen Nerv?

Wie transportiert man am helllichten Tag eine ganze Gedenkstätte ab, die

nur 15 Meter vom Bundestag entfernt steht?

Warum kann Theater so schlagkräftig Politik machen?

Und: Was ist eigentlich Politische Schönheit?

Philipp Ruch und Stefan Pelzer reisen aus der sagenumworbenen &quot;Zentrale&quot;

(O-TON &quot;BILD&quot;-Zeitung) des Zentrums für Politische Schönheit an und

nehmen Euch mit auf einen einstündigen Roadtrip an die EU-Außenmauern.

Unterwegs suchen sie Antworten auf diese und andere Fragen; mit

allerhand Skurilitäten und Annekdoten im Gepäck. Außerdem präsentieren

sie – in einer Welturaufführung – den SMS-Verkehr mit

Bundestagsabgeordneten der CDU/CSU Fraktion. Köpfe werden rollen. Und du

kannst dabei mithelfen.</description>

<persons>

<person id="5261">Stefan Pelzer</person>

<person id="5266">Philipp Ruch</person>

</persons>

<links/>

</event>

<event guid="HLDDEFxCxCrQryx8fEacZw" id="5960">

<date>2014-12-27T16:00:00+01:00</date>

<start>16:00</start>

<duration>01:00</duration>

<room>Saal 2</room>

<slug>31c3\_-\_5960\_-\_en\_-\_saal\_2\_-\_201412271600\_-\_revisiting\_ssl\_tls\_implementations\_-\_sebastian\_schinzel</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Revisiting SSL/TLS Implementations</title>

<subtitle>New Bleichenbacher Side Channels and Attacks</subtitle>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>We present four new Bleichenbacher side channels, and three successful Bleichenbacher attacks against the Java Secure Socket Extension (JSSE) SSL/TLS implementation and against hardware security appliances using the Cavium NITROX SSL accelerator chip.</abstract>

<description>16 years ago, Daniel Bleichenbacher presented a protocol-level padding oracle attack against SSL/TLS. As a countermeasure, all TLS RFCs starting from RFC 2246 (TLS 1.0) propose &quot;to treat incorrectly formatted messages in a manner indistinguishable from correctly formatted RSA blocks&quot;.

In our recent paper [1] we show that this objective has not been achieved yet: We present four new Bleichenbacher side channels, and three successful Bleichenbacher attacks against the Java Secure Socket Extension (JSSE) SSL/TLS implementation and against hardware security appliances using the Cavium NITROX SSL accelerator chip. Three of these side channels are timing-based, and two of them provide the first timing-based Bleichenbacher attacks on SSL/TLS described in the literature. Our measurements confirmed that all these side channels are observable over a switched network, with timing differences between 1 and 23 microseconds. We were able to successfully recover the PreMasterSecret using three of the four side channels in a realistic measurement setup.

Besides the academic relevance of breaking common SSL/TLS implementations, the timing attacks we performed are quite interesting for the hacking community. In our talk, we will thus focus on the challenges we had to solve during our attacks and on the challenges of fixing these issues.

The talk extends the topics that I presented at 28c3 [2] and 29c3 [3].

[1]: Revisiting SSL/TLS Implementations: New Bleichenbacher Side Channels and Attacks.

Meyer, Somorovsky, Weiss, Schwenk, Schinzel, Tews.

Usenix Security Symposium 2014.

[2]: https://media.ccc.de/browse/congress/2011/28c3-4640-en-time\_is\_on\_my\_side.html

[3]: https://media.ccc.de/browse/congress/2012/29c3-5044-en-time\_is\_not\_on\_your\_side\_h264.html</description>

<persons>

<person id="3205">Sebastian Schinzel</person>

</persons>

<links/>

</event>

<event guid="Bnz1quB2NHq9BEXoyNm5xQ" id="6499">

<date>2014-12-27T17:15:00+01:00</date>

<start>17:15</start>

<duration>01:00</duration>

<room>Saal 2</room>

<slug>31c3\_-\_6499\_-\_en\_-\_saal\_2\_-\_201412271715\_-\_glitching\_for\_n00bs\_-\_exide</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Glitching For n00bs</title>

<subtitle>A Journey to Coax Out Chips' Inner Secrets</subtitle>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>Despite claims of its obsolescence, electrical glitching can be a viable attack vector against some ICs. This presentation chronicles a quest to learn what types of electrical transients can be introduced into an integrated circuit to cause a variety of circuit faults advantageous to an reverser. Several hardware platforms were constructed during the quest to aid in research, including old-skool &amp; solderless breadboards, photo-etched &amp; professional PCBs, FPGAs, and cheap &amp; dirty homemade logic analyzers. The strengths and weaknesses of the various approaches will be discussed.</abstract>

<description>A shroud of mystery surrounds the topic of electrical glitching. Every now and then, you hear it thrown around as a possible attack vector - perhaps to aid in reverse-engineering efforts, or to understand an unknown cryptographic implementation. But what is glitching, exactly? And, more importantly, how can it be leveraged as a potentially powerful tool?

This presentation chronicles a quest to learn what types of electrical transients can be introduced into an integrated circuit to cause a variety of circuit faults advantageous to an reverser. Several hardware platforms were constructed during the quest to aid in research, including old-skool &amp; solderless breadboards, photo-etched &amp; professional PCBs, FPGAs, and cheap &amp; dirty homemade logic analyzers. The strengths and weaknesses of the various approaches will be discussed.

Instead of covering a hypothetical &quot;toy&quot; implementation of a victim chip - such as where the researcher/reverser implements a cryptographic algorithm themselves as software in a common microcontroller, and then attempts to glitch the implementation - a successful blackbox attack against a production security IC will be discussed, including how the attack was mounted, how results were obtained, and approaches to interpret the results.

Despite claims of its obsolescence, electrical glitching can be a viable attack vector against a variety of ICs, with a notable exception being some ultra-modern purpose-built security ICs. It is cheap to perform, you don't need an expensive laboratory, and if done properly, is non-destructive in nature. Glitching should be another tool in the reverser's arsenal, and can potentially provide results when other approaches have failed.</description>

<persons>

<person id="5172">exide</person>

</persons>

<links/>

</event>

<event guid="oI8n77eKy3Uz2Fklmk4hVQ" id="6180">

<date>2014-12-27T18:30:00+01:00</date>

<start>18:30</start>

<duration>01:00</duration>

<room>Saal 2</room>

<slug>31c3\_-\_6180\_-\_en\_-\_saal\_2\_-\_201412271830\_-\_rocket\_science\_how\_hard\_can\_it\_be\_-\_david\_madlener\_-\_sean</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Rocket science – how hard can it be?</title>

<subtitle>First steps into space with sounding rockets</subtitle>

<track>Science</track>

<type>lecture</type>

<language>en</language>

<abstract>Three years have elapsed since the call for a &quot;Hacker Space Program&quot; during the Chaos Communication Camp 2011. In this lecture we will review the basics of space flight, discuss common problems and pitfalls encountered by a practitioner on the way to orbit, and report on the state of our sounding rocket program.</abstract>

<description>We are the Forschungsgemeinschaft Alternative Raumfahrt e. V. (Research Community on Alternative Space Travel) or FAR for short, and have been working on feasible ways into space since our foundation in August 2003. After extensive experimentation with solid and hybrid propulsion systems on the ground, we developed the sounding rocket family &quot;Arguna&quot;. Since 2005 four different versions have been designed, built, and flown with different payloads. After a short review of basic rocket science and an outline of common propulsion technologies, we will report on the results of performed flights and experiments, especially of our latest sounding rocket Arguna IV.</description>

<persons>

<person id="3008">David Madlener</person>

<person id="5361">Sean</person>

</persons>

<links/>

</event>

<event guid="i\_Dt13BFiawklEaokv3pKg" id="6142">

<date>2014-12-27T20:30:00+01:00</date>

<start>20:30</start>

<duration>01:00</duration>

<room>Saal 2</room>

<slug>31c3\_-\_6142\_-\_en\_-\_saal\_2\_-\_201412272030\_-\_space\_hacker\_-\_karsten\_becker\_-\_robert</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Space Hacker</title>

<subtitle>Uploading rover...</subtitle>

<track>Science</track>

<type>lecture</type>

<language>en</language>

<abstract>At the 26C3 we first presented our vision of sending a rover to the moon. We're still in the pursuit of doing this and are closer than ever. Many things have happened in the past 5 years and we want to share our story with you.

But this talk is not just about us, it is also about you! You will have the possibility to contribute to our mission, just tune in to get all the details :)</abstract>

<description>In the past five years, we developed several lunar rovers. Each got more and more sophisticated and better suited for our mission.

In this presentation we will also unveil our latest upgrade to the the well known R3 rover, as well as the latest camera technology. Those two allowed us to participate in an interims competition of the Google Lunar X Prize.

This interims prize enables us to further pursue our dream of sending a rover to the moon.

In our mission to the moon, we also have the ability to bring payloads up on the lunar surface for the first time in a few decades (unless you have some good connection to the chinese who were there last year).

We are calling out to you, to develop an interesting payload, that we could potentially bring to the surface of the moon!</description>

<persons>

<person id="3798">Karsten Becker</person>

<person id="3052">Robert</person>

</persons>

<links>

<link href="http://ptscientists.com/go/space">To the moon!</link>

<link href="https://twitter.com/ptscientists">Twitter</link>

<link href="https://www.facebook.com/PartTimeScientists">Facebook</link>

<link href="https://plus.google.com/107778888097122544837">Google Plus</link>

</links>

</event>

<event guid="\_lVlmBO98KMg4M-n-\_A3FA" id="6103">

<date>2014-12-27T21:45:00+01:00</date>

<start>21:45</start>

<duration>01:00</duration>

<room>Saal 2</room>

<slug>31c3\_-\_6103\_-\_en\_-\_saal\_2\_-\_201412272145\_-\_amd\_x86\_smu\_firmware\_analysis\_-\_rudolf\_marek</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>AMD x86 SMU firmware analysis</title>

<subtitle>Do you care about Matroshka processors?</subtitle>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>You definitely should care. The aim of this talk is to provide insight to the security, architecture and yes you guessed it, vulnerability of the AMD System Management Unit (SMU) firmware found in modern AMD x86 processors.</abstract>

<description>Every modern x86 platform contains several other auxiliary processors, which kind of erase the line between pure hardware and software. How well are those processors secured? What is running on them? Is there a way to analyze them?

Great attention had the Intel ME engine, but similar, although not so unfriendly processor(s) exists on the AMD platforms too. The aim of this talk is to provide insight to the security, architecture and vulnerability of the AMD SMU firmware found in modern AMD x86 processors.

The SMU is designed to prevent unauthorized code execution, thus making it ideal candidate to verify if it is so. This is where the fun starts.

The overall goal is to educate the audience enough that they may (and want to) start to tinker around various non-x86 firmwares found on x86 systems on their own.

</description>

<persons>

<person id="4759">Rudolf Marek</person>

</persons>

<links/>

</event>

<event guid="67baa392-2af9-4213-a9ce-bf63331d43a4" id="6575">

<date>2014-12-27T23:00:00+01:00</date>

<start>23:00</start>

<duration>01:00</duration>

<room>Saal 2</room>

<slug>31c3\_-\_6575\_-\_en\_-\_saal\_2\_-\_201412272300\_-\_rocket\_kitten\_advanced\_off-the-shelf\_targeted\_attacks\_against\_nation\_states\_-\_tw\_-\_gadi</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Rocket Kitten: Advanced Off-the-Shelf Targeted Attacks Against Nation States</title>

<subtitle>A Deep Technical Analysis</subtitle>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>Rocket Kitten is an advanced APT set of campaigns, with a twist - off-the-shelf malware that won’t shame a nation state. The talk will combine an assessment of the threat group’s modus operandi with a technical deep dive. Prepare for some hex dumps.</abstract>

<description>This talk will uncover a set of high profile espionage campaigns from 2014 that involve a commercial attack framework – a highly specialized tool that has not been publicly documented and remained undetected in multiple operations. We will discuss the framework's technical design and review its features and capabilities that make it a premium instrument for stealth intrusions. We will further discuss how the tool was delivered to victims and how the compromise was carried out.</description>

<persons>

<person id="4135">tw</person>

<person id="1342">gadi</person>

</persons>

<links/>

</event>

</room>

<room name="Saal G">

<event guid="SXxWu-U4pNjjFZLl9XXDDA" id="6417">

<date>2014-12-27T12:45:00+01:00</date>

<start>12:45</start>

<duration>01:00</duration>

<room>Saal G</room>

<slug>31c3\_-\_6417\_-\_en\_-\_saal\_g\_-\_201412271245\_-\_3d\_casting\_aluminum\_-\_julia\_longtin</slug>

<recording>

<license>CC by SA 3.0</license>

<optout>false</optout>

</recording>

<title>3D Casting Aluminum</title>

<subtitle>Too Much Fun with Microwaves</subtitle>

<track>Hardware &amp; Making</track>

<type>lecture</type>

<language>en</language>

<abstract>We use microwaves to cast aluminum from 3D printed objects. This gives us the ability to cast high quality 6040 aluminum pieces using a 3D printer and commercially available consumer microwaves. </abstract>

<description>We manufacture microwave safe kilns for melting aluminum. We create microwave transparent molds that allow us to burn out plastic without heating the mold itself therefor creating a quicker method of accomplishing the lost PLA process.</description>

<persons>

<person id="4937">Julia Longtin</person>

</persons>

<links>

<link href="http://fosscar.faikvm.com/">FossCar Project</link>

</links>

</event>

<event guid="KJiq3wTS9cMLTTrgJ8PqHA" id="6240">

<date>2014-12-27T14:00:00+01:00</date>

<start>14:00</start>

<duration>01:00</duration>

<room>Saal G</room>

<slug>31c3\_-\_6240\_-\_en\_-\_saal\_g\_-\_201412271400\_-\_reproducible\_builds\_-\_mike\_perry\_-\_seth\_schoen\_-\_hans\_steiner</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Reproducible Builds</title>

<subtitle>Moving Beyond Single Points of Failure for Software Distribution</subtitle>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>Software build reproducibility is the ability to use independent build machines to compile bit-identical binaries from program source code. In this talk, we will discuss the motivation for and the technical details behind software build reproducibility. We will describe the technical mechanisms used by the Tor Project to produce

reproducible builds of the Tor Browser, and also introduce the early efforts of both F-Droid and Debian to achieve these same build integrity properties on a more wide-scale basis.</abstract>

<description>For the past several years, we've been seeing a steady increase in the weaponization, stockpiling, and the use of software exploits by many parties. In particular, there are an increasing number of vectors to &quot;bridge the air gap&quot; and exploit even disconnected machines. Software build systems make a worrisome target for these types of exploits, as they provide a stepping stone to compromise very large numbers of machines.

To underscore this point, we will demonstrate a simple Linux rootkit that is capable of infecting the compilation process while otherwise leaving no traces on the machine.

We will discuss a powerful solution to this problem: Build Reproducibility. We will focus on the build system used by The Tor Project to build Tor Browser - our Firefox-based browser. We will also touch upon current work by Debian, as well as by F-Droid and the Guardian Project for Android.</description>

<persons>

<person id="5030">Mike Perry</person>

<person id="51">Seth Schoen</person>

<person id="5330">Hans Steiner</person>

</persons>

<links/>

</event>

<event guid="E95sP8WH8tLiiJj2SBAA1A" id="6267">

<date>2014-12-27T16:00:00+01:00</date>

<start>16:00</start>

<duration>01:00</duration>

<room>Saal G</room>

<slug>31c3\_-\_6267\_-\_en\_-\_saal\_g\_-\_201412271600\_-\_osmo-gmr\_what\_s\_up\_with\_sat-phones\_-\_sylvain\_munaut</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>osmo-gmr: What's up with sat-phones ?</title>

<subtitle>Piecing together the missing bits</subtitle>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>At 28C3 we introduced the very first steps of the osmo-gmr projects. During this talk, we will present the various advances that have been made in this project on various aspects (voice codec, crypto algorithm, ...)</abstract>

<description>GMR-1 (GEO Mobile Radio) is a satellite phone protocol derived from GSM. The main operator using this protocol is Thuraya and is mainly active in the middle east and asia.

osmo-gmr is a project of the osmocom family whose goal is to implement the various levels of a GMR stacks, starting from SDR signal acquisition up to the actual voice layer.

At 28C3 we gave and introductory talk to the project which was pretty new at the time. On this talk, we will quickly summarize what was presented last time and then move on to the new stuff.

The two main obstacles to implement a practical monitoring software for GMR-1 were the secret crypto algorithm and the unknown voice codec. Both obstacles have now been lifted and we will present the details of how that happened. We will also look toward the next steps and other aspects of the system that we're planning to dig into.</description>

<persons>

<person id="3123">Sylvain Munaut</person>

</persons>

<links>

<link href="http://gmr.osmocom.org/">osmo-gmr website</link>

</links>

</event>

<event guid="sAZoeOc6Qu4bMPxrU8yEpw" id="6184">

<date>2014-12-27T17:15:00+01:00</date>

<start>17:15</start>

<duration>01:00</duration>

<room>Saal G</room>

<slug>31c3\_-\_6184\_-\_de\_-\_saal\_g\_-\_201412271715\_-\_mein\_bot\_der\_kombattant\_-\_josch\_-\_arche3000</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Mein Bot, der Kombattant</title>

<subtitle>Operative Kommunikation im digitalen Informationskrieg</subtitle>

<track>Science</track>

<type>lecture</type>

<language>de</language>

<abstract>Der Vortrag bietet eine sprachwissenschaftlich informierte Perspektive auf den Informationskrieg mit Fokus auf operative Kommunikation in sozialen Medien. Am Beispiel eines selbst entwickelten Bots werden wir linguistische Prozeduren zur Manipulation von Kommunikation mit dem Ziel der Beeinflussung von Wissen, Werten, Gefühlen und Handlungsdispositionen vorstellen. </abstract>

<description>Der Meinungskampf im Netz wird professioneller: Während der Ukrainischen Maidan-Proteste sahen sich die Redaktionen von Online-Zeitungen mit einer Flut von russlandfreundlichen Kommentaren konfrontiert, die die Proteste als Werk amerikanischer Geheimdienste und die Regierung in Kiew als Nazi-Junta zu diskreditieren suchten. Verursacher war die &quot;Agentur zur Analyse des Internets&quot; aus St. Petersburg, die mutmaßlich von staatlichen Akteuren damit beauftragt wurde, die öffentliche Meinung in anderen Ländern durch verdeckte Operationen in sozialen Netzwerken zu beeinflussen. Und in Südkorea hat die Abteilung Psychologische Strategie des National Intelligence Service (NIS) mittels gefälschter Twitter-Accounts im Vorfeld der Präsendentschaftswahlen 1,2 Millionen Tweets versendet, um Stimmung für Park Geun Hye, Kandidatin der konservativen Saenuri-Partei zu machen.

Der digitale Informationskrieg ist also längst im Gang. Er zielt wie traditionelle Psychologische Operationen auf die Beeinflussung von Wissen, Werten, Gefühlen und Handlungsdispositionen und will Agenda Setting in der gegnerischen Öffentlichkeit betreiben. Von den traditionellen PSYOPS unterscheidet ihn, dass er maschinell und klandestin geführt wird und statt massenkommunikativ zu agieren über die Möglichkeit verfügt, jeden, der sich in sozialen Netzwerken bewegt, persönlich und mit einer individuellen Strategie anzusprechen. Der Bot ist ein Kombattant mit der Aufgabe, Menschen zu beeinflussen, konstruktive Diskussionen zu verhindern und Social-Media-Monitoring-Systeme und Aggregatoren zu manipulieren. Sein Medium ist in erster Linie die Sprache, die einordnen, bewerten, konfrontieren und überzeugen will, die eine Wirklichkeit erschaffen will, in der das Handeln der eigenen Konfliktpartei als legitim, gerecht und zwingend und das des Feindes als falsch, unrecht und unwahrhaftig erscheint.

In unserem Vortrag werden wir den Begriff der operativen Kommunikation aus sprachwissenschaftlicher Perspektive definieren, ihre rechtlichen Rahmenbedingungen im Informationskrieg bestimmen und die Legitimität von operativer Kommunikation für unterschiedliche Regimetypen diskutieren. Anhand eines selbst entwickelten einfachen Bots wollen wir im zweiten Teil des Vortrags Szenarien für den operativen Einsatz in der semantischen Matrix vorstellen und die linguistischen Operationen illustrieren, die zur Manipulation von Kommunikation führen können. </description>

<persons>

<person id="4168">josch</person>

<person id="5007">arche3000</person>

</persons>

<links/>

</event>

<event guid="1hSKsR-r9B0BnpLfUvpDAg" id="6255">

<date>2014-12-27T18:30:00+01:00</date>

<start>18:30</start>

<duration>01:00</duration>

<room>Saal G</room>

<slug>31c3\_-\_6255\_-\_de\_-\_saal\_g\_-\_201412271830\_-\_10\_jahre\_openstreetmap\_-\_thomas\_skowron\_-\_ubahnverleih</slug>

<recording>

<license>CC-BY-3.0</license>

<optout>false</optout>

</recording>

<title>10 Jahre OpenStreetMap</title>

<subtitle>Wir leben noch und zwar sehr gut.</subtitle>

<track>Hardware &amp; Making</track>

<type>lecture</type>

<language>de</language>

<abstract>Seit nun über 10 Jahren gibt es OpenStreetMap. Besonders in den letzten drei Jahren war die Entwicklung überwältigend, sowohl was die Datenlage als auch das gesamte Ökosystem anbelangt. Wir wollen zeigen, was möglich ist und was in der Zukunft (hoffentlich) passieren wird.</abstract>

<description/>

<persons>

<person id="3938">Thomas Skowron</person>

<person id="4059">ubahnverleih</person>

</persons>

<links/>

</event>

<event guid="n2DFvyl\_lWjW-gm317vT3A" id="6050">

<date>2014-12-27T20:30:00+01:00</date>

<start>20:30</start>

<duration>01:00</duration>

<room>Saal G</room>

<slug>31c3\_-\_6050\_-\_en\_-\_saal\_g\_-\_201412272030\_-\_code\_pointer\_integrity\_-\_gannimo</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Code Pointer Integrity</title>

<subtitle>... or how we battle the daemons of memory safety</subtitle>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>Programs are full of bugs, leading to vulnerabilities. We'll discuss power and limitations of code-pointer integrity (CPI), a strong but practical security policy that enforces memory safety for all code pointers, protecting against any form of control-flow hijack attack (e. g., ROP or JOP).

</abstract>

<description>Systems code is often written in low-level languages like C/C++, which offer many benefits but also delegate memory management to programmers. This invites memory safety bugs that attackers can exploit to divert control flow and compromise the system. Deployed defence mechanisms (e. g., ASLR, DEP) are incomplete, and stronger defence mechanisms (e. g., CFI) often have high overhead and limited guarantees (and are therefore not generally deployed).

In this talk we discuss code-pointer integrity (CPI), a strong security policy that guarantees the integrity of all code pointers in a program (e.g., function pointers, saved return addresses) and thereby prevents all control-flow hijack attacks, including return-oriented programming and jump-oriented programming. We also introduce code-pointer separation (CPS), a relaxation of CPI with better performance properties. Both CPI and CPS offer substantially better

security-to-overhead ratios than the state of the art, they are practical (we protect a complete FreeBSD system and over 100 packages like apache and postgresql), effective (prevent all attacks in the RIPE benchmark), and efficient, resulting in very low to negligible performance overhead.

We will also discuss technical challenges in the CPI prototype implementation, practical challenges we faced when protecting a full FreeBSD distribution, and give more details on the scope of protection which will be interesting to hackers. The full prototype implementation is open-source, all changes to FreeBSD are open-source and we're working on integrating the patches into LLVM.</description>

<persons>

<person id="2410">gannimo</person>

</persons>

<links>

<link href="http://levee.epfl.ch/">Code-Pointer Integrity project</link>

<link href="https://github.com/cpi-llvm">GitHub</link>

<link href="http://nebelwelt.net/publications/14OSDI/">Code-Pointer Integrity (2)</link>

</links>

</event>

<event guid="H\_jf4nwFLZMEY7zwBlrehA" id="6195">

<date>2014-12-27T21:45:00+01:00</date>

<start>21:45</start>

<duration>01:00</duration>

<room>Saal G</room>

<slug>31c3\_-\_6195\_-\_en\_-\_saal\_g\_-\_201412272145\_-\_the\_cloud\_conspiracy\_2008-2014\_-\_caspar\_bowden</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>The Cloud Conspiracy 2008-2014</title>

<subtitle>how the EU was hypnotised that the NSA did not exist</subtitle>

<track>Ethics, Society &amp; Politics</track>

<type>lecture</type>

<language>en</language>

<abstract>In 2011 I started trying to warn EU institutions about what we now call PRISM, after working it out from open sources. Civil society, privacy regulators, and the Commission all did nothing. This is the story of exactly how they did nothing, and why, and what is happening now</abstract>

<description>There is one law (FISA 702) and one policy (EO12333) which authorizes the US government to conduct mass surveillance on &quot;foreigners in foreign lands&quot;. These are drafted in terms which discriminate the privacy rights you have by the passport you hold - in fact there are no rights at all for non-Americans outside the US.

It is obvious that this is a reasonably important dimension of the whole Snowden affair, because it starkly conflicts with ECHR norms that rights are universal and equal.

The only possible resolution compatible with universal rights is data localization, or construction of a virtual zone in which countries have agreed mutual verifiable inspections that mass-surveillance is not occurring (and at present this seems unlikely). There is a widespread misconception that somehow the new GDPR privacy regulation will curb foreign spying, when in fact it is designed to widen loopholes into floodgates.

This talk is multidisciplinary and will cover national and international surveillance and privacy law, Five Eyes SIGINT policy, technical security and economics.</description>

<persons>

<person id="3857">Caspar Bowden</person>

</persons>

<links/>

</event>

<event guid="AvAdq20cdc8iWoNubd6ABw" id="6361">

<date>2014-12-27T23:00:00+01:00</date>

<start>23:00</start>

<duration>01:00</duration>

<room>Saal G</room>

<slug>31c3\_-\_6361\_-\_en\_-\_saal\_g\_-\_201412272300\_-\_from\_maxwell\_to\_antenna\_arrays\_-\_friederike</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>From Maxwell to antenna arrays</title>

<subtitle>How 150 year old equations still help to communicate</subtitle>

<track>Science</track>

<type>lecture</type>

<language>en</language>

<abstract>Maxwell's equations are four differential equations which form the foundation of classical electrodynamics, classical optics, and electric circuits. This talk will take a look at the connection between these equations, wave propagation and antenna arrays.

</abstract>

<description>Maxwell's equations describe how electric and magnetic fields are generated and altered by each other and by charges and currents. They are named after the Scottish physicist and mathematician James Clerk Maxwell, who published those equations exactly 150 years ago and form the foundation of classical electrodynamics. Actually Maxwell had 20 equations and it took another 20 years until they were understood and the self-taught British engineer, mathematician, and physicist Heaviside put the equations in their present form. Some years later Hertz brought the experimental prove of Maxwell's theory.

Under a lot of simplifying boundary conditions wave propagation and antenna theory can be derived from this four equations. This talk will lead from Maxwell's equations to wave equations and nice antenna forms and arrays. Also some practical aspects will be evaluated. Why do low frequencies reach farther than higher frequencies? Why do radio astronomers spread their antenna arrays over whole continents? Or why is China Mobile building antenna arrays for mobile radio consisting of 128 antennas?

</description>

<persons>

<person id="5073">Friederike</person>

</persons>

<links/>

</event>

</room>

<room name="Saal 6">

<event guid="NjtxGgpt76NkFb1Q4LLjvg" id="6100">

<date>2014-12-27T12:45:00+01:00</date>

<start>12:45</start>

<duration>01:00</duration>

<room>Saal 6</room>

<slug>31c3\_-\_6100\_-\_en\_-\_saal\_6\_-\_201412271245\_-\_personal\_tracking\_devices\_and\_online\_identity\_-\_silvia</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Personal Tracking Devices and Online Identity</title>

<subtitle/>

<track>Ethics, Society &amp; Politics</track>

<type>lecture</type>

<language>en</language>

<abstract>In the post-NSA world it is important to understand the magnitude of our online activities in order to take informative decisions on our ubiquitous shared lives.

Personal Tracking Devices is the result of a two years long study on tracking technologies and the inherent nature of the web and telecommunication networks in general.

The study, conducted as part of Ph.D. research in privacy and security at UPC Barcelona Tech, collected a large amount of metadata to raise awareness on the footprints left by users on the web and through mobile apps.

</abstract>

<description>Personal tracking devices will visualise the online footprint of a user by looking at their metadata.

A hypermedia model of the user footprint would then be introduced in order to better explore it. This model has been called hyperme.

Hyperme is a hyperdata model of a user online footprint. The hyperme model links the user identities created across different services and the features associated with them. These features are attributes that compose an identity, such as email, date of birth, place of birth and so on.

The hyperme model of the user identity permits the visualisation of the user expressed preferences, the content they have created and who or what can access this content.

The model uses context between the user’s various identities and the signals produced, to create links between different objects, obtaining an explorable graph­-like structure.

Links between data snippets are creating by exploring the keywords and categories used to describe the entities. These are provided by the user themselves through freeform annotations, particular use of language, location information, timestamps, social relationships and association with other entities such as companies and institutions.

Explicit connections are also discovered by associating such keywords with Wikipedia concepts. By exploiting links between articles, it is possible to draw relations between different entities, providing a dictionary to build strong connections between different categories.

If the identities created by a single user, and the signals generated are analysed at different levels, it would be possible to discover different subgraphs and sub­hypergraphs between the data object, therefore revealing a complex network of heterogeneous information shared across a number of services and with sets of different parties, being this social relationships or other applications and devices.

Each party in fact enjoys a certain level of access to the different documents produced by the user, by the devices used and by the application authorised to access and produce content on their behalf.

A hypergraph model therefore allows the possibility to explore the user’s different identities and the corresponding created content at different levels, exposing how different services or relationships contribute to protect or threaten the user privacy.</description>

<persons>

<person id="4036">Silvia</person>

</persons>

<links>

<link href="http://www.nopressure.co.uk/31C3/#/">Slides</link>

</links>

</event>

<event guid="BhRiQWa\_rOqEw5k-l4GRXg" id="6447">

<date>2014-12-27T14:00:00+01:00</date>

<start>14:00</start>

<duration>01:00</duration>

<room>Saal 6</room>

<slug>31c3\_-\_6447\_-\_en\_-\_saal\_6\_-\_201412271400\_-\_let\_s\_build\_our\_own\_personalized\_open\_textile\_production\_line\_-\_hong\_phuc\_dang</slug>

<recording>

<license>Public domain</license>

<optout>false</optout>

</recording>

<title>Let’s build our own personalized open textile production line </title>

<subtitle/>

<track>Hardware &amp; Making</track>

<type>lecture</type>

<language>en</language>

<abstract>The talk is about our project to develop software and hardware tools for a fair and environment friendly garment and textile production and how we break down the locks that exists on every level in the industry from design, to software, machines and distribution. </abstract>

<description>The talk is about our project to develop software and hardware tools for a fair and environment friendly garment and textile production and how we break down the locks that exists on every level in the industry from design, to software, machines and distribution.

We want to set up our own personalized open textile production line and offer an alternative to the unethical ways most of our clothes are produced today. At the talk we will present the first successes of this endeavor in our community - Open Source pattern making software, sewing robots, next generation knitting machine upgrades - and challenges that are ahead.

Democratizing digital textile production and offers the chance for a fair and environment friendly production of garments and textiles at home and in the industry. Just as 3D printers enable more and more people to become makers we want to enable digital garment makers to create their own clothes, share them online and produce it where-ever they are.

Members of our projects include software developers, fashion designers, pattern creators, knitters, textile manipulators, hardware hackers, and even industry experts. We started a FashionTec Working Group about two years ago after the annual Libre Graphics meeting in Madrid.

The traditional industry is in a state of complete lock on all levels:

\* digital fashion design locked to competing proprietary formats and software

\* production locked to machines of producers accepting formats

\* distribution lock - locked to existing large distribution channels in order to be a viable business

The Free and Open Source community has taught us that it is possible to overcome a complete proprietary lock down. Let’s repeat this success in the textile and garment industry. We need Free and Open Source software, Open Formats and Open machines. With todays development tools successes are just a short step away. Our talk will give you insights and hopes to inspire more people.

</description>

<persons>

<person id="2658">Hong Phuc Dang</person>

</persons>

<links>

<link href="http://fashiontec.org">FashionTec</link>

<link href="http://www.taumeta.org/">TauMetaTau Physica</link>

</links>

</event>

<event guid="0CpZm9-0S1ja92XDOICX0Q" id="6077">

<date>2014-12-27T16:00:00+01:00</date>

<start>16:00</start>

<duration>01:00</duration>

<room>Saal 6</room>

<slug>31c3\_-\_6077\_-\_en\_-\_saal\_6\_-\_201412271600\_-\_how\_i\_learned\_to\_stop\_reinventing\_and\_love\_the\_wheels\_-\_andreas\_bihlmaier</slug>

<recording>

<license>CC BY 3.0</license>

<optout>false</optout>

</recording>

<title>How I Learned to Stop Reinventing and Love the Wheels</title>

<subtitle>or having FUN with (home/hackerspace) robotics</subtitle>

<track>Hardware &amp; Making</track>

<type>lecture</type>

<language>en</language>

<abstract>An introduction to the Robot Operating System (ROS) for the home/hackerspace roboticist (if it physically interacts with the world through code, call it robot).</abstract>

<description>All large, feature-rich and complex frameworks suck. True, but too short for a talk. Therefore the talk tries to make a point on why one should still us these frameworks (for robotics). At least so, if one wants to have fun with (home/hackerspace) robotics and do something cool, instead of getting stuck at the usual &quot;trivial&quot; (or low-level, sounds less judging) capabilities.

In order to build robots one needs at least a basic understanding of mechanics, electronics and computer science. Obviously, more advanced robot features in each area, depend on more advanced roboticist skills – and equipment ... and money. The growing community of makers, the proliferation of hackerspaces (cooperators, equipment!) and highly useful consumer devices lessen the hardware related challenges. On the other hand, state-of-the-art open-source robotics software has been available for quite a few years already. Unfortunately, it is still somewhat neglected by the extended, i. e. non-academic, robotics community. The mindset and prejudices of too many hackerspace natives is opposed to using preexisting frameworks, especially large ones, in favor of starting from scratch. Bloat, ugly APIs, deprecated programming styles and of course bad code conventions ... good and good enough reasons to start over (I confess, too!). As a result many projects never get beyond the point of &quot;finally fixed the bug by reflashing the microcontroller with code that sets register bar42=0xf00, now it moves – sort of&quot;.

The famous &quot;Re-inventing the Wheel&quot; comic (http://www.willowgarage.com/sites/default/files/blog/201004/willow\_p1\_02s.jpg) posted by Willow Garage in 2010, does tell the life cycle of robotics in the PhD world, but not only that. Rather, unfortunately, it pertains to robotic and closely related projects in general.

So in a nutshell, yet another 'Introduction to ROS' talk? Yes, an introduction to the Robot Operating System (ROS).

However, for once without leaving behind the impression (in the hobbyists mind) that this is all cool stuff, but what to do with it when not owning a 100K dollar robot.

The goal is to show a few basics (the Plumbing), as many of the tools and capabilities as time permits and a few words about the people side of things.

(http://www.ros.org/wp-content/uploads/2013/12/ros\_equation.png)

Should the robot visually perceive the world? ROS + Webcam(s) / Kinect / Xtion. Hello, out of the box drivers, calibration, point clouds and object recognition.

Should the robot drive around and navigate in the environment? ROS + Navigation stack. Hello, out of the box SLAM.

Should the robot reach out and grasp something? ROS + MoveIt!. Hello, out of the box collision-free motion planning.

Should the robot brain be distributed across multiple computers without changing a line of code? ROS. Hello, out of the box usable(!) middleware.

Should the robot builders be able to create independent, yet compatible modules? ROS. Hello, out of the box modularity (well ok – at least kind of).

Should the robot's world be easily understandable through interactive visualizations? ROS + Rviz / rqt. Hello, out of the box advanced 3D visualization for many types of data.

Is this an advertisement? Yes, for great open source software – to make each of your lines of code do more \_interesting\_ stuff. Hello ROS world.</description>

<persons>

<person id="4896">Andreas Bihlmaier</person>

</persons>

<links/>

</event>

<event guid="hixbG3OS0o1-lkJG36qcug" id="6234">

<date>2014-12-27T17:15:00+01:00</date>

<start>17:15</start>

<duration>01:00</duration>

<room>Saal 6</room>

<slug>31c3\_-\_6234\_-\_en\_-\_saal\_6\_-\_201412271715\_-\_the\_experimental\_robot\_project\_-\_norbert\_braun\_-\_darthrake</slug>

<recording>

<license>CC-BY-3.0</license>

<optout>false</optout>

</recording>

<title>The eXperimental Robot Project</title>

<subtitle>An open-hardware bipedal walking machine</subtitle>

<track>Hardware &amp; Making</track>

<type>lecture</type>

<language>en</language>

<abstract>The talk is on the eXperimental Robot Project (XRP), a project to develop an open-hardware humanoid robot. More precisely, we are focusing on the distinguishing feature of a &lt;i&gt;humanoid&lt;/i&gt; robot - the ability to walk on two legs.

</abstract>

<description>Humanoid robots fascinate us - they appear in nearly every science fiction universe. Compared to Mr. Data or C-3PO, humanoids in reality are rather disappointing. Not only do they lack anything resembling human-level intelligence, but even their walking is slow and fragile - most of them only work on perfectly even ground. While we still have to wait a long time for true artificial intelligence, the recent years have brought substantial progress with respect to motion.

Unfortunately, most of that progress is proprietary - the leading groups, such as Schaft and Boston Dynamics, publish very little beyond Youtube videos. University projects are more open, but still usually do not publish source code or construction drawings. We think that bipedal robots are way too important to be left to the proprietary world, so we decided to learn from what is available and start to build our own, completely open one. In the talk, we will try to share what we have learned so far.

The first part of the talk will be on simulation, which allows us to test control algorithms and to get an idea about the mechanical requirements without having to build actual hardware. We will introduce the basics of rigid body dynamics, discuss the physics of walking and show how a successful walking machine can be built, at least a virtual one.

In the second part of the talk, we will discuss how a physical, human-size robot might be built without needing a 100,000+ € budget. We will present our plans and experiments on sensors, motor drivers and actuators.</description>

<persons>

<person id="4970">Norbert Braun</person>

<person id="3800">darthrake</person>

</persons>

<links>

<link href="http://www.xrpbot.org/">The eXperimental Robot Project</link>

</links>

</event>

<event guid="0a06acd5-709e-4bba-9444-e71f78cd2094" id="6559">

<date>2014-12-27T18:30:00+01:00</date>

<start>18:30</start>

<duration>01:00</duration>

<room>Saal 6</room>

<slug>31c3\_-\_6559\_-\_de\_-\_saal\_6\_-\_201412271830\_-\_jugend\_hackt\_-\_fiona\_krakenburger\_-\_maria\_reimer\_-\_philipp\_kalweit\_-\_max\_nagy\_-\_lukas\_-\_nico</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Jugend hackt</title>

<subtitle/>

<track>Hardware &amp; Making</track>

<type>lecture</type>

<language>de</language>

<abstract>Im September 2014 fand die Veranstaltung Jugend hackt statt: Ein Wochenende Hacken, Basteln und Programmieren mit 120 computerbegeisterten Jugendlichen. Wir als Organisatorinnen und Teilnehmer wollen von dem Event erzählen und unsere Erfahrungen teilen. Der Talk richtet sich gleichermaßen an Jugendliche, die sich für's Hacken begeistern, als auch an alle, die sich für Code Literacy, Medienpädagogik oder den IT-Nachwuchs interessieren.</abstract>

<description>&quot;In Deutschland lernen Kinder den Umgang mit Medien trotz Schule.&quot; Das ist das ernüchternde Fazit eines Schulforschers, der dieses Jahr die nicht weniger desillusionierende International Computer and Information Literacy Studie vorstellte. Dabei ist ein grundlegendes Verständnis von Computertechnologien Voraussetzung dafür, sich in einer Welt der digitalen Technologien zurechtzufinden und sie mitgestalten zu können. Da sind sich alle einig, und es wird viel darüber gesprochen. Doch die große Bildungsinitiative lässt auf sich warten, und Nachwuchstalente werden gesellschaftlich noch immer wenig beachtet und noch seltener aktiv gefördert.

Wir von der gemeinnützigen Open Knowledge Foundation Deutschland e.V. wollten nicht länger warten und haben deswegen 2013 das Förderprogramm Jugend hackt ins Leben gerufen. Zuletzt kamen im September 2014 rund 120 Jugendliche aus ganz Deutschland in Berlin zusammen. Gemeinsam mit Gleichgesinnten haben sie an Software- und Hardwareprojekten rund um die Themen Überwachung, Bildung, Gesundheit, Gesellschaft, Freizeit und Umwelt gearbeitet.

Die Jugendlichen, die zwischen 12 und 18 Jahre alt sind, entwickelten insgesamt 27 Projekte, mit denen sie ein deutliches Statement gegen das beliebte Narrativ der politisch desinteressierten Jugend setzten. Sie zeigten nicht nur, dass sie technisch versiert und kreativ mit Computern umgehen konnten, sondern auch einen wachsamen und kritischen Blick auf gesellschaftliche und politische Herausforderungen haben. Alle 27 Projektideen sind selbstständig von den Jugendlichen erarbeitet und umgesetzt worden. Für Fragen standen den Jugendlichen erwachsene Softwareentwickler/innen zur Seite.

Auf dem 31c3 wollen wir unsere Erfahrungen mit euch teilen. Zudem werden Teilnehmer von Jugend hackt ihre entstandenen Projekte vorstellen. Da ist z.B. &quot;Awearness&quot;, ein Armband, das vibriert, wenn eine Überwachungskamera in der Nähe ist. Oder &quot;Dapro&quot;, ein Datenschutzproxy, der über aufgezeichnete Metadaten informiert. Oder die &quot;intelligente Pillenbox&quot;, die Tabletten an demenzkranke Patienten ausgibt und bei Nicht-Einnahme einen Notruf an den Pfleger absetzt.</description>

<persons>

<person id="5289">Fiona Krakenbürger</person>

<person id="5285">Maria Reimer</person>

<person id="5322">Philipp Kalweit</person>

<person id="5323">Max Nagy </person>

<person id="5324">Lukas</person>

<person id="5325">Nico</person>

</persons>

<links/>

</event>

<event guid="qdo1rVjUVrQBHvjWYYx8sQ" id="6412">

<date>2014-12-27T20:30:00+01:00</date>

<start>20:30</start>

<duration>01:00</duration>

<room>Saal 6</room>

<slug>31c3\_-\_6412\_-\_en\_-\_saal\_6\_-\_201412272030\_-\_towards\_general\_purpose\_reconfigurable\_computing\_on\_novena\_-\_stars\_-\_andy\_isaacson</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Towards General Purpose Reconfigurable Computing on Novena</title>

<subtitle>FPGAs for Everybody with Novena</subtitle>

<track>Hardware &amp; Making</track>

<type>lecture</type>

<language>en</language>

<abstract>The Novena open source laptop contains a FPGA, but free software support for FPGAs is lacking and requires root access to the hardware.</abstract>

<description>Our work is on providing a framework and a demonstration application for general purpose accelerator cores for Novena's FPGA.</description>

<persons>

<person id="3431">stars</person>

<person id="4229">Andy Isaacson</person>

</persons>

<links/>

</event>

<event guid="P27IBlfmjGfZIib1deB\_xg" id="6530">

<date>2014-12-27T21:45:00+01:00</date>

<start>21:45</start>

<duration>01:00</duration>

<room>Saal 6</room>

<slug>31c3\_-\_6530\_-\_en\_-\_saal\_6\_-\_201412272145\_-\_in\_security\_of\_mobile\_banking\_-\_ericfiliol\_-\_paul\_irolla</slug>

<recording>

<license>CC-BY-3.0</license>

<optout>false</optout>

</recording>

<title>(In)Security of Mobile Banking</title>

<subtitle/>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>This talk presents a deep analysis of banking mobile apps available in the world. Based on static and dynamic analysis as well as on the analysis of the final source code we show that a vast majority of them are not respecting users' privacy and users' data protection. Worse a few of them contains critical bugs</abstract>

<description>Mobile banking is about to become the de facto standard for banking activities. Banking apps – on smartphones and tablets - are widespreading more and more and this evolution aims at strongly limiting the classical access to bank (physical, through PC browser, through ATM…). The aim is first to cut the cost but also to make the personal data explode.

Then three critical issues arise. Since we entrust those mobile applications by feeding them with passwords, private information, and access to one of the most critical part of our like (money):

• Do those applications protect our private life and especially which kind of information is leaking to the bank?

• Are they containing vulnerabilities that could be exploited by attackers?

In this talk, we are going to present a deep analysis of many banking apps collected in the world. We have performed static and dynamic analysis based on the binaries AND the source code. We will show that almost all apps are endangering our private data (sometimes severely) but in a few cases the presence of vulnerabilities are extremely concerning. While we tried to contact all the relevant banks for a free, detailed technical feedback and to help them fixing their apps, we will explain that a few of them did not care about this feedback and therefore did not want to take any security measure.

This talk contains demos and operational results on existing apps.

</description>

<persons>

<person id="3066">ericfiliol</person>

<person id="5221">Paul Irolla</person>

</persons>

<links/>

</event>

<event guid="13hAy7IIWod2RIuLMvnELw" id="6531">

<date>2014-12-27T23:00:00+01:00</date>

<start>23:00</start>

<duration>01:00</duration>

<room>Saal 6</room>

<slug>31c3\_-\_6531\_-\_en\_-\_saal\_6\_-\_201412272300\_-\_ss7map\_mapping\_vulnerability\_of\_the\_international\_mobile\_roaming\_infrastructure\_-\_laurent\_ghigonis\_-\_alexandre\_de\_oliveira</slug>

<recording>

<license>CC-BY-3.0</license>

<optout>false</optout>

</recording>

<title>SS7map : mapping vulnerability of the international mobile roaming infrastructure</title>

<subtitle/>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>SS7 has been shown repeatedly as an insecure protocol: spoofing, faking, crash through fuzzing, fraud. The main question of our study is to determine how this insecurity is mitigated by network operator’s action to prevent compromise on both network exposure of infrastructure and privacy compromise of subscribers. It's why we wanted to come out with SS7map.</abstract>

<description>SS7 has been shown repeatedly as an insecure protocol: spoofing, faking, crash through fuzzing, fraud. The main question of our study is to determine how this insecurity is mitigated by network operator’s action to prevent compromise on both network exposure of infrastructure and privacy compromise of subscribers.

The goal of SS7map is to provide a global overview by building the first SS7 signaling network world map revealing how vulnerable and exposed are telecom operators and their subscribers. We explain how it is possible for each mapped network to abuse legitimate signalling messages and call flows to discover and fingerprint equipment, intercept SMS messages, and perform massive location tracking of subscribers. More than pure analysis of vulnerability, this map rates and ranks the vulnerability of countries and operators showing discrepancies in the level and type of protection: SCCP screening, SS7 policing, MAP filtering, rate limiting, Network Element security configurations. We then conclude on the direction of signaling security and its current trend and development in the LTE world that shares many similar design insecurities with SS7.</description>

<persons>

<person id="5170">Laurent Ghigonis</person>

<person id="5328">Alexandre De Oliveira</person>

</persons>

<links/>

</event>

</room>

</day>

<day date="2014-12-28" end="2014-12-29T04:00:00+01:00" index="2" start="2014-12-28T11:30:00+01:00">

<room name="Saal 1">

<event guid="Km3oA97mSXAMOZGte\_v8Fg" id="6196">

<date>2014-12-28T11:30:00+01:00</date>

<start>11:30</start>

<duration>01:00</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6196\_-\_en\_-\_saal\_1\_-\_201412281130\_-\_switches\_get\_stitches\_-\_eireann\_leverett</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Switches Get Stitches</title>

<subtitle>Industrial System Ownership</subtitle>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>This talk will introduce you to Industrial Ethernet Switches and their vulnerabilities. These are switches used in industrial environments, like substations, factories, refineries, ports, or other other homes of industrial automation. In other words: DCS, PCS, ICS &amp; SCADA switches. It is a very good companion talk to Damn Vulnerable Chemical Process? Own your own critical infrastructures today!</abstract>

<description>This talk will introduce you to Industrial Ethernet Switches and their vulnerabilities. These are switches used in industrial environments, like substations, factories, refineries, ports, or other other homes of industrial automation. In other words: DCS, PCS, ICS &amp; SCADA switches.

The researchers focus on attacking the management plane of these switches, because we all know that industrial system protocols lack authentication or cryptographic integrity. Thus, compromising any switch allows the creation of malicious firmwares for further MITM manipulation of a live process.

Not only will vulnerabilities be disclosed for the first time (exclusively at 31C3), but the methods of finding those vulnerabilities will be shared. All vulnerabilities disclosed will be in the default configuration state of the devices. While these vulnerabilities have been responsibly disclosed to the vendors, SCADA/ICS patching in live environments tends to take 1-3 years. At least three vendors switches will be examined: Siemens, GE, Garrettcom.

Therefore, this presentation matters to any hackers or anarchists, who believe they have a right to examine the resilience and security of the infrastructures that support their communities.

Own your own critical infrastructures today!

</description>

<persons>

<person id="4081">Eireann Leverett</person>

</persons>

<links/>

</event>

<event guid="DvpNPWPGVgSqGcOI1WK45g" id="6308">

<date>2014-12-28T12:45:00+01:00</date>

<start>12:45</start>

<duration>01:00</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6308\_-\_en\_-\_saal\_1\_-\_201412281245\_-\_beyond\_pnr\_exploring\_airline\_systems\_-\_saper</slug>

<recording>

<license>CC-BY-3.0</license>

<optout>false</optout>

</recording>

<title>Beyond PNR: Exploring airline systems</title>

<subtitle/>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>Ever wondered what the cryptic &lt;code&gt;QNY27R&lt;/code&gt; on your airline reservaton means? This talk explores typical computing environment as seen in the air transport industry. Discover ancient software, old communication protocols and cryptic systems. What data are stored and how they are exchanged to keep the air transport industry running. </abstract>

<description>&lt;h2&gt;Airport environment&lt;/h2&gt;

&lt;ul&gt;

&lt;li&gt;Air traffic control systems&lt;/li&gt;

&lt;li&gt;Flight information systems (FIDS)&lt;/li&gt;

&lt;li&gt;Terminal environment&lt;/li&gt;

&lt;li&gt;Baggage control&lt;/li&gt;

&lt;li&gt;Access control&lt;/li&gt;

&lt;li&gt;Networks and networks&lt;/li&gt;

&lt;/ul&gt;

&lt;h2&gt;Airline environment&lt;/h2&gt;

&lt;ul&gt;

&lt;li&gt;Reservations/ticketing&lt;/li&gt;

&lt;li&gt;Airline inventory&lt;/li&gt;

&lt;li&gt;Departure control (check-in)&lt;/li&gt;

&lt;li&gt;Flight management&lt;/li&gt;

&lt;li&gt;Load control&lt;/li&gt;

&lt;li&gt;Avionics&lt;/li&gt;

&lt;li&gt;In-flight entertainment&lt;/li&gt;

&lt;/ul&gt;

&lt;h2&gt;Global Distribution Systems&lt;/h2&gt;

&lt;ul&gt;

&lt;li&gt;SABRE&lt;/li&gt;

&lt;li&gt;Galileo&lt;/li&gt;

&lt;li&gt;Worldspan&lt;/li&gt;

&lt;li&gt;Amadeus&lt;/li&gt;

&lt;/ul&gt;

&lt;h2&gt;Your data with the airline&lt;/h2&gt;

&lt;ul&gt;

&lt;li&gt;Passenger Name Record&lt;/li&gt;

&lt;li&gt;Departure control data&lt;/li&gt;

&lt;li&gt;Electronic Ticket&lt;/li&gt;

&lt;li&gt;Frequent Travel Data&lt;/li&gt;

&lt;/ul&gt;

&lt;h2&gt;No human is illegal&lt;/h2&gt;

&lt;ul&gt;

&lt;li&gt;APIS data&lt;/li&gt;

&lt;li&gt;TIMATIC&lt;/li&gt;

&lt;li&gt;PAXLST message&lt;/li&gt;

&lt;li&gt;APP/AQQ&lt;/li&gt;

&lt;li&gt;PNR data exported to the US&lt;/li&gt;

&lt;/ul&gt;

&lt;h2&gt;Communication networks and protocols&lt;/h2&gt;

&lt;ul&gt;

&lt;li&gt;Telex&lt;/li&gt;

&lt;li&gt;SITA network&lt;/li&gt;

&lt;li&gt;AIRIMP manual&lt;/li&gt;

&lt;/ul&gt;

&lt;h2&gt;Typical airport workstation&lt;/h2&gt;

&lt;ul&gt;

&lt;li&gt;Terminal emulated on PC&lt;/li&gt;

&lt;li&gt;Boarding pass printers (thermal)&lt;/li&gt;

&lt;li&gt;Bag tag printers&lt;/li&gt;

&lt;li&gt;Document printers (dot matrix)&lt;/li&gt;

&lt;li&gt;Device standarization&lt;/li&gt;

&lt;/ul&gt;

&lt;h2&gt;Software enviroment&lt;/h2&gt;

&lt;ul&gt;

&lt;li&gt;Direct terminal access&lt;/li&gt;

&lt;li&gt;(Java-based) Terminal emulators&lt;/li&gt;

&lt;li&gt;CUTE enviroment&lt;/li&gt;

&lt;li&gt;Departure from direct mainframe access: EDI&lt;/li&gt;

&lt;/ul&gt;

</description>

<persons>

<person id="2680">saper</person>

</persons>

<links>

<link href="http://pinboard.in/t:BeyondPNR">Collection of #BeyondPNR links</link>

<link href="http://saper.info/talk/31c3">Slide deck online</link>

</links>

</event>

<event guid="yMuYr5eW4o9FpJMw-NwXrg" id="6344">

<date>2014-12-28T14:00:00+01:00</date>

<start>14:00</start>

<duration>01:00</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6344\_-\_en\_-\_saal\_1\_-\_201412281400\_-\_security\_analysis\_of\_estonia\_s\_internet\_voting\_system\_-\_j\_alex\_halderman</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Security Analysis of Estonia's Internet Voting System</title>

<subtitle/>

<track>Ethics, Society &amp; Politics</track>

<type>lecture</type>

<language>en</language>

<abstract>Estonia is the only country in the world that relies on Internet voting in a significant way for legally-binding national elections — up to 30% of all voters cast their ballots online. This makes the security of Estonia's Internet voting system of interest to technologists and citizens the world over. Over the past year, I helped lead the first rigorous, independent security evaluation of the system, based on election observation, code review, and laboratory testing. The findings are alarming: there are staggering gaps in Estonia's procedural and operational security, and the architecture of the system leaves it open to cyberattacks from foreign powers. Our investigation confirmed the viability of these attacks in the lab, but the Estonian government has chosen to downplay them. We urgently recommend that Estonia discontinue use of the system before the country suffers a major attack.</abstract>

<description>When Estonia introduced its online voting system in 2005, it became the first country to offer Internet voting nationally. Today, people around the world look to Estonia's example, and some wonder why they can't vote online too. Nevertheless, the system remains controversial. While many Estonians view Internet voting as a source of national pride, one major political party has repeatedly called for it to be abandoned.

Over the past year, I took part in the first rigorous and fully independent security analysis of the Estonian Internet voting system. My team observed operations during the October 2013 and May 2014 elections, conducted interviews with the system developers and election officials, assessed the software through source code review and reverse engineering, and performed tests on a reproduction of the complete system in our lab.

The threats facing national elections have shifted significantly since the Estonian system was designed more than a decade ago. State-level cyberattacks, once a largely hypothetical threat, has become a well documented reality, and attacks by foreign states are now a credible threat to a national online voting system. To test the feasibility of such attacks, we reproduced the I-voting system and played the role of a sophisticated attacker during a mock election. We developed client-side attacks that silently steal votes on voters' own computers We also demonstrated server-side attacks that target introduce malware into the vote counting server, allowing a foreign power or dishonest insider to shifting results in favor of their preferred candidate.

These risks are even more serious because of deviations from procedure and serious lapses in operational security that we observed during real elections. Election workers downloaded security-critical software over unsecured Internet connections, typed server root passwords in full view of observers and public video cameras, and prepared election software for distribution to the public on insecure personal computers, among other examples. These actions indicate a dangerously inadequate level of professionalism in security administration that leaves the whole system open to attack and manipulation.

When we made our study public in Estonia, government responses ranged from dismissive to absurd. Officials discounted them, and the President and Prime Minister insinuated that we had been bought off by a rival political party. We hope that the country can separate technical reality from politics in time to avert a major attack. For other countries that are considering adopting Internet voting, we hope that the weaknesses of the Estonian system can be an important cautionary lesson.</description>

<persons>

<person id="4228">J. Alex Halderman</person>

</persons>

<links>

<link href="https://estoniaevoting.org">Website about our study</link>

<link href="https://jhalderm.com/pub/papers/ivoting-ccs14.pdf">Our full research paper</link>

</links>

</event>

<event guid="psS7-V3-VqYDuiKCr5PmWg" id="6131">

<date>2014-12-28T16:00:00+01:00</date>

<start>16:00</start>

<duration>00:30</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6131\_-\_en\_-\_saal\_1\_-\_201412281600\_-\_safer\_playing\_with\_lasers\_-\_sarah</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Safer playing with lasers</title>

<subtitle/>

<track>Hardware &amp; Making</track>

<type>lecture</type>

<language>en</language>

<abstract>How to play with lasers without injuring Yourself and others and how to design the safety circuits of a laser system.</abstract>

<description>This talk covers:

Laser classification

Laser safety

Effects of laser radiation to tissue and eyes

Real world don'ts

Other dangers of laser systems

What to do to be safe

Technical implementation of safety systems

Relevant standards</description>

<persons>

<person id="4642">Sarah</person>

</persons>

<links/>

</event>

<event guid="rHjqtfbslD\_ucUr8kW5wcQ" id="6236">

<date>2014-12-28T16:45:00+01:00</date>

<start>16:45</start>

<duration>00:30</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6236\_-\_en\_-\_saal\_1\_-\_201412281645\_-\_iridium\_pager\_hacking\_-\_sec\_-\_schneider</slug>

<recording>

<license>public domain</license>

<optout>false</optout>

</recording>

<title>Iridium Pager Hacking</title>

<subtitle/>

<track>Hardware &amp; Making</track>

<type>lecture</type>

<language>en</language>

<abstract>The chronicles of reversing the Iridium pager system.</abstract>

<description>The Iridium satellite system provides voice and data coverage to satellite phones, pagers and integrated transceivers over Earth's entire surface. It was built by Motorola over 15 years ago, and parts of it remain unchanged to this day.

Iridium pagers are similar to other pager systems from that time (they are receive-only devices) with the benefit that they will work anywhere on earth. Additionally they work on a receiver-pays subscription model, and due to their age are probably not using cryptography.

Broadcasting messages all over the world sounds interesting enough to take a closer look. As Iridium is a proprietary system, documentation is scarce and hard to come by. But with the rise of software defined radio we can take a peek at what happens over the air...

</description>

<persons>

<person id="2506">Sec</person>

<person id="5339">schneider</person>

</persons>

<links/>

</event>

<event guid="lWgvj2btOjK-\_XxUtIs-qw" id="6358">

<date>2014-12-28T17:30:00+01:00</date>

<start>17:30</start>

<duration>00:30</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6358\_-\_en\_-\_saal\_1\_-\_201412281730\_-\_information\_control\_and\_strategic\_violence\_-\_anita\_gohdes</slug>

<recording>

<license>CC-BY-3.0</license>

<optout>false</optout>

</recording>

<title>Information Control and Strategic Violence</title>

<subtitle>How governments use censorship and surveillance as part of their violent repressive tactics</subtitle>

<track>Science</track>

<type>lecture</type>

<language>en</language>

<abstract>Simple access to social media and cell phone has widely been accepted as a positive tool for citizens to voice dissatisfaction with their government and coordinate protest. But why would rulers permit these tools if they merely pose a threat to their own survival? This talk will investigate how a government’s ability to censor and limit the flow of information feeds into its choice of violent responses to protest. I will talk about the conditions under which a government is likely to benefit more from surveilling the free flow of information, and under which conditions it is more likely to benefit from censorship.

</abstract>

<description>A few weeks before the first mass protests ensued across Syria in March 2011, the Regime led by President Bashar Al-Assad lifted a large number of bans on social networking platforms, including Facebook and Youtube. Up to that point, the Regime had controlled the most regulated media landscape and telecommunications market in the Middle East, which is why the move towards providing access to social media sites not even permitted in China was not something to be expected. Why, after all these years of extreme censorship, does a government suddenly permit free access to, and generation of, information?

The ability to connect via large social network platforms has been celebrated as an important way for ordinary citizens to collectively organise protest in light of repressive rulers. The revolutions in the Middle East and North Africa have spurred a new and important research area on the effects of digital communication technology on citizen’s propensity to voice dissent and organise protest and resistance. The fact that anyone with a working network connection can now access, generate, and exchange content on the internet has been termed a ‘game changer’ for authoritarian regimes intent on maintaining control in light of mass popular protest.

What has remained largely unanswered, is how regimes resolved to stay in power can make use of their ability to surveil, censor, and limit the flow of information in an age where the majority of communication has been relegated to the inter- net and mobile phones. Understanding the way in which this new form of control feeds into more traditional means of repression, such as the use of extreme forms of physical coercion, is a crucial part of this process. In this talk, I will discuss under which conditions the free flow of information is likely to prove helpful in conducting effective state repression, and under which conditions the censoring of information access is likely to be more beneficial.

Regimes intent on maintaining power against all adversaries have long since combined the use of censorship with physical violations of those deemed threatening to their position. The introduction of digital communication technology has, however, altered the costs and benefits of limiting the flow of information when conducting coercive campaigns. When Syria’s government decided to unblock social networking sites, it might thus have simultaneously increased its intelligence for counterinsurgency operations, while also providing new ways of collective action for the opposition. Investigating these changes and how they affect the tactics of state violence is a crucial first step in understanding how contemporary and future governments are likely to incorporate their control of communication technology into strategies of repression.

I use supervised machine-learning to analyze over 60,000 records of killings perpetrated by the Syrian Regime in the ongoing conflict, and classify them according to their event circumstances, to arrive at a categorization between targeted and untargeted acts of repression. I find that higher levels of information accessibility are consistently linked to an increase in the proportion of targeted repression, whereas areas with little or no access witness more indiscriminate campaigns of violence.

</description>

<persons>

<person id="5080">Anita Gohdes</person>

</persons>

<links/>

</event>

<event guid="xmlu4jFXkob2t8CUHi0Rng" id="6294">

<date>2014-12-28T18:15:00+01:00</date>

<start>18:15</start>

<duration>00:30</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6294\_-\_de\_-\_saal\_1\_-\_201412281815\_-\_vor\_windows\_8\_wird\_gewarnt\_-\_ruedi</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Vor Windows 8 wird gewarnt</title>

<subtitle>Und nichts (Secure) Bootet mehr?</subtitle>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>de</language>

<abstract>Im Vortrag sollen technische und gesellschaftliche Konsequenzen der von Microsoft kontrollierten Windows-8-Secure-Boot-Architektur und mögliche Gegenmaßnahmen diskutiert werden.</abstract>

<description>Nachdem die Einführung einer Microsoft-kontrollierten Sicherheitsinfrastruktur durch politischen Widerstand lange aufgehalten werden konnte, hat Microsoft inzwischen ein weiteres Mal Fakten geschaffen. In den Hardwareanforderungen für Windows 8 wird Secure Boot verpflichtend vorausgesetzt. Andere Betriebssysteme können in der Praxis bisher nur mit technisch und rechtlich problematischen Notkonstruktionen gestartet werden.

Für die stark wachsende ARM-Prozessorwelt soll dem Nutzer sogar komplett die Kontrolle entzogen werden. Dies beinhaltet sogar eine Zwangsaktivierung und ein Verbot der Deaktivierung des Microsoft-kontrollierten Secure-Boot-Prozesses.

Was vielen lange Zeit als der bekannte Kampf zwischen Hackern und Microsoft um die freie Nutzung unserer Gerätschaften erschien, erhielt durch die politischen Entwicklungen höchste Brisanz für die gesamte Industrie. Microsoft kann und hat auch schon ohne nachvollziehbare Begründung konkurrierende Bootloader deaktiviert.

Ein Szenario, dass Microsoft (möglicherweise durch US-Regierungsdruck) die Berechtigung für die von Microsoft unterschriebene Bootloader für Linux-Distributionen zurückzieht, will man sich insbesondere für sicherheitskritische Systeme oder eingebettete Systeme nicht wirklich vorstellen.

Während deutsche Behörden darüber diskutieren, wie sehr vor Windows 8 gewarnt werden sollte, verbot China völlig die Verwendung von Windows 8 auf staatlichen Computern.

Im Vortrag sollen weitere technische und gesellschaftliche Konsequenzen vom Microsoft-kontrollierten Sicherheitsinfrastrukturen und mögliche Gegenmaßnahmen diskutiert werden.</description>

<persons>

<person id="1545">ruedi</person>

</persons>

<links/>

</event>

<event guid="defd3b01-c39d-433f-b3c4-dbea1ea2fe00" id="6595">

<date>2014-12-28T19:00:00+01:00</date>

<start>19:00</start>

<duration>00:30</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6595\_-\_en\_-\_saal\_1\_-\_201412281900\_-\_hard\_drive\_punch\_-\_aram\_bartholl</slug>

<recording>

<license>CC-BY-3.0</license>

<optout>false</optout>

</recording>

<title>»Hard Drive Punch«</title>

<subtitle>Destroying data as a performative act</subtitle>

<track>Art &amp; Culture</track>

<type>lecture</type>

<language>en</language>

<abstract>In general data is stored on technically sensitive systems and can easily be lost. At the same time files today appear often as indestructible once uploaded to the Internet.</abstract>

<description>In this presentation I will talk about a variety of approaches on data destruction and how these connect to current events and questions in society. From professional hard drive punch systems and art projects to DIY thermite melting, the art of destroying data is a wide spread cultural phenomenon.

Workshop: Bring your old hard drives to have them crushed with the IDEAL 0101 hard drive punch or cut the data platter yourself by hand.

Competition: You think you can still recover files from this drive? Which methods are the best?

</description>

<persons>

<person id="4383">Aram Bartholl</person>

</persons>

<links>

<link href="http://datenform.de">Aram Bartholl</link>

</links>

</event>

<event guid="1NE5joYD0o-gaf5SqL-1Nw" id="6258">

<date>2014-12-28T20:30:00+01:00</date>

<start>20:30</start>

<duration>01:00</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6258\_-\_en\_-\_saal\_1\_-\_201412282030\_-\_reconstructing\_narratives\_-\_jacob\_-\_laura\_poitras</slug>

<recording>

<license>CC-BY-3.0</license>

<optout>false</optout>

</recording>

<title>Reconstructing narratives</title>

<subtitle>transparency in the service of justice</subtitle>

<track>Ethics, Society &amp; Politics</track>

<type>lecture</type>

<language>en</language>

<abstract>Surveillance, cryptography, terrorism, malware, economic espionage, assassination, interventions, intelligence services, political prisoners, policing, transparency, justice and you.</abstract>

<description>Structural processes and roles are designed to create specific outcomes for groups. Externally facing narratives are often only one of many and they seek to create specific outcomes by shaping discourse. We will cover a wide range of popular narratives surrounding the so-called Surveillance State. We intend to discuss specific historical contexts as well as revealing new information as part of a longer term research project.</description>

<persons>

<person id="1083">Jacob</person>

<person id="5258">Laura Poitras</person>

</persons>

<links/>

</event>

<event guid="gRbk7OprwZBqF3cv0NddMQ" id="6156">

<date>2014-12-28T21:45:00+01:00</date>

<start>21:45</start>

<duration>01:00</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6156\_-\_en\_-\_saal\_1\_-\_201412282145\_-\_fernvale\_an\_open\_hardware\_and\_software\_platform\_based\_on\_the\_nominally\_closed-source\_mt6260\_soc\_-\_bunnie\_-\_xobs</slug>

<recording>

<license>CC-BY-SA 3.0</license>

<optout>false</optout>

</recording>

<title>Fernvale: An Open Hardware and Software Platform, Based on the (nominally) Closed-Source MT6260 SoC</title>

<subtitle>A Lawful Method for Converting Closed IP into Open IP</subtitle>

<track>Hardware &amp; Making</track>

<type>lecture</type>

<language>en</language>

<abstract>We introduce Fernvale, a reverse-engineered, open hardware and software platform based upon Mediatek's MT6260 value phone SoC. The MT6260 is the chip that powers many of the $10 GSM feature phones produced by the Shanzhai.

Fernvale is made available as open-licensed schematics, board layouts, and an RTOS based upon the BSD-licensed NuttX, as well as a suite of open tools for code development and firmware upload. We discuss our technical reverse engineering efforts, as well as our methodology to lawfully import IP from the Shanzhai ecosystem into the Maker ecosystem. We hope to establish a repeatable, if not labor-intensive, model for opening up previously closed IP of interest, thereby outlining a path to leveling the playing field for lawful Makers.

</abstract>

<description>There is a set of technology which Makers are legally allowed access, and there is a much larger set of technology which is used to make our every day gadgets. Access to the best closed-source technology is prevented via barriers such as copyright (limiting your ability to learn how it works), patent (limiting your ability to make something similar), and supply-chain (limiting your ability to buy it). As a result, open-licensed, Maker-friendly technologies have trailed closed-source technology in terms of cost, performance, and features.

Makers operating under Western IP law are legally bound by these barriers, and are forced to settle for Arduinos, Beaglebones, Raspberry Pis and Novenae. However, all of these are a far cry in terms of cost, performance, and features from what consumers typically expect from boxes purchased in retail stores.

Our research into the Chinese ecosystem indicates there is another way. Originally marginalized as outlaws and copycats, the Shanzhai of China – China's counterpart to the Western hacker-maker – exist in a realm where copyright and patent barriers are permeable, a state which we refer to as 'gongkai'. As a result, knowledge and access to state of the art closed source technology has diffused into the Shanzhai ecosystem. Today, they have moved beyond the rote copying of Nokia, Samsung, and Apple, and have created a thriving, vibrant ecosystem where mobile technology is rip/mix/burned; their products are mass-produced at a rate of millions per month for the “rest of the world”, e.g. emerging markets such as Africa, Brazil, India, Indonesia, and Russia.

About a year ago, we did a tear-down of an example $12 phone, and contrasted it to the Arduino Uno. For $29, the Arduino Uno gets you a 16MHz, 8-bit CPU with 2.5k of RAM, and USB plus a smattering of GPIO as the sole interfaces. For $12, a phone out of the Chinese gongkai ecosystem gets you a 260 MHz, 32-bit CPU with 8MiB of RAM, with USB, microSD, SIM, quad-band GSM, Bluetooth, an OLED display and a battery. It begs the question of why, when Makers talk about IoT technologies in the West, they typically think of wifi-powered solutions in the $20-70 range, versus a GSM platform in the $10-$20 range.

In this lecture, we disclose an attempt to short-circuit the disclosure barrier. We are releasing an open hardware and software solution built around the Mediatek MT6260. The MT6260 is a 32-bit ARM7EJ-S SoC with 8MiB of PSRAM in-package, as well as USB, LCD, touchscreen, audio, Bluetooth, quad-band GSM, dual-SIM, FM radio, UART, keypad, SD card, camera, and other peripherals integrated. The chip can be purchased on the over-the-counter market for about $2-3 in China. We call our solution built around this chip “Fernvale”.

Fernvale is similar to the “LinkIt ONE” recently released by Mediatek and Seeed Studios, based upon the MT2502A SoC and targeted at IoT and wearables. LinkIt indicates a new direction for Mediatek and we are optimistic that their effort indicates a new pattern of openness toward Makers. At the time of this proposal's submission, the details of the LinkIt ONE platform are still unfolding, but the basic feature set looks comparable to that of Fernvale. However, it seems the LinkIt SDK is still based upon a closed-source Nucleus RTOS providing services to an open Arduino-like API.

Unlike LinkIt ONE, Fernvale runs a port of NuttX, a small-footprint BSD-licensed RTOS that is Posix and ANSI compliant, and includes a partial set of drivers for the available hardware peripherals. The mainboard is laid out to function as either a SoM (system on module) or as a truncated Arduino shield (with the appropriate headers populated), and focuses on the computational abilities of the platform. In other words, Fernvale is not positioned as a mobile phone solution per se, but rather as an Engineering Development Kit (EDK) for embedded applications that can benefit from a highly-integrated, low-cost high-performance microcontroller solution such as the MT6260. As a result, the mainboard breaks out a selection of GPIO as well as the speaker, battery, USB, and SD card interfaces. The mainboard also serves as a base platform for rallying a larger community of developers who can aid with the task of reverse engineering and writing legally open drivers for its massive peripheral set.

Two expansion headers are provided on the mainboard. A larger UX header can be used to attach a keypad + LCD + audio interface, for applications that require UI elements. A smaller analog header enables users to attach an RF front-end of their choosing, which could potentially enable GSM-compatible voice and data services, if drivers were to exist.

This lecture will also discuss our experiences reverse engineering, and our approach to open-sourcing the MT6260. We had to reverse engineer significant portions of the system, including but not limited to circuit board layouts, hardware configuration options, bootloader protocols, partial register maps, and the internal boot ROM of the SoC. This reverse engineering effort was necessary to create a blob-free software implementation, and to give developers an alternative to Mediatek's proprietary firmware flashing utilities to upload code. It was also necessary to create schematics and circuit board maskworks which have an original copyright thereby giving us the right to pick an open license for the hardware designs.

We took special pains to ensure our method was lawful and the resulting work is copyright-clean under U.S. law. We did review some non-open-licensed chip documentation and code examples available for download from open file-sharing sites. None of these materials were restricted by DRM. American copyright law contains a fair-use exception that allows limited copying and examination of such materials for the purpose of understanding the ideas and functional concepts embodied in them. We believe our download and review of those materials is fair use. Should potential copyright holders disagree with our interpretation, we invite any offended parties to engage us in rational discourse.

We believe that Makers have for too long lived in the shadow of overbearing copyright laws. We need to develop an example of how to import ideas from less strict IP jurisdictions where innovation is flourishing; failing this, hardware Makers run the risk of being eternally behind the Shanzhai. Fernvale is our first attempt at developing a legal context for importing IP from the gongkai ecosystem into a fully open source solution; we hope our example will embolden other developers to pursue more ambitious targets. We also hope our work may, in the long term, catalyze meaningful Maker-friendly reform to Western IP law by raising awareness of the disparity between East and West, with the success of the Shanzhai serving as evidence of how permissive IP policy can be good for both grass-roots innovators (the Shanzhai) and big businesses (Mediatek and the phone network operators) alike.

</description>

<persons>

<person id="3155">bunnie</person>

<person id="4376">Xobs</person>

</persons>

<links/>

</event>

<event guid="6bXRd7c5UJbIlb4QiTd1ng" id="6321">

<date>2014-12-28T23:00:00+01:00</date>

<start>23:00</start>

<duration>00:30</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6321\_-\_en\_-\_saal\_1\_-\_201412282300\_-\_the\_matter\_of\_heartbleed\_-\_zakir\_durumeric</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>The Matter of Heartbleed</title>

<subtitle>What went wrong, how the Internet reacted, what we can learn for the future</subtitle>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>The Heartbleed vulnerability took the Internet by surprise in April of this year. The vulnerability was one of the most consequential in the history of the Internet, since it allowed attackers to potentially steal login credentials, cryptographic keys, and other private data from up to half of all popular HTTPS sites. In this talk, we take a detailed look at Heartbleed and its aftermath, based on comprehensive measurements and analysis that our research team performed over the past six months. We began tracking Heartbleed's impact within hours of its disclosure using massive ZMap scans and large network telescopes. This allowed us to track which sites remained vulnerable, observe certificate revocations, and monitor for large scale attacks in close to real time. Based on this data, we also conducted one of the largest ever mass vulnerability notifications, informing the network administrators for all devices still susceptible to Heartbleed across the entire IPv4 address space. Finally, we investigated the question of whether attackers knew about and exploited Heartbleed prior to its public disclosure---and we will present new details about this question in the talk. We hope that by learning from the Heartbleed security disaster, our community can prepare to respond more effectively to such events in the future. </abstract>

<description>&lt;p&gt;In March 2014, researchers found a catastrophic vulnerability in OpenSSL, the cryptographic library used to secure connections in popular servers including Apache and Nginx. The bug allowed attackers to extract cryptographic keys, login credentials, and other private data from an estimated 22-55% of HTTPS sites. Worsening its severity, the bug was both simple to understand and exploit.&lt;/p&gt;

&lt;p&gt;We used ZMap to perform comprehensive scans of the IPv4 address space and popular web servers in the days and months following disclosure. We provide more extensive estimates on who was originally vulnerable, track who patched their sites, and replaced certificates. We will present exactly which server products and devices were vulnerable. We will further discuss how Heartbleed affected the HTTPS CA ecosystem. Worryingly, we find that only 10% of the known vulnerable sites replaced their certificates within the next month, and of those that did, 14% neglected to change the private key, gaining no protection from certificate replacement! We'll also present the shortcomings in the public key infrastructure that Heartbleed unearthed and problems our community needs to focus on moving forward.&lt;/p&gt;

&lt;p&gt;We investigated widespread attempts to exploit Heartbleed post disclosure at four network sites. We will discuss the subsequent exploit attempts we observed from almost 700 sources and the Internet-wide scans that started post disclosure. We also investigated whether exploit attempts took place prior to Heartbleed's public disclosure, including examining suspicious network traces recorded months earlier. We will disclose new details of these traces and their implications in the talk.&lt;/p&gt;

&lt;p&gt;Even with global publicity, Heartbleed patching plateaued after two weeks. To try to help, we notified network administrators responsible for more than 500,000 unpatched systems. While much of the security community (including us!) assumed that mass vulnerability notifications would be too difficult or ineffective, we found that it increased the Heartbleed patching rate by nearly 50%. We will discuss how we performed these notifications, the reactions of network operators, and prospects for performing automatic mass notifications based on Internet-wide scanning in future vulnerability events.&lt;/p&gt;

&lt;p&gt;Throughout the talk, we will use real world data to frame what went well and what went poorly in the Internet's response to Heartbleed. The vulnerability's severe risks, widespread impact, and costly global cleanup qualify it as a security disaster. However, by understanding what went wrong and learning from it, the Internet security community can be better prepared to address major security failures in the future.&lt;/p&gt;</description>

<persons>

<person id="5006">Zakir Durumeric</person>

</persons>

<links>

<link href="https://jhalderm.com/pub/papers/heartbleed-imc14.pdf">The Matter of Heartbleed Research Paper</link>

<link href="https://zmap.io/heartbleed/">ZMap Heartbleed Health Report</link>

<link href="https://jhalderm.com">Alex Halderman's web site</link>

<link href="https://zakird.com">Zakir Durumeric's web site</link>

</links>

</event>

<event guid="4aOXU9cdQYbirV0Q-k5usw" id="6212">

<date>2014-12-28T23:30:00+01:00</date>

<start>23:30</start>

<duration>00:30</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6212\_-\_en\_-\_saal\_1\_-\_201412282330\_-\_heartache\_and\_heartbleed\_the\_insider\_s\_perspective\_on\_the\_aftermath\_of\_heartbleed\_-\_nick\_sullivan</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Heartache and Heartbleed: The insider’s perspective on the aftermath of Heartbleed</title>

<subtitle>The untold story of what really happened, how it was patched and what was learned.</subtitle>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>Two weeks after the Heartbleed bug was announced, CloudFlare patched the Heartbleed bug, created a challenge to prove the bug could be used to find private keys (uncovering a second bug in OpenSSL) and turned its entire network into a giant honeypot. This session will discuss the specific steps taken to prevent early disclosure, creating and scaling the first public vulnerability test, how the CloudFlare Heartbleed challenge showed that you can reveal private SSL keys (how a second bug in OpenSSL made this possible) the incredible impact of revoking over 100,000 certificates in a single day, and the results of our honeypot revealing the proportion of attack traffic versus research traffic. </abstract>

<description>CloudFlare was notified about Heartbleed as soon as it was discovered--ahead its public announcement--and took extreme precaution to not reveal anything about the bug. This required communicating only over secure channels, restricting the visibility of the branch from which we built the workaround, and using secure software deployment methods.

After the patch was announced, there was a rush to reverse engineer the bug and create an exploit. The cloudFlare team immediately started working proof of concept, and hosted it on a website allowing others to scan for vulnerable sites. Within minutes, the original site was flooded with requests. CloudFlare’s Nick Sullivan will share this process and the feats pulled off to make sure the site could scale and provide accurate results. He will go into the numbers and technical details of the PoC and speak about its bugs and how they were found. Statistics and anonymized raw data of the 70+ millions of results will be provided, giving an overview of the patching process over time.

It was clear soon after the bug was revealed that the number of servers affected by this bug was massive. What wasn’t clear was the scope of data that was vulnerable to attack. In order to determine the risk to private keys from this vulnerability, his team launched the CloudFlare Heartbleed Challenge. They set up a site that was vulnerable to the attack, added logging and created a webpage to submit a signed proof of key ownership. In less than a day, there were several successful submissions. Nick will go over the naive (but successful) strategy used to extract keys and the more advanced technique based on Coppersmith’s Method. Finally he will discuss the \*second\* OpenSSL bug we discovered that allowed the private key to be extracted via Heartbleed.

After the exploits were in the wild, his team added logging to see who was trying to exploit this bug. Nick will reveal the results of this analysis and cross-reference the results with the IPs of the test site. These numbers give new insight into how many people were attempting to maliciously exploit this flaw versus research done to probe vulnerable sites.

Once the dust settled and the team worked out the details with our CA, we revoked over 80,000 of CloudFlare’s SSL certificates. This turned into an internet scaling nightmare, resulting in a constant flood of more than 40 gigabits per second of traffic to serve overgrown certificate revocation lists. Since CloudFlare provides caching for its CA, the team bore the brunt of this traffic. Their revocation lists would have DDoSed most sites (and some certificate authorities) off the internet. Nick will talk about caching CRLs, and how the revocation system was not designed for this scale of internet flaw.

In conclusion we he will summarize the many ways this coding error revealed some of the deeper flaws in the internet, and discuss ways we can move forward. Nick will share actionable advice and the security strategies used by cloud service companies on how to monitor the way companies store keys internally.

Attendees will leave with actionable advice on how to better secure their own systems against the next Heartbleed and the security strategies used by cloud service companies on how to monitor the way companies store keys internally.</description>

<persons>

<person id="5003">Nick Sullivan</person>

</persons>

<links>

<link href="http://blog.cloudflare.com/answering-the-critical-question-can-you-get-private-ssl-keys-using-heartbleed">Answering the Critical Question: Can You Get Private SSL Keys Using Heartbleed?</link>

<link href="http://blog.cloudflare.com/the-results-of-the-cloudflare-challenge">The Results of the CloudFlare Challenge</link>

<link href="http://blog.cloudflare.com/the-hard-costs-of-heartbleed">The Hidden Costs of Heartbleed</link>

</links>

</event>

<event guid="Mw1wjnNzwxzSkM3Ip5Lg0g" id="6109">

<date>2014-12-29T00:15:00+01:00</date>

<start>00:15</start>

<duration>01:30</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6109\_-\_de\_-\_saal\_1\_-\_201412290015\_-\_fnord\_news\_show\_-\_frank\_-\_fefe</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Fnord News Show</title>

<subtitle>Wir helfen Euch die Fnords zu sehen.</subtitle>

<track>Entertainment</track>

<type>lecture</type>

<language>de</language>

<abstract>Im Format einer lockeren Abendshow werden wir die Nachrichten-Highlights des Jahres präsentieren, die Meldungen zwischen den Meldungen, die subtilen Sensationen hinter den Schlagzeilen.</abstract>

<description>Kommen Sie, hören Sie, sehen Sie! Lassen Sie sich mitreißen!</description>

<persons>

<person id="1633">frank</person>

<person id="1621">Fefe</person>

</persons>

<links/>

</event>

</room>

<room name="Saal 2">

<event guid="1116a02b-0312-4949-9921-d605148bfccb" id="6573">

<date>2014-12-28T11:30:00+01:00</date>

<start>11:30</start>

<duration>01:00</duration>

<room>Saal 2</room>

<slug>31c3\_-\_6573\_-\_en\_-\_saal\_2\_-\_201412281130\_-\_from\_computation\_to\_consciousness\_-\_joscha</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>From Computation to Consciousness</title>

<subtitle>How computation helps to explain mind, universe and everything</subtitle>

<track>Science</track>

<type>lecture</type>

<language>en</language>

<abstract>How can the physical universe give rise to a mind? I suggest to replace this confusing question by another one: what kind of information processing system is the mind, and how is the mind computed? As we will see, even our ideas of the physical universe turn out to be computational. Let us explore some fascinating scenery of the philosophy underlying Artificial Intelligence.</abstract>

<description>How do minds work? In my view, this is the most interesting question of all, and our best bet at answering it lies in building theories that we can actually test in the form of computer programs, that is, in building Artificial Intelligence. Let us explore some of the philosophical ideas that explicitly or implicitly form the basis of Artificial Intelligence.

The idea that minds are some kind of machine, mechanical contraptions, seems to be unconvincing, even offending to many people, even if they accept that the physical universe is a machine, and minds are part of that universe. Computer science has revolutionized our concept of machines, though: no longer do we see machines as mechanical arrangements of parts that pull and push against each other, but as arbitrary, stable causal arrangements that perform regular changes on their environment. We can think about mathematical machines, like cellular automatons, about financial, social or ecological machines. Machines do not have to be human-made artifacts, they are a way of conceptualizing regular processes and dynamic systems. In the case of conceptualizing the human mind, what matters is not biology, chemistry, or structural properties of the brain, but what these implement: a class of machine that is capable to process information, in very specific ways. The mind is not necessarily a mechanical machine, but certainly an information processing machine, a computational system.

Computationalism is the notion that minds can and have to be modeled as computational, and in its strong form, it maintains that the mind actually \_is\_ a computer, implemented by a physical mechanism. But the ideas of computation have permeated our understanding of the world even further. Our understanding of physics no longer conforms to mechanical world views (i.e. parts and particles pulling and pushing against each other), but requires us to switch to the broader notion of how the universe processes information. The foundational theories of physics are concerned with how the universe is computed.

In the view of universal computationalism, the question of what sort of thing minds are resolves into the question whether hypercomputation is possible, and if not, what classes of computation are involved in their functionality.

Computationalism systematizes the intuitions we get naturally while we program computers, and it helps us understand some of the deepest questions of cosmology, epistemology and the nature of the mind in ways that did not exist in the past.</description>

<persons>

<person id="4034">Joscha</person>

</persons>

<links/>

</event>

<event guid="e8e29f6a-11df-491a-acae-1253879ae8f9" id="6600">

<date>2014-12-28T12:45:00+01:00</date>

<start>12:45</start>

<duration>01:00</duration>

<room>Saal 2</room>

<slug>31c3\_-\_6600\_-\_en\_-\_saal\_2\_-\_201412281245\_-\_tell\_no-one\_-\_james\_bamford</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Tell no-one</title>

<subtitle>A century of secret deals between the NSA and the telecom industry</subtitle>

<track>Ethics, Society &amp; Politics</track>

<type>lecture</type>

<language>en</language>

<abstract>For nearly one hundred years, the NSA and its predecessors have been engaging in secret, illegal deals with the American telecom industry, with both virtually immune from prosecution.</abstract>

<description>How did this begin? How does it work? How much have US presidents known? What happens when they get caught? Will it change after the Snowden revelations? A fascinating look at a hundred years of handshakes and backroom deals between the eavesdroppers and the telecom executives. </description>

<persons>

<person id="5307">James Bamford</person>

</persons>

<links/>

</event>

<event guid="ELK9-ZQeFcqKxBYW8eay8g" id="5956">

<date>2014-12-28T14:00:00+01:00</date>

<start>14:00</start>

<duration>01:00</duration>

<room>Saal 2</room>

<slug>31c3\_-\_5956\_-\_en\_-\_saal\_2\_-\_201412281400\_-\_cyber\_necromancy\_-\_joseph\_tartaro\_-\_matthew\_halchyshak</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Cyber Necromancy</title>

<subtitle>Reverse Engineering Dead Protocols</subtitle>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>Reverse engineering is not all binaries and byte-code. The black art also extends to networks and unobtainable game servers. In this talk we go into the gruesome details of how we dug through the graveyards of console binaries and mausoleums of forgotten network protocols in order to stitch together the pieces necessary to bring our favorite game Metal Gear Online back to life.

We will be examining the process of reverse engineering the games custom network protocols in all angles from packet logs to low level disassembly of client code.</abstract>

<description>In this presentation we will be discussing the path we took to successfully develop our own private server for Metal Gear Online on the Sony PlayStation 2 and PlayStation 3 video game consoles. Interestingly enough this was a private server that was developed after the original was already taken offline, so we did not have a live active server to help with the reverse engineering. Due to this we ran into some issues but ultimately succeeded. We believe that the details of the techniques that we used will prove useful for anyone attempting similar actions in the future. The topics that we will discuss in this talk will cover a wide range of high and low level issues related to network protocol and binary reversing.

We will begin with an overall survey of the general problems faced by anyone attempting this type of work. The talk will quickly delve from the high-level and simple issues into the more technical aspects of reverse engineering in the blind. We will be including the techniques we used to determine the protocol and payload responses that the client was expecting. Describing in detail how we honed in on common traits that we expected to see on the network, using open source knowledge and binary level reverse engineering of client code to determine the expected response.

We expect the attendees of this talk to walk away with knowledge that will help them in the future when working on similar projects or any activities related to protocol reverse engineering.</description>

<persons>

<person id="4720">Joseph Tartaro</person>

<person id="4705">Matthew Halchyshak</person>

</persons>

<links/>

</event>

<event guid="66379bd1-4e68-4bcf-9d1e-0f4c38fbe78e" id="6582">

<date>2014-12-28T16:00:00+01:00</date>

<start>16:00</start>

<duration>00:30</duration>

<room>Saal 2</room>

<slug>31c3\_-\_6582\_-\_de\_-\_saal\_2\_-\_201412281600\_-\_das\_transparenzportal\_hamburg\_-\_lothar\_hotz</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Das Transparenzportal Hamburg</title>

<subtitle>Inhalt und Umsetzung</subtitle>

<track>Ethics, Society &amp; Politics</track>

<type>lecture</type>

<language>de</language>

<abstract>Im Vortrag wird die technische Umsetzung des Transparenzportals Hamburg vorgestellt.</abstract>

<description>Die Inhalte des Portals werden durch das Hamburger Transparenzgesetz bestimmt. Aufgrund der Vielzahl der anzubindenden heterogenen Systeme wurde eine umfassende Architektur entwickelt, die es erlaubt, über einen dezidierten Zugang

alle angebundenen Systeme zu erreichen. Der Zugang besteht aus einem Webportal sowie einer API, die die maschinelle Abfrage der Portalinhalte erlaubt.</description>

<persons>

<person id="5256">Lothar Hotz</person>

</persons>

<links/>

</event>

<event guid="oBQMMNfX5t-5TBIk3z6pOg" id="6295">

<date>2014-12-28T16:45:00+01:00</date>

<start>16:45</start>

<duration>00:30</duration>

<room>Saal 2</room>

<slug>31c3\_-\_6295\_-\_de\_-\_saal\_2\_-\_201412281645\_-\_krypto\_fur\_die\_zukunft\_-\_ruedi</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Krypto für die Zukunft</title>

<subtitle>Verteidigung gegen Dunkle Künste</subtitle>

<track>Science</track>

<type>lecture</type>

<language>de</language>

<abstract>(K)ein kleiner Rant über Elliptische Kurven, Quantencomputer, Bitcoins und die NSA et al.</abstract>

<description>1 Was würde Ihrer Meinung nach passieren, wenn ein funktionierender

Quantencomputer entwickelt würde? Auf welche Arten von Kryptografie

würde sich das wie auswirken?

Quantencomputer können mit Hilfe des Shor Algorithmus die gängigen

Public Key Verfahren, wie beispielsweise RSA und DSA, sehr effektiv

attackieren. Aber auch die neueren Verfahren, welche Elliptische

Kurven verwenden, sind betroffen. Für diese Angriffe benötigt man eine

von der Schlüssellänge abhängigen Anzahl von qubits. Elliptisch Kurven

Kryptosysteme nutzen deutlich kürzere Schlüssel, im Falle von Bitcoin

256 bit. Das klassische RSA System verwendet in der heutigen Praxis

mindestens 2048 bit.

2 Wären Bitcoins dann wertlos? Wenn ja, warum genau?

Ein erfolgreicher Angriff gegen die in Bitcoin verwendete

Signaturfunktion, würde wegen des geschickten Design, nicht sofort

alle Bitcoins wertlos machen.

Bitcoin nutzt zunächst statt des eigentlichen öffentlichen Schlüssels

eine von diesem mit Hilfe von zwei verschiedenen Hashfunktionen

abgeleiteten Adresse. Der Public Key wird erst bei einer Überweisung

selbst enthüllt. Dieses Vorgehen verkürzt die möglichen

Angriffszeiten, falls nicht noch Geld auf dem Konto gelassen wird. Aus

Sicherheitsgründen sollte für jede Transaktion eine neue Adresse

verwendet werden, was bisher nur aus Datenschutzgründen empfohlen

wurde.

3 Was sehen Sie an der bei Bitcoin verwendeten Kryptografie kritisch?

Auch wenn man sicher an einigen Stellen aus Sicht der

Kryptographieforschung die ein oder andere Verbesserung vorschlagen

könnte, welche auch teilweise schon in alternativen Systemen

erfolgreich eingesetzt werden, ist jedoch gerade die Einfachheit und

Robustheit der eingesetzten Konstruktionen zu loben. Die Autoren

verfügen über ausgezeichnete Kryptographiekenntnisse.

Die in bitcoin verwendete Kurve Secp256k1 wurde zwar begründet

ausgewählt, bedarf jedoch einer intensiveren Beforschung. Die 256 bit

Schlüssellänge verschafft keinen beruhigenden Sicherheitsspielraum.

Eine Wahl von 512 bit wäre die bessere Wahl gewesen. Auch würde eine

Wahl von unterschiedlichen Kurven für jede Transaktion stärker der

Bitcoin-Philosophie entsprechen.

4 Können Sie grob einschätzen wie lange es noch dauert bis der erste

echte funktionierende Quantencomputer entwickelt wird? Wie hoch ist

Ihrer Einschätzung nach die Chance, dass das in den kommenden

Jahrzehnten passiert?

Es ist leider von außen sehr schwer einzuschätzten wie weit die

amerikanischen Dienste bei der Entwicklung von Quantencomputern

gekommen ist. Die Enthüllung von Snowden zeigten, dass die US

Regierung erhebliche Mittel zur Erforschung von neuartigen

Angriffsmöglichkeiten aufwendet In jedem Falle erscheinen Public Key

Schlüssellängen von mehr als die üblichen 256 bit empfehlenswert.

5 Warum wird heute PostQuantum-Kryptographie so gut wie noch nicht

verwendet? Was sind die Hürden beim Einsatz? Wäre es möglich Bitcoin auf

PostQuantum-Kryptographie umzustellen, ohne dass dabei alle vorhanden

Coins ihren Wert verlieren?

PostQuantum-Kryptographie ist eine recht junge Forschungsrichtung. Die

bisher vorgeschlagenen Verfahren können oftmals noch nicht

hinsichtlich Schlüssellängen und Ausführungsgeschwindigkeit mit den

bisherigen Ansätzen konkurrieren.

Es erscheint wegen der umfassenden Gefährdung der gesamten

Internetkommunikation, die bei einem Quantencomputerdurchbruch sehr

schnell eintreten würde, unabdingbar mathematische Grundlagenforschung

zur Entwicklung zukunftsicheren Verfahren stärker zu fördern.

Bitcoin könnte auf PostQuantum-Kryptographie umgestellt werden, ohne

dass dabei alle vorhanden Coins ihren Wert verlieren.</description>

<persons>

<person id="1545">ruedi</person>

</persons>

<links/>

</event>

<event guid="UqfjLnUNKqc6-WzUjP6YQg" id="6541">

<date>2014-12-28T17:30:00+01:00</date>

<start>17:30</start>

<duration>00:30</duration>

<room>Saal 2</room>

<slug>31c3\_-\_6541\_-\_en\_-\_saal\_2\_-\_201412281730\_-\_forging\_the\_usb\_armory\_-\_andrea\_barisani</slug>

<recording>

<license>CC-BY-3.0</license>

<optout>false</optout>

</recording>

<title>Forging the USB armory</title>

<subtitle>Creating an open source secure flash-drive-sized computer</subtitle>

<track>Hardware &amp; Making</track>

<type>lecture</type>

<language>en</language>

<abstract>The presentation will cover the journey that we have taken to develop the USB armory board from scratch, explaining the lessons learned and its prospected applications.</abstract>

<description>Inverse Path recently introduced the USB armory project (http://inversepath.com/usbarmory), an open source hardware design, implementing a flash drive sized computer for security applications. The USB armory is a compact USB powered device that provides a platform for developing and running a variety of applications.

The security features of the USB armory System on a Chip (SoC), combined with the openness of the board design, empower developers and users with a fully customizable USB trusted device for open and innovative personal security applications.

The presentation will cover the journey that we have taken to develop the USB armory board from scratch, explaining the lessons learned and its prospected applications.</description>

<persons>

<person id="4941">Andrea Barisani</person>

</persons>

<links>

<link href="http://inversepath.com/usbarmory">USB armory project</link>

<link href="https://github.com/inversepath/usbarmory">USB armory github</link>

<link href="http://dev.inversepath.com/download/usbarmory/forging\_the\_usb\_armory.pdf">Presentation</link>

</links>

</event>

<event guid="lcqCv-SWZ2OTU7b2xqw9tg" id="6202">

<date>2014-12-28T18:15:00+01:00</date>

<start>18:15</start>

<duration>00:30</duration>

<room>Saal 2</room>

<slug>31c3\_-\_6202\_-\_en\_-\_saal\_2\_-\_201412281815\_-\_privacy\_and\_consumer\_markets\_-\_reuben\_binns</slug>

<recording>

<license>CC BY 3.0</license>

<optout>false</optout>

</recording>

<title>Privacy and Consumer Markets</title>

<subtitle>Reversing the Surveillance Business Model</subtitle>

<track>Ethics, Society &amp; Politics</track>

<type>lecture</type>

<language>en</language>

<abstract>The internet may be the nervous system of the 21st century, but its main business purpose is helping marketers work out how to make people buy stuff. This talk maps out a possible alternative, where consumers co-ordinate online, pooling their data and resources to match demand with supply.</abstract>

<description>The internet, perhaps the most incredible communications medium ever created, is fast becoming the nervous system of the 21st century. But right now its primary business function is to gather data about us, to categorise and sort us, to machine learn our most intimate secrets, all so that marketers can craft advertisements designed to extract as much money out of us as possible.

As well as being the cause of our current privacy and surveillance woes, this business model is also a surprisingly inefficient way of matching consumers with stuff they actually want and need. A vast infrastructure of ad servers, data brokers, CRMs, and real-time bidding platforms exists in order to quietly nudge consumers to buy a different brand of soap. The problem is that we are easily nudged, and being a rational consumer in the modern economy requires an impossible amount of time, information and intelligence. Realistically, it is beyond the powers of human computation.

The seeds of a technology-driven alternative are emerging in some corners of the economy. A range of new tools crunch through masses of pricing and product data to help consumers avoid getting ripped off, and find the products they really need. Collective buying schemes have enabled households to club together in their thousands to negotiate better, cheaper, more sustainable suppliers of home energy and other products. The growth of free software, peer production and decentralised systems demonstrate that technology for independence, co-operation and empowerment are possible outside of the traditional market model. Combining these trends suggests a possible future where ordinary people collectively pool their data, computation and buying power to drive the production and allocation of goods and services, rendering the surveillance-advertising business model redundant in the process.</description>

<persons>

<person id="5014">Reuben Binns</person>

</persons>

<links/>

</event>

<event guid="T7Ta13fUuQaAbv1JlO4-Qg" id="6459">

<date>2014-12-28T19:00:00+01:00</date>

<start>19:00</start>

<duration>01:00</duration>

<room>Saal 2</room>

<slug>31c3\_-\_6459\_-\_en\_-\_saal\_2\_-\_201412281900\_-\_the\_invisible\_committee\_returns\_with\_fuck\_off\_google\_-\_anonymous\_member\_of\_tarnac\_solidarity\_committee\_-\_tarnac\_nine</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>The Invisible Committee Returns with &quot;Fuck Off Google&quot;</title>

<subtitle>Cybernetics, Anti-Terrorism, and the ongoing case against the Tarnac 10</subtitle>

<track>Ethics, Society &amp; Politics</track>

<type>lecture</type>

<language>en</language>

<abstract>“There will be people who resist adopting and using technology, people who want nothing to do with virtual profiles, online data systems or smart phones. Yet a government might suspect that people who opt out completely have something to hide and thus are more likely to break laws, and as a counterterrorism measure, that government will build the kind of ‘hidden people’ registry we described earlier. If you don’t have any registered social-networking profiles or mobile subscriptions, and on-line references to you are unusually hard to find, you might be considered a candidate for such a registry. You might also be subjected to a strict set of new regulations that includes rigorous airport screening or even travel restrictions.”</abstract>

<description>The figure of the hacker contrasts point by point with the figure of the engineer, whatever the artistic, police-directed, or entrepreneurial efforts to neutralize him may be. Where the engineer would capture everything that functions in such a manner that everything functions better, in order to place it in the service of the system, the hacker asks himself “How does that work?” in order to find its flaws, but also to invent other uses, to experiment. Experimenting then means exploring what such and such a technique implies ethically. The hacker pulls techniques out of the technological system in order to free them. If we are slaves of technology, this is precisely because there is a whole ensemble of artifacts of our everyday existence that we take to be specifically “technical” and that we will always regard simply as black boxes of which we are the innocent users. The use of computers to attack the CIA attests rather clearly that cybernetics is no more the science of computers than astronomy is the science of telescopes. Understanding how any of the devices that surround us brings an immediate increase in power, giving us a purchase on what will then no longer appear as an environment, but as a world arranged in a certain way and one that we can shape. This is the hacker’s perspective on the world.

These past few years, the hacker milieu has gained some sophistication politically, managing to identify friends and enemies more clearly. Several substantial obstacles stand in the way of its becoming-revolutionary, however. In 1986, “Doctor Crash” wrote: “Whether you know it or not, if you are a hacker you are a revolutionary. Don’t worry, you’re on the right side.” It’s not certain that this sort of innocence is still possible. In the hacker milieu there‘s an originary illusion according to which “freedom of information,” “freedom of the Internet,” or “freedom of the individual” can be set against those who are bent on controlling them. This is a serious misunderstanding. Freedom and surveillance, freedom and the panoptical belong to the same paradigm of government.

Historically, the endless expansion of control procedures is the corollary of a form of power that is realized through the freedom of individuals. Liberal government is not one that is exercised directly on the bodies of its subjects or that expects a filial obedience from them. It’s a background power, which prefers to manage space and rule over interests rather than bodies. A power that oversees, monitors, and acts minimally, intervening only where the framework is threatened, against that which goes too far. Only free subjects, taken en masse, are governed. Individual freedom is not something that can be brandished against the government, for it is the very mechanism on which government depends, the one it regulates as closely as possible in order to obtain, from the amalgamation of all these freedoms, the anticipated mass effect. Ordo ab chao.

Government is that order which one obeys “like one eats when hungry and covers oneself when cold,” that servitude which I coproduce at the same time that I pursue my happiness, that I exercise my “freedom of expression.” “Market freedom requires an active and extremely vigilant politics,” explained one of the founders of neoliberalism. For the individual, monitored freedom is the only kind there is. This is what libertarians, in their infantilism, will never understand, and it’s this incomprehension that makes the libertarian idiocy attractive to some hackers. A genuinely free being is not even said to be free. It simply is, it exists, deploys its powers according to its being. We say of an animal that it is en liberté, “roaming free,” only when it lives in an environment that’s already completely controlled, fenced, civilized: in the park with human rules, where one indulges in a safari. “Friend” and “free” in English, and “Freund” and “frei” in German come from the same Indo-European root, which conveys the idea of a shared power that increases. Being free and having ties was one and the same thing. I am free because I have ties, because I am linked to a reality greater than me. In ancient Rome, the children of citizens were liberi : through them, it was Rome that was growing. Which goes to show how ridiculous and what a scam the individual freedom of “I do what I feel like doing” is. If they truly want to fight the government, the hackers have to give up this fetish. The cause of individual freedom is what prevents them from forming strong groups capable of laying down a real strategy, beyond a series of attacks; it’s also what explains their inability to form ties beyond themselves, their incapacity for becoming a historical force. A member of Telecomix alerts his colleagues in these terms: “What is certain is that the territory you’re living in is defended by persons you would do well to meet. Because they’re changing the world and they won’t wait for you.”

Another obstacle for the hacker movement, as every new meeting of the Chaos Computer Club demonstrates, is in managing to draw a front line in its own ranks between those working for a better government, or even the government, and those working for its destitution. The time has come for taking sides. It’s this basic question that eludes Julian Assange when he says: “We high-tech workers are a class and it’s time we recognize ourselves as such.” France has recently exploited the defect to the point of opening a university for molding “ethical hackers.” Under DCRI supervision, it will train people to fight against the real hackers, those who haven’t abandoned the hacker ethic.

These two problems merged in a case affecting us. After so many attacks that so many of us applauded, Anonymous/LulzSec hackers found themselves, like Jeremy Hammond, nearly alone facing repression upon getting arrested. On Christmas day, 2011, LulzSec defaced the site of Strafor, a “private intelligence” multinational. By way of a homepage, there was now the scrolling text of The Coming Insurrection in English, and $700,000 was transferred from the accounts of Stratfor customers to a set of charitable associations – a Christmas present. And we weren’t able to do anything, either before or after their arrest. Of course, it’s safer to operate alone or in a small group – which obviously won’t protect you from infiltrators – when one goes after such targets, but it’s catastrophic for attacks that are so political, and so clearly within the purview of global action by our party, to be reduced by the police to some private crime, punishable by decades of prison or used as a handle for pressuring this or that “Internet pirate” to turn into a government agent.

</description>

<persons>

<person id="5124">Anonymous member of Tarnac Solidarity Committee</person>

<person id="5296">tarnac nine</person>

</persons>

<links>

<link href="https://twitter.com/@anosamis">Twitter: A nos amis</link>

<link href="http://www.bloom0101.org/">bloom0101.org</link>

</links>

</event>

<event guid="T7aunKcOFBLl5b8IGVqJWQ" id="6129">

<date>2014-12-28T20:30:00+01:00</date>

<start>20:30</start>

<duration>01:00</duration>

<room>Saal 2</room>

<slug>31c3\_-\_6129\_-\_en\_-\_saal\_2\_-\_201412282030\_-\_attacks\_on\_uefi\_security\_inspired\_by\_darth\_venamis\_s\_misery\_and\_speed\_racer\_-\_rafal\_wojtczuk\_-\_corey\_kallenberg</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Attacks on UEFI security, inspired by Darth Venamis's misery and Speed Racer</title>

<subtitle/>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>On modern Intel based computers there exists two powerful and protected code regions: the UEFI firmware and System Management Mode (SMM). UEFI is the replacement for conventional BIOS and has the responsibility of initializing the platform. SMM is a powerful mode of execution on Intel CPUs that is even more privileged than a hypervisor. Because of their powerful positions, SMM and UEFI are protected by a variety of hardware mechanisms. In this talk, Rafal Wojtczuk and Corey Kallenberg team up to disclose several prevalent vulnerabilities that result in SMM runtime breakin as well as arbitrary reflash of the UEFI firmware.

</abstract>

<description>In 2009 Rafal Wojtczuk and Alexander Tereshkin described the first publicly presented BIOS reflash exploit. Then in 2013 Corey Kallenberg presented the second instance of this class of vulnerability with an exploit targeting Dell BIOS. Now, in 2014, Rafal and Corey have joined forces to complete the destruction of the jedi^H^H BIOS.

The UEFI firmware is normally the first code to execute on the CPU, putting it in a powerful position to subvert other components of the platform. Because of its security critical nature, the UEFI code resides on a flash chip that is protected against arbitrary writes via a number of chipset protection mechanisms. Besides initializing the platform and bootstrapping to an operating system, UEFI is also charged with instantiating the all powerful System Management Mode (SMM). SMM is neither readable or writeable by any other code on the platform. In fact, SMM has the ability to read and write hypervisor protected memory, but the converse is not true! These properties make SMM an ideal place to store a rootkit. Similar to the UEFI firmware, because of these security critical properties, there are hardware mechanisms that protect the integrity and confidentiality of SMM.

This talk will explore attack surface against SMM and UEFI that has not previously been discussed. We will highlight a bug in one of the critical hardware protection mechanisms that results in a compromise of the firmware. We will also directly target a part of the UEFI specification that provides SMM exploitation opportunities. The vulnerabilities disclosed and their corresponding exploits are both prevalent among UEFI systems and reliably exploitable.

The consequences of these vulnerabilities include hypervisor and TXT subversion, bricking of the victim platform, insertion of powerful rootkits, secure boot break, among other possibilities.

</description>

<persons>

<person id="4940">Rafal Wojtczuk</person>

<person id="4934">Corey Kallenberg</person>

</persons>

<links/>

</event>

<event guid="78e2d419-0adc-43ff-989e-95a78ac9ddd4" id="6585">

<date>2014-12-28T21:45:00+01:00</date>

<start>21:45</start>

<duration>01:00</duration>

<room>Saal 2</room>

<slug>31c3\_-\_6585\_-\_en\_-\_saal\_2\_-\_201412282145\_-\_inside\_field\_station\_berlin\_teufelsberg\_-\_bill\_scannell</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Inside Field Station Berlin Teufelsberg</title>

<subtitle>The story of the NSA listening post – told by an ex-SIGINT analyst who worked there</subtitle>

<track>Ethics, Society &amp; Politics</track>

<type>lecture</type>

<language>en</language>

<abstract>Of all the NSA's Cold War listening posts, their intelligence facility on top of Berlin's Teufelsberg was their most secretive.</abstract>

<description>Field Station Berlin – its white tower and geodesic domes visible for miles around – was the epicenter of of the western intelligence community's most sensitive SIGINT operations. Now abandoned, the ghosts of &quot;The Hill&quot; know many stories left untold.

Ever wondered how it was to work there at the height of the Cold War? What did people do there, anyway? And what it was really like inside the day Ronald Reagan said, &quot;we begin bombing in five minutes&quot;?

Wonder no longer. As a young SIGINT analyst straight out of college in the 1980's, Bill Scannell was there and will tell (almost) all.</description>

<persons>

<person id="5306">Bill Scannell</person>

</persons>

<links/>

</event>

<event guid="xyADKdXtvEgJWo6eaTmUBQ" id="6291">

<date>2014-12-28T23:00:00+01:00</date>

<start>23:00</start>

<duration>01:00</duration>

<room>Saal 2</room>

<slug>31c3\_-\_6291\_-\_en\_-\_saal\_2\_-\_201412282300\_-\_doing\_right\_by\_sources\_done\_right\_-\_sarah\_harrison\_-\_grace\_north</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Doing right by sources, done right</title>

<subtitle/>

<track>Ethics, Society &amp; Politics</track>

<type>lecture</type>

<language>en</language>

<abstract>Whistleblowing is becoming a progressively popular topic and ways to technically support anonymous submissions by journalistic sources are being increasingly discussed and developed. However, there is much more to protecting sources than the technical side. There is currently little discussion about the surrounding ethics, operational security and public protections of sources. Two women that have expertise in all areas of source protection; from submission, to publication, to after-care explain and discuss what source protection really means, issues that have arisen in recent years, often causing disastrous consequences, as well as the important lessons to learn from these and successful cases.</abstract>

<description>Speakers: Sarah Harrison: Courage Acting Director and WikiLeaks Investigations Editor and Grace North: Jeremy Hammond campaign manager

With current technology the ability for journalists to be provided with large data sets securely is increasing. With the surveillance revelations from Snowden there is much talk about ways for the public and journalists to work online safely, and how this can be used to help protect sources. However, there are few to no discussions about a holistic attitude to source protection. In fact we can see in the past that its often not technical, but operational security issues that pose the greatest threat to source's ongoing safety, whether that is the source's or journalist's operational security, informants, or lack of after care.

Source protection begins at the point of contact, and it doesn’t stop at publication - in some cases, the real work actually begins at publication. From the angle of investigations editor at WikiLeaks, a publishing organisation with a clean record of source protection, Harrison is well placed to explain the nuanced areas of source protection for media, from submission through to publication.

But its not just within the publication process that source protection needs to be considered. Simply not printing a sources name is not enough. It’s irresponsible for journalists to speculate about sources they know little about, or to publicly speculate that an unnamed source is on the loose. Recently media outlets have suggested there is another NSA source, leaking information to the Intercept and elsewhere. What has that incurred? The US government launched an internal investigation to hunt out any other suspected sources, and we know well what the United States does to whistleblowers.

And for media and the public alike there is an aftercare responsibility to sources that have risked so much for our right to know - how they are supported and spoken about. Both Harrison and North are experts in how media and the public have and should protect sources. Media generally abandons sources (they did in the case of Manning and Hammond in a devastating way), this can and should change. In addition public solidarity is vital for sources, we have this past year seen a growing trend in pitting sources against one another in the public domain: Harrison and North will discuss the dangers and consequences of this.

While the use of the term “whistleblower” is increasingly used and understood, it doesn’t always describe a source. Courage uses the term ‘truthteller’ to encompass all people who bring secret truths to public light. Someone like Jeremy Hammond, who did not work for Stratfor or its clients, but knew its operations were of interest to the public at large, to the citizens of a government that subscribes to Stratfor’s services, is a truthteller. He is an outsider who worked, allegedly, to make important truths public, and thus a vital journalistic source, without whom we wouldn’t have hundreds upon hundreds of valuable news stories on the private intelligence industry.

These lessons give us a better understanding of what has gone right and wrong with recent high-level sources, like Manning, Snowden and Hammond, but they should also be building blocks for an understanding of the principles involved and how we can employ them in the future. Courage wants to continue protecting the sources we know about, but we also work to engender a culture of support for whistleblowing, a knowledgeable and ethical media class, and a trust among sources that journalists will protect them from start to finish. We encourage whistleblowing as a key method to keeping governments and powerful corporations accountable to the public, but we must be responsible first. This talk will explain and highlight these lessons from a first hand perspective, giving an understanding of what real source protection means, and how the media and public can perform it. The speakers will take questions after.

</description>

<persons>

<person id="5055">Sarah Harrison</person>

<person id="4690">Grace North</person>

</persons>

<links/>

</event>

<event guid="74711c06-8813-4158-b102-36dbbe374d13" id="6606">

<date>2014-12-29T00:15:00+01:00</date>

<start>00:15</start>

<duration>01:30</duration>

<room>Saal 2</room>

<slug>31c3\_-\_6606\_-\_de\_-\_saal\_2\_-\_201412290015\_-\_fnord\_news\_show\_stream\_-\_fefe\_-\_frank\_rieger</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Fnord News Show (Stream)</title>

<subtitle>Wir helfen Euch die Fnords zu sehen.</subtitle>

<track>Entertainment</track>

<type>lecture</type>

<language>de</language>

<abstract>Im Format einer lockeren Abendshow werden wir die Nachrichten-Highlights des Jahres präsentieren, die Meldungen zwischen den Meldungen, die subtilen Sensationen hinter den Schlagzeilen.</abstract>

<description>Kommen Sie, hören Sie, sehen Sie! Lassen Sie sich mitreißen!</description>

<persons>

<person id="1621">Fefe</person>

<person id="5183">Frank Rieger</person>

</persons>

<links/>

</event>

</room>

<room name="Saal G">

<event guid="XGqu620EKR92-WUWMXNRvA" id="6021">

<date>2014-12-28T11:30:00+01:00</date>

<start>11:30</start>

<duration>01:00</duration>

<room>Saal G</room>

<slug>31c3\_-\_6021\_-\_en\_-\_saal\_g\_-\_201412281130\_-\_why\_is\_gpg\_damn\_near\_unusable\_-\_arne\_padmos</slug>

<recording>

<license>CC-BY-3.0</license>

<optout>false</optout>

</recording>

<title>Why is GPG &quot;damn near unusable&quot;?</title>

<subtitle>An overview of usable security research</subtitle>

<track>Science</track>

<type>lecture</type>

<language>en</language>

<abstract>GPG has been correctly described as &quot;damn near unusable&quot;. Why is this so? What does research into usable security tell us? This talk covers the history, methods, and findings of the research field, as well as proposed solutions and open questions.</abstract>

<description>With all the frustration around trying to get Glen Greenwald to use encryption [0,1], it is not surprising that Edward Snowden has described GPG as &quot;damn near unusable&quot; [2]. Such usability problems of end-to-end email encryption tools have been around for a long time. In 1999, a seminal study found that most participants were unable to use PGP 5.0 to encrypt an email when given 1.5 hours to do so [3]. Others have tried to solve these usability problems by automating the key exchange and encryption [4]. However, issues persist around a lack of end-user trust in the software [5], difficulties in getting encryption widely implemented, and having to deal with a general absence of understanding the email architecture [6].

Despite being almost 50 years old [7], email is still not widely encrypted on an end-to-end basis. In this year's SOUPS keynote (the major conference on usable security), Christopher Soghoian described how we as a community are not doing nearly enough to get security into the hands of consumers: we are mostly stuck with the same broken interface as PGP 5.0 from back in 1999, people still face the same conceptual barriers, and we still have crappy defaults [8]. While there has been renewed interest in end-to-end email encryption after the Snowden revelations [9], many projects do not take usability into account.

This talk goes into some of the dos and don'ts gleaned from the usable security research field. Building on a discussion of the history, methodology, and findings of the research, the talk will cover topics including the constraints of humans, the need for clear mental models, and the usefulness of user testing. Some examples of successes and failures will be used to illustrate a range of usable security principles. Remaining pain points such as metadata protection, key management, and end-user understanding will be covered, including proposals for fixing these such as anonymous routing, more appropriate metaphors, and trust on first use. Various open questions will also be discussed, including:

- Should we patch the existing email architecture or should we move towards new protocols?

- How can the crypto community build subversion-resistant collaboration platforms?

- Is there a way to standardise our cryptoplumbing to a restricted set of secure algorithms?

- Can we provide developers with usable coding technologies to prevent nightmares like OpenSSL?

- How should we involve end-users into the development cycle of open source software?

- Can we empower end-users to take security back into their own hands?</description>

<persons>

<person id="4773">Arne Padmos</person>

</persons>

<links>

<link href="http://vimeo.com/56881481">[0] GPG for Journalists, anon108</link>

<link href="http://en.wikipedia.org/wiki/No\_Place\_to\_Hide\_(Greenwald\_book)">[1] No place to hide, Glenn Greenwald</link>

<link href="https://www.youtube.com/watch?v=onrTo1sYri8">[2] Snowden speaks at HOPE X in 2014 with Ellsberg</link>

<link href="http://www.gaudior.net/alma/johnny.pdf">[3] Why Johnny can't encrypt</link>

<link href="http://groups.csail.mit.edu/lapis/projects/secure-email/soups05.pdf">[4] Johnny 2</link>

<link href="https://cups.cs.cmu.edu/soups/2013/proceedings/a5\_Ruoti.pdf">[5] Confused Johnny</link>

<link href="https://www.petsymposium.org/2014/papers/Renkema.pdf">[6] Why doesn't Jane protect her privacy?</link>

<link href="http://www.multicians.org/thvv/anhc-34-1-anec.html">[7] Electronic mail and text messaging in CTSS</link>

<link href="https://www.youtube.com/watch?v=is9luGFzqgA">[8] Sharing blame for NSA's dragnet surveillance</link>

<link href="https://github.com/OpenTechFund/secure-email">[9] Overview of projects working on next-generation secure email</link>

</links>

</event>

<event guid="c3efec0b-cfb1-4e59-88fd-f519dd31d9a6" id="6563">

<date>2014-12-28T12:45:00+01:00</date>

<start>12:45</start>

<duration>02:15</duration>

<room>Saal G</room>

<slug>31c3\_-\_6563\_-\_en\_-\_saal\_g\_-\_201412281245\_-\_lightning\_talks\_day\_2\_-\_gedsic</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Lightning Talks Day 2</title>

<subtitle/>

<track>Other</track>

<type>lecture</type>

<language>en</language>

<abstract>Lightning Talks are short lectures (almost) any congress participant may give! Bring your infectious enthusiasm to an audience with a short attention span! Discuss a program, system or technique! Pitch your projects and ideas or try to rally a crew of people to your party or assembly! Whatever you bring, make it quick! </abstract>

<description/>

<persons>

<person id="5263">gedsic</person>

</persons>

<links>

<link href="https://events.ccc.de/congress/2014/wiki/Static:Lightning\_Talks">31C3 Wiki: Lightning Talks</link>

</links>

</event>

<event guid="1Xe2U3LqTfMTXAvI6hrgxg" id="6325">

<date>2014-12-28T16:00:00+01:00</date>

<start>16:00</start>

<duration>00:30</duration>

<room>Saal G</room>

<slug>31c3\_-\_6325\_-\_de\_-\_saal\_g\_-\_201412281600\_-\_gifs\_tod\_eines\_mediums\_und\_sein\_leben\_nach\_dem\_tod\_-\_felix\_mutze</slug>

<recording>

<license>CC-BY-3.0</license>

<optout>false</optout>

</recording>

<title>GIFs: Tod eines Mediums. Und sein Leben nach dem Tod.</title>

<subtitle>Wie es kommt, dass technischer Fortschritt den Nutzern gänzlich egal sein kann.</subtitle>

<track>Science</track>

<type>lecture</type>

<language>de</language>

<abstract>Im Grunde sind GIFs Schnee von gestern. Es gibt zahlreiche Alternativen, die das, was ein GIF kann, besser können. Und trotzdem haben sich GIFs als Kulturtechnik durchgesetzt. Oder war es nur ein letzter Hype vor dem Tod? Wie kommt es, dass ein Medium, das schon in den 90ern veraltet war, sich noch zwei Jahrzehnte später bester Beliebtheit erfreut? Und was können wir daraus über die Diskrepanz zwischen aktueller technischer Entwicklung einerseits und der tatsächlichen Nutzung von Technologie andererseits lernen?</abstract>

<description>In seiner langen Geschichte hat das Dateiformat GIF einiges an Auf und Ab erlebt. Mittlerweile ist es technisch völlig überholt, wurde mehrfach totgesagt, teils aktiv bekämpft und wurde trotzdem nicht völlig von der technisch besseren Konkurrenz abgelöst. Zu verdanken ist diese Entwicklung neben einigen Zufällen vor allem den Internetnutzern selbst. Denn obwohl sich GIFs technisch seit 1998 nicht mehr verändert haben, findet das Internet immer wieder neue Anwendungen für die Zappelbilder.

Der Vortrag blickt kurz auf die vielen Tode zurück, welche das GIF-Format schon gestorben ist – oder die ihm gewünscht wurden – und behandelt die aktuelle Entwicklung, bei der WebM angetreten ist, das Kapitel GIF zu beenden.

Viel wichtiger ist jedoch der Blick auf die Seite der Nutzer. Anhand von Beispielen aus den letzten Jahrzehnten werden Gründe dafür analysiert, weshalb GIFs immer wieder belebt werden konnten.

Am Ende bleibt die Frage, ob und wie sich das Erfolgsrezept GIF auf andere Medien und Technologien übertragen lässt.

Und: Ja, natürlich spielt auch Pr0n eine Rolle.</description>

<persons>

<person id="5063">Felix Mütze</person>

</persons>

<links>

<link href="http://metagif.wordpress.com">metagif blog</link>

</links>

</event>

<event guid="0T8GTXjwMVJLM\_n5VEuE0A" id="6144">

<date>2014-12-28T16:45:00+01:00</date>

<start>16:45</start>

<duration>00:30</duration>

<room>Saal G</room>

<slug>31c3\_-\_6144\_-\_en\_-\_saal\_g\_-\_201412281645\_-\_finding\_the\_weak\_crypto\_needle\_in\_a\_byte\_haystack\_-\_ben\_h</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Finding the Weak Crypto Needle in a Byte Haystack</title>

<subtitle>Automatic detection of key-reuse vulnerabilities</subtitle>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>Using the same stream cipher key twice is known to be a Very Bad Idea, but keystream-resuse vulnerabilities are still very much a thing of the present - both in legitimate software and in the malware landscape. We describe a heuristic algorithm which can detect vulnerabilities of this kind. We explain the inner workings of the algorithm and demonstrate a proof-of-concept attack on sevreral examples of vulnerable data, including files encrypted by the DirCrypt malware and encrypted traffic generated by malware such as variants of Zeus and Ramnit.</abstract>

<description>When operating a stream cipher, reusing a keystream introduces a critical weakness to the resulting ciphertext: the encryption becomes vulnerable to easy (and sometimes /very/ easy) cryptographic attacks. This is due to the encryption's linear nature - for instance, XORing a plaintext with the corresponding ciphertext yields keystream bytes. While key reuse is a widely known issue, it's an issue that keeps arising in practice. The soviets did it during WWII, Microsoft did it in the implementation of Word 2003 document encryption, and malware authors did it when designing variants of Zeus, DirCrypt and Ramnit.

To exploit a vulnerability, you must first realize it's there. Unfortunately, many instances of homebrew crypto operate on the &quot;security by obscurity&quot; principle, and don't reveal their implementation details. As a result, detecting key reuse often requires trial and error, an accidental epiphany or a night spent reverse engineering - and in all these cases, luck and human effort. In this presentation we show an approach to automating this task - based on the linear properties of stream ciphers, redundancy in the text and Bayesian reasoning. Finally, we demonstrate the algorithm's operation in several real-world use cases.

Math Ph.D. not required.</description>

<persons>

<person id="4950">Ben H.</person>

</persons>

<links/>

</event>

<event guid="n8k2uElFR872zYbrs7kycQ" id="6071">

<date>2014-12-28T17:30:00+01:00</date>

<start>17:30</start>

<duration>00:30</duration>

<room>Saal G</room>

<slug>31c3\_-\_6071\_-\_en\_-\_saal\_g\_-\_201412281730\_-\_hacking\_ethics\_in\_education\_-\_jeroen\_van\_der\_ham</slug>

<recording>

<license>CC-BY-3.0</license>

<optout>false</optout>

</recording>

<title>Hacking Ethics in Education</title>

<subtitle/>

<track>Ethics, Society &amp; Politics</track>

<type>lecture</type>

<language>en</language>

<abstract>Ethics in Computer Science is now finally gaining some well deserved attention. At the University of Amsterdam, we have started an ethical committee for the System and Network Engineering Master. In this talk we describe how and why we started this committee, and also look back at our first results.</abstract>

<description>Ethics in Computer Science is now finally gaining some well deserved attention. With the advent of Big Data, Cloud Computing, and the Internet of Things, much of our daily life is happening through digital channels. As most of us have learned, developers do not consider security to be an important point, imagine how much they consider the social aspect of their product or code. This is a huge problem, not only because it presents security and privacy risks for the users, but also presents moral dilemmas for hackers and researchers.

Since my PirateBay blocking study, I have become interested in ethics in computer science. In that study I gathered personally identifiable information, to be able to prove that the website blockade was ineffective. These kinds of moral dilemmas are hard to judge, and in computer science we have no history of teaching or awareness about this.

At the University of Amsterdam, we have started an ethical committee for the System and Network Engineering Master. In this talk we describe how and why we started this committee, and also look back at our first results.</description>

<persons>

<person id="4812">Jeroen van der Ham</person>

</persons>

<links>

<link href="https://www.os3.nl/2014-2015/info/ethics">Ethical Procedures for SNE Master</link>

<link href="https://1sand0s.nl">Personal Blog</link>

</links>

</event>

<event guid="KNu4tX4NRJCFiFCsIh-FxA" id="6399">

<date>2014-12-28T18:15:00+01:00</date>

<start>18:15</start>

<duration>00:30</duration>

<room>Saal G</room>

<slug>31c3\_-\_6399\_-\_en\_-\_saal\_g\_-\_201412281815\_-\_global\_civil\_society\_under\_attack\_-\_michael\_carbone</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Global Civil Society Under Attack</title>

<subtitle>Reports from the Frontlines</subtitle>

<track>Ethics, Society &amp; Politics</track>

<type>lecture</type>

<language>en</language>

<abstract>An update to our Reports from the Frontlines talk at OHM 2013, we will provide the latest stories and figures from Access' digital security helpline that provides security incident response and technical support to civil society groups and human rights defenders around the world.</abstract>

<description>Access runs a dedicated 24-hour digital security helpline for civil society groups out of three offices in Tunisia, Costa Rica, and the Philippines. We serve groups around the world in a variety of contexts, securing communications, providing website security support, incident response, and strategic security planning and training.

In this talk we'll explore what trends we've seen on the helpline, both in reactive incident response and technical support requests by civil society groups. We'll also discuss the recent Digital First Aid Kit worked on by a number of organizations including Access, and some longer term initiatives and goals such as an official civil society CERT (CiviCERT).</description>

<persons>

<person id="5086">Michael Carbone</person>

</persons>

<links>

<link href="https://program.ohm2013.org/event/126.html">OHM 2013 talk</link>

<link href="https://www.accessnow.org/pages/tech">Tech page on Access website</link>

<link href="https://digitaldefenders.org/digitalfirstaid/">Digital First Aid Kit</link>

<link href="http://www.trusted-introducer.org/directory/teams/civicert.html">CiviCERT</link>

</links>

</event>

<event guid="qRQclNxyOV7ZYPwbrXrw1Q" id="6370">

<date>2014-12-28T19:00:00+01:00</date>

<start>19:00</start>

<duration>00:30</duration>

<room>Saal G</room>

<slug>31c3\_-\_6370\_-\_en\_-\_saal\_g\_-\_201412281900\_-\_internet\_of\_toilets\_-\_tbsprs</slug>

<recording>

<license>CC-BY-3.0</license>

<optout>false</optout>

</recording>

<title>Internet of toilets</title>

<subtitle>Trends in the sanitarian territory</subtitle>

<track>Hardware &amp; Making</track>

<type>lecture</type>

<language>en</language>

<abstract>A toilet is a toilet is a toilet ... was a toilet. Nowadays hackers discover a larger interest in doing more with toilets then just what they were designed for in the first place. Within the &quot;Internet of things&quot; scene the sanitarian sphere claims a place of its own. This talk will present current projects, technologies used and research published.</abstract>

<description>This talk provides an overview of past and current hardware installations, services and publications that focus on the sanitarian territory. People track a wide variety of things: doors, water consumption, visiting times, paper usage and not to forget the habits of their pets. The range of implementations starts of with dedicated Twitter streams, exploratory websites and ends of with APIs, consumable services and extensive statistics which allow analysis over time. You will get to know the detailed installation architecture which allows building your own toilet tracking.

Furthermore, the talk outlines the serious aspects of the Internet of toilets and its importance for the society. Hygiene facts and economic considerations are discussed.

One of the motivations for this talk besides a general interest in the topic itself is the vision to realize such an installation for the congress in the near future (talking about 31c3).

</description>

<persons>

<person id="4983">tbsprs</person>

</persons>

<links/>

</event>

<event guid="xvPazrSLJdMwzpnphpOEIQ" id="6534">

<date>2014-12-28T20:30:00+01:00</date>

<start>20:30</start>

<duration>01:00</duration>

<room>Saal G</room>

<slug>31c3\_-\_6534\_-\_en\_-\_saal\_g\_-\_201412282030\_-\_mining\_for\_bugs\_with\_graph\_database\_queries\_-\_fabs</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Mining for Bugs with Graph Database Queries</title>

<subtitle/>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>While graph databases are primarily known as the backbone of the modern dating world, this nerd has found a much more interesting application for them: program analysis. This talk aims to demonstrate that graph databases and the typical program representations developed in compiler construction are a match made in heaven, allowing large code bases to be mined for vulnerabilities using complex bug descriptions encoded in simple, and not so simple graph database

queries.</abstract>

<description>This talk will bring together two well known but previously unrelated

topics: static program analysis and graph databases. After briefly

covering the &quot;emerging graph landscape&quot; and why it may be interesting for hackers, a graph representation of programs exposing syntax, control-flow, data-dependencies and type information is presented, designed specifically with bug hunting in mind. Our open-source program analysis platform Joern (http://mlsec.org/joern/) is then introduced, which implements these ideas and has been successfully used to uncover various vulnerabilities in the Linux kernel. Capabilities and limitations of the system will then be demonstrated live as we craft queries for buffer overflows, memory disclosure bugs and integer-related vulnerabilities.</description>

<persons>

<person id="5200">fabs</person>

</persons>

<links>

<link href="http://mlsec.org/joern">Joern Code Analysis Platform</link>

</links>

</event>

<event guid="1lKbMS92kS0J0pQAAO6XZA" id="6170">

<date>2014-12-28T21:45:00+01:00</date>

<start>21:45</start>

<duration>01:00</duration>

<room>Saal G</room>

<slug>31c3\_-\_6170\_-\_en\_-\_saal\_g\_-\_201412282145\_-\_net\_neutrality\_days\_of\_future\_past\_-\_rejo\_zenger\_-\_thomas\_lohninger</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>net neutrality: days of future past? </title>

<subtitle>Taking stock after two years of net neutrality in the Netherlands</subtitle>

<track>Ethics, Society &amp; Politics</track>

<type>lecture</type>

<language>en</language>

<abstract>Our talk will highlight the current debates surrounding net neutrality in Europe, the United States and other parts of the world. We will look at the results of the &lt;a href=&quot;https://savetheinternet.eu&quot;&gt;SaveTheInternet.eu&lt;/a&gt; campaign which was lunched a year ago on 30c3. We will discuss various legal protections for net neutrality, look closer at the experience of the Netherlands and we will give an overview of all important open ends of the debate.</abstract>

<description>Since two years net neutrality is on the agenda of politicians world wide. These are important debates, as net neutrality became one of the central questions about our freedom on the internet. With different faces around the globe we see a trend towards more violations of the neutrality principle which the internet was founded upon. The efforts of telecommunication companies to find new ways to monetize their networks and us users within them are countered in some countries with legislation preventing this new business models.

In 2010, after two years of preparation and a fierce battle, the Dutch

parliament accepted a change to the Telecommunications Act which made net neutrality a principle that was protected by law. In this talk we will take stock after two years of legal protection of net neutrality in The Netherlands. Did it work and do the Dutch now have undiscriminated access to all services on the internet? Has the doomsday scenario of the providers, that subscriptions would become outrageously expensive, become reality? In which cases was the Dutch law enforced?

Are there any loopholes in the Dutch implementation? If others are to

fight for net neutrality, what are the pitfalls to avoid? And, on a more

meta-level, is it enough? Will net neutrality protect your freedom to

access websites and services, or do we need a broader type neutrality?</description>

<persons>

<person id="3699">Rejo Zenger</person>

<person id="4366">Thomas Lohninger</person>

</persons>

<links>

<link href="https://savetheinternet.eu">SaveTheInternet campaign</link>

<link href="https://netzfreiheit.org">Initiative für Netzfreiheit</link>

<link href="https://www.bof.nl">Bits of Freedom</link>

<link href="https://edri.org">European Digital Rights (EDRi)</link>

<link href="https://digitalegesellschaft.de">Digitale Gesellschaft</link>

</links>

</event>

<event guid="2f68e356-6c3f-4034-9640-c06d717ed96b" id="6558">

<date>2014-12-28T23:00:00+01:00</date>

<start>23:00</start>

<duration>01:00</duration>

<room>Saal G</room>

<slug>31c3\_-\_6558\_-\_de\_-\_saal\_g\_-\_201412282300\_-\_traue\_keinem\_scan\_den\_du\_nicht\_selbst\_gefalscht\_hast\_-\_david\_kriesel</slug>

<recording>

<license>CC BY 3.0</license>

<optout>false</optout>

</recording>

<title>Traue keinem Scan, den du nicht selbst gefälscht hast</title>

<subtitle>&quot;Bei Kopierern kommt das raus, was man reinsteckt.&quot; – Wer das denkt, sollte diesen Vortrag besuchen.</subtitle>

<track>Ethics, Society &amp; Politics</track>

<type>lecture</type>

<language>de</language>

<abstract>Kopierer, die spontan Zahlen im Dokument verändern: Im August 2013 kam heraus, dass so gut wie alle Xerox-Scankopierer beim Scannen Zahlen und Buchstaben einfach so durch andere ersetzen. Da man solche Fehler als Benutzer so gut wie nicht sehen kann, ist der Bug extrem gefährlich und blieb lange unentdeckt: Er existiert über acht Jahre in freier Wildbahn.</abstract>

<description>Das gemeine ist, dass die gefälschten Zahlen perfekt in die gescannte Textseite hineinlayoutet sind. Das klingt so gemein wie unglaublich, es ist aber wahr (siehe Beispielbilder im Originalartikel-Link rechts). Der Bug existiert auf hunderttausenden Xerox-Scankopierern weltweit.

Die Problematik hat nichts mit OCR zu tun, die Zahlenersetzung passiert hart in den Pixeldaten. So ein perfekt getarntes Kompressionsartefakt kann ein Benutzer nicht sehen. Das ist lebensgefährlich, wenn man eine Autobahnbrücke oder eine Medikamentendosierung scannt oder die Lithiumakkus der Boing 787 vielleicht doch für die 767 gedacht waren.

Der Vortrag hat drei rote Fäden.

&lt;ul&gt;

&lt;li&gt;&lt;b&gt;Auseinandersetzung mit Xerox.&lt;/b&gt; In diesem Vortrag erzählt David auf unterhaltsame Weise, wie er diese Urgroßmutter aller Bugs entdeckt hat. Die Geschichte ging von seinem Blog aus durch die Weltpresse, was zu einem unterhaltsamen öffentlichen Schlagabtausch zwischen Xerox und ihm führte. Xerox musste einen Patch für einen riesigen Gerätepark liefern. Die Folgen von acht Jahren an subtil falschen Dokumentenproduktionen in zigtausenden Institutionen weltweit sind bis heute unabsehbar. &quot;Xerox Can Fix Number-Switching Scanners, but Not Altered Docs&quot;, titelte das Wirtschaftsmagazin &quot;Businessweek&quot; treffend.

&lt;li&gt;&lt;b&gt;Für die Aktivisten unter euch&lt;/b&gt; leitet David konkrete Regeln ab, wie man einen Großkonzern zum Handeln zwingt, und wie das für einen selbst aussieht. Er skizziert genau, wie er vorgegangen ist, wo er Angst hatte, und wo er aus seinen Fehlern lernen mußte.

&lt;li&gt;&lt;b&gt;Für die Verschwörungstheoretiker&lt;/b&gt; wird verraten, was der Bug mit Barack Obamas Geburtsurkunde zu tun hat.

&lt;/ul&gt;

&lt;b&gt;Spread the word! &lt;/b&gt; Aller Wahrscheinlichkeit nach existieren immer noch hunderttausende nummernvertauschende Scankopierer. Euer Kommen ist wichtig. </description>

<persons>

<person id="5240">David Kriesel</person>

</persons>

<links>

<link href="http://www.dkriesel.com/xerox">Originalartikel; genaue Beschreibung der Story samt Timeline und Bildern</link>

</links>

</event>

</room>

<room name="Saal 6">

<event guid="hnRe8t6JYI\_8PYnFh-dsug" id="6084">

<date>2014-12-28T11:30:00+01:00</date>

<start>11:30</start>

<duration>01:00</duration>

<room>Saal 6</room>

<slug>31c3\_-\_6084\_-\_en\_-\_saal\_6\_-\_201412281130\_-\_uncaging\_microchips\_-\_peter\_laackmann\_-\_marcus\_janke</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Uncaging Microchips</title>

<subtitle>Techniques for Chip Preparation</subtitle>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>An entertaining, thrilling and educational journey through the world of chip preparation. Deep insight into amateur- as well as professional methods and equipment is given, for the first, most important steps for analysis and attacks on dedicated hardware.</abstract>

<description>Marcus Janke and Dr. Peter Laackmann focus on the first challenge a smart card hacker would encounter – the appropriate preparation of a microchip from its environment for further analysis and attacks.

The direct sight on microchips, especially on their secured variants, is not only impressive and informative, but will also open up interesting opportunities for various security attacks, like demonstrated in their 30C3 overview &quot;25 Years of Smart Card Attacks&quot;.Therefore, useful ways of releasing the chips from their packages are needed in order to get access to the chip's surface without destroying the device.

The authors open up their bag of tricks, filled with physical and chemical methods that can be used to carefully liberate the silicon from its environment. These packages include smart cards, tags as well as standard packages for microcontrollers and special enclosures.

Creative methods for amateurs and inexpensive ways for &quot;domestic use&quot; are depicted, including the manufacture of specialized devices and the production of dedicated preparation chemicals. For comparison, professional methods are presented in parallel, giving insight into today's industrial processes of chip preparation for reverse engineering.

The authors look back to over 25 years of private security research and nearly 20 years of professional engagement. They held their first chipcard talks and workshops 1991-93 at the CCC congress in the Eidelstädter Bürgerhaus.</description>

<persons>

<person id="4262">Peter Laackmann</person>

<person id="4408">Marcus Janke</person>

</persons>

<links/>

</event>

<event guid="Fj7J1P7FKCiWEl7lIaDaXg" id="6244">

<date>2014-12-28T12:45:00+01:00</date>

<start>12:45</start>

<duration>01:00</duration>

<room>Saal 6</room>

<slug>31c3\_-\_6244\_-\_de\_-\_saal\_6\_-\_201412281245\_-\_serenitat\_anleitung\_zum\_glucklichsein\_-\_elektra\_-\_andrea\_behrendt\_-\_read\_delete</slug>

<recording>

<license>CC-BY-3.0</license>

<optout>false</optout>

</recording>

<title>Serenität – Anleitung zum Glücklichsein</title>

<subtitle>Das Duo 'read &amp; delete' präsentiert radikale philosophische Texte mit musikalischer Begleitung</subtitle>

<track>Art &amp; Culture</track>

<type>other</type>

<language>de</language>

<abstract>Die radikalen philosophischen Texte von Elektra W. haben das Ziel - seien wir offen und direkt - einen Headcrash des Ich-Erlebens herbeizuführen, das sich im Laufe unserer Enkulturation und Erziehung im Vorderlappen des Großhirns breit gemacht hat. </abstract>

<description>'Echtes Denken ist eine Sache, die das Gehirn selbständig per Autopilot erledigt.'

Der Vortrag bringt Texte aus dem Buch 'Serenität – Anleitung zum Glücklichsein' der Edition 'Operation Mindcrash' zum Klingen. Elektra trägt die Texte vor, während Andi B. auf dem Keyboard dazu improvisiert. Durch die Kombination von Text und Musik kann man entspannt zuhören und sich dabei in eine heitere, gelassene Stimmung versetzen lassen.

Serenität – ein deutsches Wort, dass vermutlich aus der französischen Sprache übernommen wurde, ist heute vergessen. Es passt auch gar nicht so recht zur deutschen Mentalität. Überliefert ist, dass im 18. Jahrhundert im deutschen Sprachraum Personen höchsten Respekts als 'Ihre Serenität' angesprochen wurden, im Sinne von 'Ihre Erhabenheit' oder 'Durchlaucht'. Im Französischen und Englischen ist der Begriff dagegen geläufiger und bedeutet Heiterkeit, Gelassenheit, Erhabenheit, Klarheit, innere Ruhe, Frieden mit sich selbst.

Hinter dem Buch steckt eine radikale materialistische Philosophie über das Gehirn und das Denken. Es geht um - oder besser gegen – die innere Narration der eigenen Heldengeschichte, durch die viele Menschen heute Ordnung in ihr inneres Erleben bringen wollen, indem sie sich selbst in ihrem Kopf eine Fabel, das Märchen ihres Lebens erzählen.

Der Vortrag geht an die Wurzel des Strukturmodells der menschlichen Psyche. Assoziationen mit dem Science-Fiction-Klassiker 'Snowcrash' von Neal Stephenson sind nicht ganz zufällig, aber nicht beabsichtigt. Wer Angst davor hat, dass sich in seinem Leben etwas ändert, sollte diesem Programm besser nicht beiwohnen.

Zu Wort kommen auch Franz Kafka, Friedrich Hölderlin, Epikur, Julien Offray de La Mettrie, Jiddu Krishnamurti und Max Stirner. Vor allem letzterer hat es Elektra angetan. Über Stirner haben einige Philosophen gesagt, dass der Untergang des Menschengeschlechtes bevor stünde, wenn sich seine Gedanken gegen die Entfremdung der Menschen verbreiten würden.

Um Kopfschmerzen oder Schlimmeres zu vermeiden, sollte man nicht über den Inhalt des Vortrags nachdenken. Echtes Denken ist eine Sache, die das Gehirn selbständig per Autopilot erledigt. Machen Sie sich daher keine Sorgen! Nur echtes Denken hilft in Zeiten der Krise!

</description>

<persons>

<person id="1281">Elektra</person>

<person id="5273">Andrea Behrendt - read &amp; delete</person>

</persons>

<links>

<link href="http://read-and-delete.elektrad.info/de/index.html">Read and Delete:</link>

<link href="http://read-and-delete.elektrad.info/download/Read\_And\_Delete-Live\_vom\_5ten\_Weltkongress\_der\_hedonistischen\_Internationale/10-Achtsamkeit.mp3">Audio:</link>

<link href="http://side-ways.net/portrait1\_de/">Web-Portrait über Elektra Wagenrad bei Side-ways.net:</link>

</links>

</event>

<event guid="JhCUm-jQqCMx\_jDfrzH24Q" id="6162">

<date>2014-12-28T14:00:00+01:00</date>

<start>14:00</start>

<duration>01:00</duration>

<room>Saal 6</room>

<slug>31c3\_-\_6162\_-\_en\_-\_saal\_6\_-\_201412281400\_-\_programming\_with\_dependent\_types\_in\_idris\_-\_raichoo</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Programming with dependent types in Idris</title>

<subtitle/>

<track>Science</track>

<type>lecture</type>

<language>en</language>

<abstract>Idris is a relatively young research programming languages that attempts to bring dependent types to general purpose programming. In this talk I will introduce the concept of dependent types and the Curry-Howard isomorphism and how these can be applied to prove properties about software and eradicate whole classes of bugs and security issues.</abstract>

<description>Building robust software is a hard task these days. As software gets more complex it gets increasingly hard to reason about it, this leads to a larger attack surface for bugs and security flaws.

Some of these bugs can be completely eliminated with the introduction of type systems that keep our values at runtime in check. Type systems are in fact the most widespread mechanism to verify correctness properties of programs, with dependent types we take this to the next level.

While most dependently typed systems (e.g. Coq and Agda) aim to be proof assistants rather than programming languages. Idris tries to answer the question how a general purpose programming language with dependent types could look like, it also enables us to produce self contained binaries as well as JavaScript applications today.

In this talk I will introduce techniques for programming with dependent types as well as interaction with the programming language itself. Examples will present resource tracking in the type system e.g. tracking file handles and yielding compilation errors on resource leaks, modeling specifications of protocols as types and enforcing them.

I argue that functional programming and dependently typed programming languages provide various exciting opportunities to the programmer, including a powerful mental model, compositionality and machine assisted programming through interactive editing capabilities. The presentation software for this talk will be a web application written in Idris which compiles to JavaScript using a compiler backend written by the lecturer.</description>

<persons>

<person id="3518">raichoo</person>

</persons>

<links>

<link href="https://github.com/idris-hackers/IdrisScript">IdrisScript</link>

<link href="https://github.com/raichoo/strangegroup-idris-June2014.">StrangeGroup Talk code examples</link>

</links>

</event>

<event guid="2yBK0TAIqddmCWa1MJUNQQ" id="6265">

<date>2014-12-28T16:00:00+01:00</date>

<start>16:00</start>

<duration>00:30</duration>

<room>Saal 6</room>

<slug>31c3\_-\_6265\_-\_en\_-\_saal\_6\_-\_201412281600\_-\_the\_automobile\_as\_massive\_data\_gathering\_source\_and\_the\_consequences\_for\_individual\_privacy\_-\_jimmy\_schulz\_-\_dr\_rudiger\_hanig</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>The automobile as massive data gathering source and the consequences for individual privacy</title>

<subtitle>The next big privacy heist</subtitle>

<track>Ethics, Society &amp; Politics</track>

<type>lecture</type>

<language>en</language>

<abstract>We report about a LOAD e. V. study regarding data collection of cars, future developments of this technology field, how this data is accessed and secured and what the stakeholders (car manufacturers, car owners and users) positions are on this data gathering. In a summary we outline necessary consequences.</abstract>

<description>We present a LOAD-study regarding car data. Aspects within the study are:

- Car data gathering today and expected developments,

- Data security and privacy of this data,

- Car manufacturers position regarding data ownership and access to this data,

- Survey results regarding current knowledge and understanding of car data gathering from car owners and users.

Aim of the study is to highlight current issues with car data gathering and outlining necessary consequences.

Über LOAD e. V. :

Das Internet ist ein Versprechen von Freiheit. LOAD ist der Zusammenschluss von Menschen, die sich gemeinsam für den Schutz dieser Freiheit einsetzen. LOAD ist Denkfabrik und Interessenvertretung und fördert die aktuellen und zukünftigen Netzbürgerinnen und Netzbürger bei der Verwirklichung ihrer Grundrechte. Wir werden den gesellschaftlichen digitalen Wandel konstruktiv unterstützen. Unsere Grundwerte sind Freiheit, Eigenverantwortung und das vorurteilsfreie Interesse an Neuerungen.</description>

<persons>

<person id="5017">Jimmy Schulz</person>

<person id="5359">Dr. Rüdiger Hanig</person>

</persons>

<links/>

</event>

<event guid="oN5AzdecYPpDFbE3nkJZFg" id="6406">

<date>2014-12-28T16:45:00+01:00</date>

<start>16:45</start>

<duration>00:30</duration>

<room>Saal 6</room>

<slug>31c3\_-\_6406\_-\_en\_-\_saal\_6\_-\_201412281645\_-\_long\_war\_tactics\_-\_sacha\_van\_geffen</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Long war tactics</title>

<subtitle>or how we learned to stop worrying and love the NSA</subtitle>

<track>Ethics, Society &amp; Politics</track>

<type>lecture</type>

<language>en</language>

<abstract>Referring to the seminal talk Dymaxion gave at the closing of the NoisySquare at OHM in 2013. This talk will explore what has happened and what has not in the mean time on the &quot;battle ground&quot;. An overview will be presented on the technical, legal, political and social battles going on and will provide pointers to further tactics. Finally we will look at how to make sure we keep ourselves safe and sane.</abstract>

<description>In many ways people have tried to rise against the extensive spying and logging of the five eyes and their allies. This talk tries to summarize the actions that have happened in different domains.

From this we will look forward to things that need to be done, effective tactics that we have seen from other domains and how to rewrite the rulebook.

This talk is meant to keep morale up and celebrate some of our victories, while at the same time proposing some tactics for future victories.</description>

<persons>

<person id="4227">Sacha van Geffen</person>

</persons>

<links/>

</event>

<event guid="8283fa4f-a6eb-4296-a6a8-20c3f9d80a4c" id="6589">

<date>2014-12-28T17:30:00+01:00</date>

<start>17:30</start>

<duration>00:30</duration>

<room>Saal 6</room>

<slug>31c3\_-\_6589\_-\_en\_-\_saal\_6\_-\_201412281730\_-\_mr\_beam\_goes\_kickstarter\_-\_teja\_philipp\_-\_philipp\_engel</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Mr Beam goes Kickstarter</title>

<subtitle>Lessons learned from crowdfunding a hardware project</subtitle>

<track>Hardware &amp; Making</track>

<type>lecture</type>

<language>en</language>

<abstract>Mr Beam was started as a hobby project aiming to get more experience in 3D printing. For fun we put it on Kickstarter and ended up in kind of a roller coaster. </abstract>

<description>After many years as a all purpose developer in several startups, I decided to explore the shiny new world of 3D printing.

Laser cutting seemed to be cool, useful and fun. The idea of reusing a dvd burner laser was nice and budget saving, some weeks later the first prototype wrote &quot;hello world&quot; on a piece of wood.

After spending another two month of improvements two friends joined and the idea of kickstarting a mini series production was born.

Finally the Kickstarter campaign was the reason for a lot of travel: Erfurt, Berlin, Barcelona, Tiflis, Vienna, Rome, Austin, San Francisco. On the road were awesome highlights as well as deep depressions.

All in all we didn't get rich in the end, but we got lots of experience in many different areas.

We believe that crowdfunding is a huge opportunity to develop things that otherwise never would have been done. We are happy to share all the lessons learned on our way. Hopefully other projects cause less headache with this knowledge.

</description>

<persons>

<person id="5257">Teja Philipp</person>

<person id="5320">Philipp Engel</person>

</persons>

<links>

<link href="www.mr-beam.org">Mr Beam - a DIY laser cutter &amp; engraver kit</link>

</links>

</event>

<event guid="1J0sEDUwTplMXgNU2Q7hrw" id="6148">

<date>2014-12-28T18:15:00+01:00</date>

<start>18:15</start>

<duration>00:40</duration>

<room>Saal 6</room>

<slug>31c3\_-\_6148\_-\_en\_-\_saal\_6\_-\_201412281815\_-\_open-bci\_diy-neuroscience\_maker-art\_mind-hacking\_-\_metamind\_evolution</slug>

<recording>

<license>CC-BY-SA</license>

<optout>false</optout>

</recording>

<title>Open-BCI DIY-Neuroscience Maker-Art Mind-Hacking</title>

<subtitle>open source DIY brain-computer-interfaces | technology and applications crash-course | &quot;BCI Mind-Hacking&quot; intro</subtitle>

<track>Hardware &amp; Making</track>

<type>lecture</type>

<language>en</language>

<abstract>leading hackers and researchers

from the worldwide hackerspace,

universitiy, and DIY artist community,

explain current technological

possibilites in BCI,

and show ways

to use open source

hardware and software

for hackers, makers, artists,

personal development, citizen science,

providing a framework

for alternative culture and free expression

balancing the soon coming commercial expansion

in &quot;Neurogaming&quot;, &quot;Neuromarketing&quot; and &quot;eHealth&quot;

talk will illustrate

the mutually beneficial relationship

between &quot;hacking&quot; and science,

with the example of hacking BCIs,

as well as an overview into the new field

of &quot;BCI Mind-Hacking&quot;, such as exploiting

remote consumer Neuroheadsets,

and Data-Mining the human-brain

for sensitive data during casual use.

</abstract>

<description>&lt;a href=&quot;https://events.ccc.de/congress/2014/wiki/Assembly:MindHacker-NeuroVillage&quot;&gt;

31C3-Assembly MindHacker-NeuroVillage&lt;/a&gt;

the talk is envisioned with 3-4 speakers:

1 x hacker / artist / visionary (15 years chaos-angel)

1 x university BCI Phd-candidate (Neuroscience)

1 x electronics engineer working 40 years in EEG

and can therefore include

various aspects of this topic:

artistic, political, scientific,

technological, instructional, etc ...

+ + +

talk will also illustrate

the mutually beneficial relationship

between &quot;hacking&quot; and science,

with the example of hacking BCI systems.

+ + +

&lt;a href=&quot;http://www.facebook.com/metavolution&quot;&gt;

LINK: MeTaMiNd EvoLuTioN (facebook)&lt;/a&gt;

&lt;a href=&quot;http://www.flickr.com/photos/metavolution/sets&quot;&gt;

LINK: MeTaVoLuT1oN photo gallery&lt;/a&gt;

+ + +

Exploiting consumer brain-computer-interfaces

A talk about future applications of consumer EEG devices, reflecting security risks, such as ways to leak private user information (health conditions, PIN-codes, known people and locations, EEG biometrics), and how to avoid this from happening. We introduce different exploit approaches that also have been proposed by academia. We will evaluate security risks by considering a few, conceivable scenarios coming up the next decade.

Finally, a call for participation:

we would like to discuss a possible open-source platform to exchange EEG data anonymously, suggested neurofeedback protocols, as well as machine learning powered EEG pattern simulations, covering some of the most prominent cognitive processes.

~ ~ ~

we are from the original

non-commercial and fully

open-source project wWw.Open-BCI.ORG,

as has been present at congress since 2007,

and publicly introduced with a talk at 28C3:

&lt;a href=&quot;http://youtu.be/GwzDXb4fzxo?t=18m48s&quot;&gt;

LINK: 28C3 Open-BCI talk video&lt;/a&gt;

&lt;br&gt;

- - - -

&lt;br&gt;

+ + +

Danc und GruC

&quot;MeTaMiNd EvoLuT1oN&quot;

~MeTA | OfficerOfTheSpacestation c-base

web: wWw.MeTa-MiNd.dE | www.Open-BCI.org

http://www.flickr.com/photos/metavolution/sets

http://www.open-bci.org/pix-promo-press

http://www.facebook.com/metavolution

http://twitter.com/metavolution/

youtube: http://bit.ly/ZijrIv

</description>

<persons>

<person id="4301">MeTaMiNd EvoLuTioN</person>

</persons>

<links>

<link href="http://wWw.Open-BCI.org">wWw.Open-BCI.oRG</link>

<link href="https://www.facebook.com/pages/MeTaVoLuTion-Open-BCI-Berlin/248072478585322">MeTaVoLuTion Open-BCI facebook page</link>

<link href="http://video.open-bci.org">MeTaVoLuT1oN-d3Mo bRAiNwAVe VIDEO</link>

<link href="http://open-bci.org/31c3/slides">Talk sLiDeS</link>

<link href="http://video-talk-28c3.open-bci.org">28C3 talk video </link>

<link href="http://kickstarter.open-bci.org">brain-Du1n0 kickstarter</link>

<link href="http://youtu.be/EbBGiqU6l28?list=PLbbCsk7MUIGcO\_lZMbyymWU2UezVHNaMq">Modern-BCI-Tech DataAnalysis INTRO</link>

</links>

</event>

<event guid="MBpSOQzfPD4ky0hqL6B-hg" id="5997">

<date>2014-12-28T20:30:00+01:00</date>

<start>20:30</start>

<duration>01:00</duration>

<room>Saal 6</room>

<slug>31c3\_-\_5997\_-\_en\_-\_saal\_6\_-\_201412282030\_-\_preserving\_arcade\_games\_-\_ange\_albertini</slug>

<recording>

<license>CC-BY-3.0</license>

<optout>false</optout>

</recording>

<title>Preserving arcade games</title>

<subtitle/>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>Old-school arcade games were so protected that hacking is the only way to preserve them before all boards are dead, and the games are lost.</abstract>

<description>- an overview of famous old-school arcade games

- their incredible hardware

- the permanent piracy

- the awesome protections (designed to commit suicide !)

- what was required to preserve some of them from being lost for ever.

This talk is a homage to Michael Steil's Ultimate Commodore 64 presentation at 25c3: you should watch it, it's inspiring in content and quality !</description>

<persons>

<person id="4585">Ange Albertini</person>

</persons>

<links/>

</event>

<event guid="lEFQRUU823FUOPqKG85vWg" id="6166">

<date>2014-12-28T21:45:00+01:00</date>

<start>21:45</start>

<duration>01:00</duration>

<room>Saal 6</room>

<slug>31c3\_-\_6166\_-\_en\_-\_saal\_6\_-\_201412282145\_-\_too\_many\_cooks\_-\_exploiting\_the\_internet-of-tr-069-things\_-\_lior\_oppenheim\_-\_shahar\_tal</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Too Many Cooks - Exploiting the Internet-of-TR-069-Things</title>

<subtitle/>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>TL;DR We unravel the story of a bug that would become one of the most important vulnerabilities released this year. Also, we have free cookies.

The findings we published earlier this year demystified the voodoo that is TR-069, demonstrated how mass pwnage can be achieved via server-side attacks, and proved the landscape is ripe for harvesting. We will continue where we left off to explore TR-069 client-side vulnerabilities; we analyze client implementations, pour some insight into mysterious results from our internet-wide scans, and follow to mass pwnage through remote code execution on millions of online devices. again.

</abstract>

<description>TR-069 is the de-facto standard remote management protocol that ISPs surreptitiously use to control consumer-premises equipment (these would be your home routers, set-top boxes, VoIP phones etc.), rumored to be a well-thought conspiracy devised by Internet Service Provider secret societies since the 17th century.

Since its establishment in 2004, there has been a growing trend of endorsement and deployment of the CWMP/TR-069 protocol in global carriers and service providers.

Despite the rising popularity of this black magic, it is often overlooked in penetration tests and security assessments of Internet gateway device attack surfaces, and wrongly so. Would they reconsider if they knew TR-069 the second most popular service openly listening on the Internet (after HTTP)?

This talk will begin by describing our previous efforts presented this summer (DEF CON 22 &amp; more), where our group revealed critically vulnerable TR-069 server deployments and discussed the incomprehensible asymmetry between the trust instated in this protocol and the measures taken to protect it (or lack thereof).

Subsequently, we decided to go after clients – exposing a critical attack surface by design, listening on 0.0.0.0 with a publicly available IP address. While centralized servers are rather easily patched to close security holes, clients may take more effort…

We will conclude with the shocking unveiling of one of the year's security stories, walking the audience through the discovery and exploitation of a memory corruption vulnerability in an extremely popular client implementation. Our weapon of choice this round would be embedded device reverse engineering (some soldering required), leading us all the way to remote code execution on millions of devices.</description>

<persons>

<person id="4861">Lior Oppenheim</person>

<person id="5294">Shahar Tal</person>

</persons>

<links>

<link href="https://www.defcon.org/html/defcon-22/dc-22-speakers.html#Tal">Previous talk description</link>

<link href="http://shahart.al/I-hunt-TR-069-admins-shahar-tal-dc22.pdf">Previous talk presentation</link>

</links>

</event>

<event guid="bX1J\_FaFjsFbyn15h7OGdg" id="6175">

<date>2014-12-28T23:00:00+01:00</date>

<start>23:00</start>

<duration>01:00</duration>

<room>Saal 6</room>

<slug>31c3\_-\_6175\_-\_en\_-\_saal\_6\_-\_201412282300\_-\_superheroes\_still\_need\_phoneboxes\_-\_ben\_dalton</slug>

<recording>

<license>CC-BY-3.0</license>

<optout>false</optout>

</recording>

<title>Superheroes Still Need Phoneboxes</title>

<subtitle>The art of making a free phonebox and the culture of anonymous communication</subtitle>

<track>Art &amp; Culture</track>

<type>lecture</type>

<language>en</language>

<abstract>This talk asks how we might plan for the continuation of a privacy sustaining internet in light of growing trends in enforced identity checking and demonisation of everyday anonymity. It presents a 'free phonebox' project, which was tested at the FutureEverything art and technology festival in 2014, as an example of a social-technical system that promotes identity ambiguity in communication through the sharing of 'free' mobile phone minutes between strangers.</abstract>

<description>The project presented in this talk uses a computer running debian to connect a USB handset to one of a number of 'donor' mobile phones by acting as a bluetooth handsfree headset to each of the mobiles. The project is based on No Hands a GPLv2 implementation of the Bluetooth HFP 1.5 Hands Free Protocol. A free phonebox that randomly assigns calls made to one of the participating mobiles nearby acts a little like a low-tech remailer (mix network node). Lending strangers your phone creates 'data chaff' that helps to muddy the call record metadata logs that otherwise tie your device to you as a form of identification and tracking. It provides (some) deniability for any calls made while nearby the phonebox. Borrowing a stranger's phone lets you call someone without revealing yourself through caller-id. The close range of bluetooth, imposes a geographic limit on users.

This talk considers why a project like a free phonebox may be useful in countering growing moves to criminalise anonymous communication. People generally see the 'free time' in their mobile cell phone call plans as something that belongs to them. Lending someone in need your phone is also seen as charitable and positive. Therefore, a system that shares phone minutes between strangers provides an easier forum for debate around preservation of anonymity in communication than a similar project lending wifi connectivity. Open wifi has been gradually characterised as a tool for malicious hackers, unethical pirates and tech-savvy criminals despite the significant advantages universal connectivity could offer. Historical examples of anonymising connectivity including phoneboxes and postal systems are discussed.

The public phonebox in particular has long been associated with elements of privacy, secrecy and anonymity. The physical box affords a semi-private space in a public setting. Sound is difficult to overhear, but the caller is still in view of those nearby. Phoneboxes have historically used an anonymous payment system of coins, and require no identity authentication for access. In many countries policies of regulating call costs and mandating maintained phonebox coverage have established phoneboxes as anonymous connectivity commons. Many accounts of phoneboxes in popular culture portray them as valued resources of personal independence. Phoneboxes often provide the backdrop for narratives of family contact, emergency assistance or first kisses. The cheap and near universal nature of the phonebox makes them a recognisable anchor of reliability in new situations and locations. I would argue it is no coincidence that Superman turns to the phonebox for a moment of privacy when changing from one pseudonym to another.

Ben Dalton is an artist and academic researcher trained in physics, electronics and communication design, who has worked on projects on distributed sensor networks and ubiquitous computing at the MIT Media Lab, USA, big screens and pocket screens in public space at Leeds Beckett University, UK, the aesthetic, ethical and spatial dimensions of the politics of data at the National Academy of Art &amp; Design in Bergen (KHiB), Norway, and digital pseudonymity at the Royal College of Art, UK. He has presented recent work on identity and pseudonmyity at the Institute of Contemporary Art (ICA) London, Foundation for Art and Creative Technology (FACT) Liverpool, FutureEverything Manchester, Today's Art The Hague, Abandon Normal Devices Liverpool, World Wide Web Conference (WWW2013) Rio de Janeiro, Sensuous Knowledge Bergen, and Designing Interactive Systems (DIS) Newcastle.</description>

<persons>

<person id="4863">Ben Dalton</person>

</persons>

<links>

<link href="http://futureeverything.org/events/nopayphone/">Project page at FutureEverything 2014</link>

<link href="http://skreened.com/dumbstuff/mouse-character">link to the t-shirt I was wearing</link>

</links>

</event>

</room>

</day>

<day date="2014-12-29" end="2014-12-30T04:00:00+01:00" index="3" start="2014-12-29T11:30:00+01:00">

<room name="Saal 1">

<event guid="iWU6RrYVPk7Q-fLuBE-LoQ" id="6123">

<date>2014-12-29T11:30:00+01:00</date>

<start>11:30</start>

<duration>01:00</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6123\_-\_en\_-\_saal\_1\_-\_201412291130\_-\_freedom\_in\_your\_computer\_and\_in\_the\_net\_-\_richard\_stallman</slug>

<recording>

<license>CC-ND</license>

<optout>false</optout>

</recording>

<title>Freedom in your computer and in the net</title>

<subtitle/>

<track>Ethics, Society &amp; Politics</track>

<type>lecture</type>

<language>en</language>

<abstract>For freedom in your own computer, the software must be free.

For freedom on the internet, we must organize against

surveillance, censorship, SaaSS and the war against sharing.</abstract>

<description>To control your computing, you need to control the software that does it. That means it must be \_free software\_, free as in freedom. Nonfree software is inherently unjust, and nowadays is often malware too. We developed the GNU system as a way to avoid nonfree software on our computers.

That assumes you're running your own copy of the programs. That means shunning Service as a Software Substitute, where someone else's copy in someone else's server does your computing.

Beyond that, we face the danger of censorship, and surveillance both on and off the internet. Lurking behind them is the menace of the War on Sharing, the publishers' decades-long campaign to control what we do in our computers. Increasingly, computer hardware itself is becoming malicious.

This talk will discuss these threats and the possible solutions.

</description>

<persons>

<person id="4948">Richard Stallman</person>

</persons>

<links/>

</event>

<event guid="7bdbb7a1-63f2-400f-97a1-d7abfc455f73" id="6583">

<date>2014-12-29T12:45:00+01:00</date>

<start>12:45</start>

<duration>02:15</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6583\_-\_de\_-\_saal\_1\_-\_201412291245\_-\_jahresruckblick\_des\_ccc\_-\_frank\_rieger\_-\_erdgeist\_-\_linus\_neumann\_-\_heckpiet\_-\_constanze\_kurz</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Jahresrückblick des CCC</title>

<subtitle/>

<track>CCC</track>

<type>lecture</type>

<language>de</language>

<abstract>Auch das Jahr 2014 geht irgendwann vorbei. Deshalb werfen wir einen Blick zurück auf die für uns besonders relevanten Themen und versuchen abzuschätzen, was im Jahr 2015 auf uns zukommen könnte.</abstract>

<description/>

<persons>

<person id="5183">Frank Rieger</person>

<person id="1544">erdgeist</person>

<person id="3995">Linus Neumann</person>

<person id="4834">heckpiet</person>

<person id="1630">Constanze Kurz</person>

</persons>

<links/>

</event>

<event guid="Rm1YndV-p\_f5\_NFEyPZMNA" id="6342">

<date>2014-12-29T16:00:00+01:00</date>

<start>16:00</start>

<duration>01:00</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6342\_-\_de\_-\_saal\_1\_-\_201412291600\_-\_deine\_rechte\_sind\_in\_diesen\_freihandelsabkommen\_nicht\_verfugbar\_-\_katharina\_nocun\_-\_maritta\_strasser</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Deine Rechte sind in diesen Freihandelsabkommen nicht verfügbar</title>

<subtitle>Der Protest gegen TTIP und CETA</subtitle>

<track>Ethics, Society &amp; Politics</track>

<type>lecture</type>

<language>de</language>

<abstract>Die Kritik am Freihandelsabkommen TTIP und CETA auf die Chlorhühnchen zu beschränken, greift viel zu kurz. Denn bei den beiden Abkommen zwischen der EU und den USA und der EU und Kanada steht noch viel mehr auf dem Spiel. Egal ob Datenschutz, Demokratie oder Urheberrecht – Abkommen, an denen Konzerne unter Ausschluss der Öffentlichkeit mitschreiben können, sind selten eine gute Idee. Sitzungsdokumente mit “unverbindlichen” Lobby-Vorschlägen und Leaks der Vertragstexte lassen wenig Gutes erwarten. Datenschutzstandards laufen Gefahr zu Handelshemmnissen erklärt zu werden. Konzerne pochen darauf, Staaten vor außerstaatlichen Schiedsgerichten auf Schadensersatz verklagen zu können. Was die Bürger wollen, wurde im ganzen Verhandlungsprozess der beiden Freihandelsabkommen nicht einmal gefragt. Doch “Klicktivismus” war gestern – neue Strategien und Tools halfen dabei, eine Welle des dezentralen Protests loszutreten. </abstract>

<description>Es blieb nicht bei Online-Appellen mit zusammen fast einer Million Unterzeichnern. Über das Netz wurden Flashmobs auf Wahlkampfevents der EU-Spitzenkandidaten organisiert. 6,5 Millionen “Denkzettel” wurden vor der EU-Wahl bundesweit an Türen gehängt – koordiniert über eine Software, die Verteilungsgebiete der Freiwilligen koordiniert. Ein breiter Protest sorgte dafür, dass TTIP zu einem der großen Themen im EU-Wahlkampf wurde.

230 Organisationen aus ganz Europa reichten im Sommer 2014 schließlich eine gemeinsame europäische Bürgerinitiative gegen TTIP und CETA bei der EU-Kommission ein. Ein europäischer Dachverband wurde gegründet, eine Stelle ausgeschrieben und besetzt und für die Fertigstellung der Open-Source-Software für die gemeinsame Petition fehlten nur noch wenige Code-Zeilen. Die für den Protest gegen TTIP und CETA entwickelten Petitions-Software soll außerdem auch für zukünftigen Bündnisse nutzbar sein.

Doch dann trat das Unvorstellbare ein: Die EU-Kommission will die Europäische Bürgerinitiative nicht zulassen. Doch die Bewegung gegen TTIP und CETA hat ihr Pulver noch lange nicht verschossen.

Wir zeigen, an welchen Stellen sich die Abkommen TTIP und CETA auf Netzpolitik, Datenschutz und Demokratie auswirken können, wie der kreative Protest sich mit digitalen Mitteln organisiert hat und und wie andere Kampagnen von diesen Erfahrungen möglicherweise profitieren können – und selbstverständlich auch, was die nächsten Schritte sein werden.</description>

<persons>

<person id="3869">Katharina Nocun</person>

<person id="5367">Maritta Strasser</person>

</persons>

<links>

<link href="https://www.campact.de">Campact e. V.</link>

</links>

</event>

<event guid="dN7QONPJousa5xBD6XQxgg" id="6140">

<date>2014-12-29T17:15:00+01:00</date>

<start>17:15</start>

<duration>01:00</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6140\_-\_en\_-\_saal\_1\_-\_201412291715\_-\_dp5\_pir\_for\_privacy-preserving\_presence\_-\_ian\_goldberg\_-\_george\_danezis\_-\_nikita\_borisov</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>DP5: PIR for Privacy-preserving Presence</title>

<subtitle/>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>In the wake of the Snowden revelations and the explicit targetting of address book and buddy list information, social service providers may wish to actively avoid learning which of its users are friends. In this talk, we will introduce the workings of a surprising technology called private information retrieval, or PIR. Then, we will describe its use in DP5, a new suite of privacy-preserving presence protocols that allow people to determine when their friends are online (and to establish secure communications with them), without a centralized provider ever learning who is friends with whom.</abstract>

<description>&lt;p&gt;Presenters:&lt;/p&gt;

&lt;ul&gt;&lt;li&gt;Nikita Borisov, University of Illinois at Urbana-Champaign&lt;/li&gt;

&lt;li&gt;George Danezis, University College London&lt;/li&gt;

&lt;li&gt;Ian Goldberg, University of Waterloo [currently on sabbatical at the

University of Cambridge]&lt;/li&gt;

&lt;/ul&gt;

&lt;p&gt;Description:&lt;/p&gt;

&lt;blockquote&gt;&lt;p&gt;&quot;We kill people based on metadata.&quot;&lt;br /&gt;&amp;mdash; General Michael Hayden&lt;/p&gt;&lt;/blockquote&gt;

&lt;p&gt;People like to know when their social contacts are online. Typically, this is done by a central server keeping track of who is online and offline, as well as of the complete friend graph of users. However, the Snowden revelations have shown that address book and buddy list information is routinely targetted for mass interception. Hence, some social service providers, such as activist organizations, do not want to even possess this information about their users, lest it be taken or compelled from them.&lt;/p&gt;

&lt;p&gt;Private information retrieval, or PIR, allows clients to download information from online databases without revealing to the database operators what information is being requested. In this talk, we will introduce the workings of this counterintuitive technology. Then, we will describe its use in DP5, a new suite of privacy-preserving presence protocols that allow people to determine when their friends are online (and to establish secure communications with them), without a centralized provider ever learning who is friends with whom.&lt;/p&gt;

&lt;p&gt;Bios:&lt;/p&gt;

&lt;p&gt;Nikita Borisov is an Associate Professor of Electrical and Computer Engineering at the University of Illinois at Urbana-Champaign. His research focuses on privacy and anonymity of online communications, as well as protecting the Internet from censorship. With Goldberg, he invented the Off-the-Record Messaging; his research has also influenced the design of the Tor network and the 802.11 security suite.&lt;/p&gt;

&lt;p&gt;George Danezis is a Reader in Security and Privacy Engineering at University College London (UK). In the past he has been doing security research at the University of Cambridge, KU Leuven and Microsoft Research. His research focuses on designing and analysing the privacy properties of anonymous communications systems, doing traffic analysis and understanding privacy technologies. He was the co-designer of the Mixminion remailer protocol, and proposed some of the first indirect traffic analysis, and DoS-based attacks against Tor.&lt;/p&gt;

&lt;p&gt;Ian Goldberg is an Associate Professor of Computer Science at the University of Waterloo, currently visiting the University of Cambridge. His research focuses on developing usable and useful technologies to help Internet users maintain their security and privacy. Once the Chief Scientist and Head Cypherpunk of Zero-Knowledge Systems, he is currently the chair of the board of directors of the Tor Project, Inc., one of the inventors of Off-the-Record Messaging, and a winner of the Electronic Frontier Foundation's Pioneer Award.&lt;/p&gt;</description>

<persons>

<person id="4944">Ian Goldberg</person>

<person id="5264">George Danezis</person>

<person id="5270">Nikita Borisov</person>

</persons>

<links/>

</event>

<event guid="k78-hNDINhkZS3TvxuLSrQ" id="6128">

<date>2014-12-29T18:30:00+01:00</date>

<start>18:30</start>

<duration>01:00</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6128\_-\_en\_-\_saal\_1\_-\_201412291830\_-\_thunderstrike\_efi\_bootkits\_for\_apple\_macbooks\_-\_trammell\_hudson</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Thunderstrike: EFI bootkits for Apple MacBooks</title>

<subtitle/>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>In this presentation we demonstrate Thunderstrike, a vulnerability that allows the installation of persistent firmware modifications into the EFI boot ROM of Apple's popular MacBooks. The bootkit can be easily installed by an evil-maid via the externally accessible Thunderbolt ports and can survive reinstallation of OSX as well as hard drive replacements. Once installed, it can prevent software attempts to remove it and could spread virally across air-gaps by infecting additional Thunderbolt devices.</abstract>

<description>It is possible to use a Thunderbolt Option ROM to circumvent the cryptographic signature checks in Apple's EFI firmware update routines. This allows an attacker with physical access to the machine to write untrusted code to the SPI flash ROM on the motherboard and creates a new class of firmware bootkits for the MacBook systems.

There are neither hardware nor software cryptographic checks at boot time of firmware validity, so once the malicious code has been flashed to the ROM, it controls the system from the very first instruction. It could use SMM and other techniques to hide from attempts to detect it.

Our proof of concept bootkit also replaces Apple's public RSA key in the ROM and prevents software attempts to replace it that are not signed by the attacker's private key. Since the boot ROM is independent of the operating system, reinstallation of OS X will not remove it. Nor does it depend on anything stored on the disk, so replacing the harddrive has no effect. A hardware in-system-programming device is the only way to restore the stock firmware.

Additionally, Thunderbolt devices' Option ROMs are writable from code that runs during the early boot and the bootkit could write copies of itself to new Thunderbolt devices. The devices remain functional, which would allow a stealthy bootkit to spread across air-gap security perimeters through shared Thunderbolt devices.

While the two year old Option ROM vulnerability that this attack uses can be closed with a few byte patch to the firmware, the larger issue of Apple's EFI firmware security and secure booting with no trusted hardware is more difficult to fix.</description>

<persons>

<person id="4825">Trammell Hudson</person>

</persons>

<links>

<link href="https://trmm.net/Thunderstrike">Thunderstrike overview and FAQ</link>

</links>

</event>

<event guid="Lt7ABZNFLzAgdiGcpHPHUQ" id="6366">

<date>2014-12-29T20:30:00+01:00</date>

<start>20:30</start>

<duration>00:30</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6366\_-\_de\_-\_saal\_1\_-\_201412292030\_-\_ifg\_mit\_freundlichen\_grussen\_-\_stefan\_wehrmeyer</slug>

<recording>

<license>CC-0</license>

<optout>false</optout>

</recording>

<title>IFG – Mit freundlichen Grüßen</title>

<subtitle>Neue Energie für die Informationsfreiheit</subtitle>

<track>Ethics, Society &amp; Politics</track>

<type>lecture</type>

<language>de</language>

<abstract>Die interessantesten IFG-Geschichten des Jahres mit Anfragen und Ablehnungen, Klagen und Kampagnen. Außerdem: wie wir mit Hilfe des Journalismus der Informationsfreiheit neuen Antrieb geben werden!</abstract>

<description>Nach dem Veröffentlichen eines Dokuments auf dem 30C3 fing 2014 für FragDenStaat.de mit einer Abmahnung und mehreren Anträgen auf einstweilige Verfügung an. Der erste Rechtsstreit „Bundesrepublik Deutschland gegen FragDenStaat.de“!

Einige weitere schöne Geschichten rund um das Informationsfreiheitsgesetz veranschaulichen den Zustand des IFG unter der neuen Bundesregierung und der neuen Informationsfreiheitsbeauftragten.

Außerdem möchte ich die ersten Ergebnisse der Kooperation zwischen FragDenStaat.de und dem gemeinnützigen Recherchebüro Correctiv.org vorstellen, die Informationsfreiheit bekannter und schlagkräftiger macht. </description>

<persons>

<person id="2262">Stefan Wehrmeyer</person>

</persons>

<links>

<link href="https://fragdenstaat.de">FragDenStaat.de</link>

</links>

</event>

<event guid="a7cde3ca-46a8-4f0b-be61-f60e77f3418e" id="6596">

<date>2014-12-29T21:15:00+01:00</date>

<start>21:15</start>

<duration>00:30</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6596\_-\_en\_-\_saal\_1\_-\_201412292115\_-\_the\_magical\_secrecy\_tour\_-\_leslie\_dunton-downer</slug>

<recording>

<license>CC-BY-3.0</license>

<optout>false</optout>

</recording>

<title>The Magical Secrecy Tour </title>

<subtitle>A Bus Trip into the Surveillance Culture of Berlin One Year After Snowden</subtitle>

<track>Art &amp; Culture</track>

<type>lecture</type>

<language>en</language>

<abstract>June 5, 2014 marked one year since leaks by NSA whistleblower Edward Snowden began to be introduced to a worldwide public. On this date, transmediale teamed up with N.K. Projekt and Leslie Dunton-Downer, 2014 fellow at The American Academy in Berlin, for the Magical Secrecy Tour, a bus journey exploring Berlin as the global capital of informed response to mass surveillance. This inside look at the project features first-ever screening of footage shot by filmmaker Simon Klose (TPB AFK) for his documentary about the tour.</abstract>

<description/>

<persons>

<person id="5280">Leslie Dunton-Downer</person>

</persons>

<links>

<link href="http://www.transmediale.de/content/the-magical-secrecy-tour">The Magical Secrecy Tour</link>

</links>

</event>

<event guid="5hkhmuwi5J8ZHMfd5k7veg" id="6243">

<date>2014-12-29T22:00:00+01:00</date>

<start>22:00</start>

<duration>00:30</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6243\_-\_en\_-\_saal\_1\_-\_201412292200\_-\_the\_perl\_jam\_exploiting\_a\_20\_year-old\_vulnerability\_-\_netanel\_rubin</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>The Perl Jam: Exploiting a 20 Year-old Vulnerability</title>

<subtitle/>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>tl;dr EXPLOIT ALL THE PERL.

We chained several of Perl’s ridiculous syntax quirks in order to create a surprisingly powerful attack, bringing down some of the most popular Perl-based projects in the world to their knees. Brace yourselves, RCE exploits are coming.</abstract>

<description>Deemed ‘the write-only programming language’ by many, Perl has well-served its purpose as a successful subject for less successful programmer jokes. It’s self-obfuscating ‘TMTOWTDI’ syntax is one of the top reasons for sysadmin PTSD, nervous breakdowns, and marriage problems.

Sadly, it is 2014 and Perl still maintains a top-10 position in programming language popularity indexes – sometimes higher than JavaScript. This can be attributed to the fact it is the underlying platform running many applications still widespread today such as ‘cPanel’ or ‘Bugzilla’, as well as high-profile web sites such as Craigslist, IMDb, Slashdot, DuckDuckGo and TicketMaster, among others.

This talk will spawn a wormhole 20 years into the past, and dive into some of the more hazardous and fundamental language quirks (WAT-style), walking the audience through the discovery of vulnerable core modules and the implementation of a new exploitation technique (branding and logo included!). Using this technique, we unleash a Pandora’s box of exploits to vulnerabilities hidden under the surface for years, in some of the most popular Perl-based projects in the world. Hilarity ensuance guaranteed.</description>

<persons>

<person id="5034">Netanel Rubin</person>

</persons>

<links/>

</event>

<event guid="Q41efHdmmnBkM5G8p6Wf\_w" id="5966">

<date>2014-12-29T22:45:00+01:00</date>

<start>22:45</start>

<duration>00:30</duration>

<room>Saal 1</room>

<slug>31c3\_-\_5966\_-\_en\_-\_saal\_1\_-\_201412292245\_-\_unhash\_-\_methods\_for\_better\_password\_cracking\_-\_tonimir\_kisasondi</slug>

<recording>

<license>CC-BY-3.0</license>

<optout>false</optout>

</recording>

<title>UNHash - Methods for better password cracking</title>

<subtitle/>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>This talk will show a new method for password cracking called UNHash. UNHash as a tool uses rulefiles that are something in between of a DSL (Domain specific language) and a python script to describe the password cracking process. This talk will show how to mix web service abuse, knowledge of human nature and data mining to enable far better attacks against passwords. We will be focusing on a few features: cracking default passwords on network systems with minimal effort, testing for embedded backdoors and offline attacks by data mining and modeling about 33 million user account to gain insight in how users choose their passwords and how can we use that knowledge to speed up password cracking for 20% more gain for non pseudorandom passwords.</abstract>

<description>This talk will show a new method for password cracking called UNHash. UNHash as a tool uses rulefiles that are something in between of a DSL (Domain specific language) and a python script to describe the password cracking process. That way, we have the possibility to describe complex password cracking rules that contain dictionaries, rules, bruteforcing, joining, combining and other patterns in a language that is easily human readable and extensible. To stop reinventing the wheel, UNHash generates candidate passwords for john the ripper, hashcat or a lot of other tools that can read stdin.

The usage of &quot;slow&quot; hashes like bcrypt and scrypt will require us to try a smaller quantity of possible passwords, but with more detailed targeting. The concept behind UNHash is to enable such attacks against modern slow hashes or to enable better targeting and be faster and easier then traditional methods.

To make use of the new &quot;language&quot;, we need set of rules. To generate rulesets, we will show a new machine learning algorithm that can analyze plaintext passwords and generate rules for UNHash. The machine learning algorithm shows a classifier network heuristic that we call the sieve algorithm that can classify passwords and show how users generate their passwords. Training the classifier on about 30+ million unique passwords, can yield interesting rules that describe how users pick their passwords.

Since we are already classified passwords, why not use the effort to collect all password elements like words (and see which languages do they belong), strings, numbers and mutations so we can use that as a cornerstone for a new set of dictionaries. Since we already said said that we want to identify words and their languages, we needed to create a linguistic dictionary for word the use in the classifier algorithm. We will show how to create custom dictionaries for various languages or from a specific domain by parsing wikipedia database backups or by abusing really popular web services.

A small portion of the talk will show why it is useful to scrape password dumps or obtain them via low interaction honeypots in order to collect known backdoor passwords.

We will skip the science and get to the practical part - How can you use UNHash for better password cracking and how to implement more classifiers so we can have a better models of how users create their passwords.

</description>

<persons>

<person id="2791">Tonimir Kisasondi</person>

</persons>

<links/>

</event>

<event guid="rSiFVNguzdBmx13Lb-gobg" id="6205">

<date>2014-12-29T23:30:00+01:00</date>

<start>23:30</start>

<duration>00:30</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6205\_-\_en\_-\_saal\_1\_-\_201412292330\_-\_infocalypse\_now\_p0wning\_stuff\_is\_not\_enough\_-\_walter\_van\_holst</slug>

<recording>

<license>CC-BY-SA</license>

<optout>false</optout>

</recording>

<title>Infocalypse now: P0wning stuff is not enough</title>

<subtitle>Several failure modes of the hacker scene</subtitle>

<track>Ethics, Society &amp; Politics</track>

<type>lecture</type>

<language>en</language>

<abstract>This speech about how the hacker scene is failing its own ideals and what questions must be addressed to make a real difference.</abstract>

<description>Every year Chaos Congress is a venerable display of ingenuity in the hacker scene. Every year there are more visitors, more and often better talks on security issues, society, culture and technology in general. At the same time the social and political clouds that appeared on the horizon are now overhead and are even darker than expected. Discussing last year's big exploits and congratulating each other on our ingenuity in finding them is not enough. We have to wipe the smug grins from our faces and take a long hard look into the mirror. Because there are several questions that are often unasked because we may not have the answer to them. Not solving these puzzles also means that we cannot prevent the infocoalypse of big data, the internet of things, the military-industrial-surveillance complex as well as organised crime mucking up our lives. So let us talk about our failures to:

- explain general purpose computing to laypersons;

- preventing security weaknesses from happening;

- articulate security risks to everyday people and politicians alike;

- educate fellow tech people about them,

And why they are failures and why there is an urgent need to fix them.</description>

<persons>

<person id="5016">Walter van Holst</person>

</persons>

<links/>

</event>

<event guid="Ls3UZdXbRpTYhYncqSJN\_w" id="6226">

<date>2014-12-30T00:15:00+01:00</date>

<start>00:15</start>

<duration>02:00</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6226\_-\_de\_-\_saal\_1\_-\_201412300015\_-\_googlequiz\_2015er\_edition\_-\_joran\_muuss-merholz\_-\_ralf\_appelt\_-\_blanche\_fabri\_-\_it4n6\_-\_martin\_kronke</slug>

<recording>

<license/>

<optout>true</optout>

</recording>

<title>Googlequiz – 2015er Edition</title>

<subtitle>Neue Spiele, neue Musik und noch mehr Luftballons</subtitle>

<track>Entertainment</track>

<type>other</type>

<language>de</language>

<abstract>Beim Googlequiz spielen max. 7 Teams mit je max. 7 Spielern gegeneinander. Sie dürfen dabei nicht Google benutzen. Es ist eine recht spaßorientierte Angelegenheit, so dass auch Zuschauer willkommen sind.</abstract>

<description>Beim Googlequiz werden Aufgaben gestellt, für die man im Kopf bzw. im Team Lösungen sucht. Google oder überhaupt das Internet darf dafür nicht genutzt werden. Vorkenntnisse braucht man nicht.

Das Googlequiz war 2014 schon ziemlich gut.

Für 2015 bauen wir eine komplette Neuauflage.

Die Vorbilder, von denen die 2015er Edition inspiriert ist, heißen: Der Preis ist heiß, Glücksrad, Eins-Zwei-oder-Drei, Familienduell, Ruck-Zuck, Wikipedia.

Die Dinge, die beim #30c3 neu und gut waren, werden ausgebaut: laute, irritierende Musik sowie laute, irritierende Luftballons.</description>

<persons>

<person id="3584">Jöran Muuß-Merholz</person>

<person id="5347">Ralf Appelt</person>

<person id="3693">Blanche Fabri</person>

<person id="3706">it4n6</person>

<person id="5365">Martin Krönke</person>

</persons>

<links>

<link href="http://googlequiz.de">googlequiz.de</link>

<link href="https://twitter.com/googlequiz">@googlequiz</link>

<link href="https://www.facebook.com/googlequiz">facebook.com/googlequiz</link>

<link href="https://plus.google.com/b/111843060801184524486/+GooglequizDe/photos/">Fotos bei G+</link>

</links>

</event>

</room>

<room name="Saal 2">

<event guid="Z4htibNZxLewwCmPKSdeqA" id="6430">

<date>2014-12-29T11:30:00+01:00</date>

<start>11:30</start>

<duration>01:00</duration>

<room>Saal 2</room>

<slug>31c3\_-\_6430\_-\_de\_-\_saal\_2\_-\_201412291130\_-\_nsa\_points\_of\_presence\_in\_at\_-\_erich\_moechel</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>NSA Points of Presence in AT</title>

<subtitle>Vortrag mit aktuellen Fotos aus luftigen Perspektiven</subtitle>

<track>Ethics, Society &amp; Politics</track>

<type>lecture</type>

<language>de</language>

<abstract>- Station VIENNA in der US-Botschaft 1090 Wien

- VIENNA ANNEX beim UNO-Sitz in Wien 1220

- Legacy Standort „NSA-Villa“ Wien 1180

- Relaystation Exelberg,Breitbandnetz von NSA/SCS über Wien

- Equipment und Funktion der FORNSAT-Station Königswarte.</abstract>

<description>Die weitaus größte Installation der US-Dienste befindet sich auf der Königswarte an der slowakischen Grenze. Zu Zeiten des Kalten Kriegs diente die Königswarte den Allierten als vorgeschobener Horchposten am Eisernen Vorhang bei Hainburg, um analoge Funkstrecken der Telekoms und militärische Kommunikation im Ostern abzuhören. Ab 2001 begannen neue, andersartige Antennen auf dem Areal der Königswartezu wachsen, enorme Parabolspiegel, die gen Himmel gerichtet sind. Die größten dieser Hochleistungsspiegel haben einen Durchmesser von mehr als zehn Metern, mittlerweile sind es 18 Stück, die allesamt zivile Kommunikationsatelliten anvisieren. Unter der Königswarte befindet sich ein enormes subterranes Rechenzentrum, das geht aus den Luftaufnahmen eindeutig hervor. Dazu wurde eine weitere, bis dato nicht dokumentierte US-&quot;Kommunikationsstation&quot; am Dach eines Hochhauses direkt neben der UNO-City entdeckt. Beide finden sich unter ihren Decknamen in den von Edward Snowden geleakten Dokumenten. Welche Art von Daten an diesen und den anderen Standorten - US-Botschaft in Wien und &quot;NSA-Villa&quot; - abgefangen, verarbeitet und abtransportiert werden lässt sich nun bereits abschätzen.

</description>

<persons>

<person id="5097">Erich Moechel</person>

</persons>

<links/>

</event>

<event guid="\_jFN0YWHACogrN4ddVWK0Q" id="6261">

<date>2014-12-29T12:45:00+01:00</date>

<start>12:45</start>

<duration>01:00</duration>

<room>Saal 2</room>

<slug>31c3\_-\_6261\_-\_en\_-\_saal\_2\_-\_201412291245\_-\_let\_s\_build\_a\_quantum\_computer\_-\_andreas\_dewes</slug>

<recording>

<license>CC-BY-3.0</license>

<optout>false</optout>

</recording>

<title>Let's build a quantum computer!</title>

<subtitle>Understanding the architecture of a quantum processor</subtitle>

<track>Science</track>

<type>lecture</type>

<language>en</language>

<abstract>I will explain why quantum computing is interesting, how it works and what you actually need to build a working quantum computer. I will use the superconducting two-qubit quantum processor I built during my PhD as an example to explain its basic building blocks. I will show how we used this processor to achieve so-called quantum speed-up for a search algorithm that we ran on it. Finally, I will give a short overview of the current state of superconducting quantum computing and Google's recently announced effort to build a working quantum computer in cooperation with one of the leading research groups in this field.</abstract>

<description>Google recently announced that it will partner up with John Martinis -one of the leading researchers on superconducting quantum computing- to build a working quantum processor. This announcement has sparked a lot of renewed interest in a topic that was mainly of academic interest before. So, if Google thinks it's worth the hassle to build quantum computers then there surely must be something about them after all?

With this talk, I want to provide a better understanding of why quantum computing is interesting and how we might actually build a working quantum computer one day. As an example, I will discuss the two-qubit chip that I built during my PhD thesis as a realization of a basic, functional two-qubit quantum processor. I will explain the building blocks of this processor and show how we can manipulate the qubits, read out their state with high fidelity and couple them to each other in order to realize two-qubit gate operations.

I will then show how we used this processor to demonstrate the concept of &quot;quantum speed-up&quot; by implementing and running the so-called Grover quantum search algorithm on it.

Finally, I will give a brief overview of the current state of quantum computing and explain the (likely) approach followed by Google and John Martinis to realize a working, large-scale quantum processor, as well as some problems they will have to overcome on their way.</description>

<persons>

<person id="5040">Andreas Dewes</person>

</persons>

<links>

<link href="http://www.slideshare.net/japh44/demonstrating-quantum-speedup-with-a-twotransmon-quantum-processor-phd-defense-upmc-cea-15112011">My PhD Defense Presentation (this is NOT going to be the talk I'm giving since it's way too technical)</link>

<link href="http://www.andreas-dewes.de/en/publications">Link to my publications and PhD thesis</link>

</links>

</event>

<event guid="P8L4krxqjXP7zHMZToU6CQ" id="6350">

<date>2014-12-29T14:00:00+01:00</date>

<start>14:00</start>

<duration>01:00</duration>

<room>Saal 2</room>

<slug>31c3\_-\_6350\_-\_en\_-\_saal\_2\_-\_201412291400\_-\_correcting\_copywrongs\_-\_julia\_reda</slug>

<recording>

<license>cc0</license>

<optout>false</optout>

</recording>

<title>Correcting copywrongs</title>

<subtitle>European copyright reform is finally on the horizon</subtitle>

<track>Ethics, Society &amp; Politics</track>

<type>lecture</type>

<language>en</language>

<abstract>After years of debate, EU copyright law is finally being revisited. The Commission will present a proposal for reform within 4 months of 31c3. And it's high time: There has never been a bigger discrepancy between the technical feasibility to share information and knowledge across all physical borders and the legal restrictions to actually do so. This talk outlines the unique opportunity and the challenge to bring copyright into the 21st century that lies in front of us. Hackers ensured that people were heard during last winter's public consultation. Can they now also ensure a progressive outcome of the reform process?</abstract>

<description>When copyright was last reformed on an EU level, YouTube and Facebook didn't exist, smartphones were unheard of. Last winter, the European Commission finally started a public consultation aimed at identifying all the ways in which the current copyright regime has been outdated by technological developments. Through projects such as Copywrongs.eu, which was developed at a workshop at 30c3, activists took it upon themselves to open the consultation to a wider audience and ensure that end users were heard. The tools they developed for that purpose, published under free licences, were even picked up by collecting societies to mobilise their members for replying to the consultation. The resulting over 9000 responses, half of which came from end users, reveal a deep divide: Individuals, cultural institutions such as libraries and scientists are calling for Europe-wide reform, whereas rightsholders are trying to defend the status quo. But the answers also point at some surprising similarities in the views of some respondents that can lead to new alliances and a copyright reform that truly finds a balance between competing societal goals.

The new EU commission was tasked by their president to present a proposal for copyright reform within 4 months of 31c3. After years of debate, 2001's copyright directive is finally being revisited. Promisingly, the mandate for copyright legislation in the new Commission has been moved from a directorate concerned mostly with economic issues to the one for “Digital Society &amp; Culture”. The last Commissioner responsible for this field, Neelie Kroes, ended her mandate with a passionate call for copyright reform, describing the current legal framework in the EU as &quot;fragmented, inflexible, and often irrelevant&quot;.

But what can we expect from the responsible Commissioner Guenter Oettinger, who's clearly not a digital native, and who has to answer to Commission Vice-President Andrus Ansip, formerly a fervent supporter of the Anti-Counterfeiting Trade Agreement ACTA? I'll explain what the new structure of the Commission means for copyright reform, who the players are, the expected timeline, what we may hope to achieve and how you can help ensure an ambitious, progressive and user-friendly outcome. This talk is also a call for hackers to involve themselves in traditional arenas of policy-making and to become more political in their demands and activities.</description>

<persons>

<person id="5062">Julia Reda</person>

</persons>

<links>

<link href="http://juliareda.eu">juliareda.eu</link>

</links>

</event>

<event guid="\_kPJG76FUvxbX7Z6h20Gcw" id="6161">

<date>2014-12-29T16:00:00+01:00</date>

<start>16:00</start>

<duration>01:00</duration>

<room>Saal 2</room>

<slug>31c3\_-\_6161\_-\_en\_-\_saal\_2\_-\_201412291600\_-\_emet\_5\_1\_-\_armor\_or\_curtain\_-\_rene\_freingruber</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>EMET 5.1 - Armor or Curtain?</title>

<subtitle/>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>EMET (Enhanced Mitigation Experience Toolkit) is an application which can be used to further harden a Windows system by adding additional security protections to running processes. These protections include several ROP (Return-Oriented-Programming) checks, shellcode detection mechansims, heap-spray mitigations and many more.

The talk covers techniques to bypass EMET 5.1 (the current version) and shows the audience how hard/easy it is for an attacker to accomplish this.</abstract>

<description>The Enhanced Mitigation Experience Toolkit (EMET) is an application developed by Microsoft which adds an additional layer of security to applications to prevent attackers exploiting vulnerabilities in them.

It can be used to globally enable system mitigation techniques such as Address Space Layout Randomization (ASLR), Data Execution Prevention (DEP) or Structured Exception Handler Overwrite Protection (SEHOP). In addition special per-process protections can be added such as various Return-Oriented-Programming (ROP) protections (LoadLibrary, MemProt, Caller, SimExecFlow, StackPivot), Export Address Table Access Filtering (EAF and EAF+) to prevent execution of shellcode, pre-allocations to defeat heap spraying and kernel exploitation, additional randomization (bottom-up randomization and mandatory ASLR) and advanced mitigations (deep hooks, anti detours and banned functions) to prevent different types of attacks.

If an application supports DEP together with full ASLR the difficulty to write a reliable exploit increases dramatically. The typical approach to defeat DEP is to use ROP to disable it. ROP builds on the idea to return (or jump) to small so-called gadgets (which are equal to already existing code from the code-section which end with a return or jump instruction) to chain these gadgets together to build new logic (like logic to disable DEP). If ASLR is supported by all modules of the application this approach can't be applied because the address of such gadgets is randomized by ASLR and thus unknown by the attacker. In such a case the vulnerability must be turned into an information disclosure vulnerability to first disclose an address to defeat ASLR. Techniques to accomplish this (e.g. partial overwrites, overwriting the length field of strings, ...) have already been discussed in the past and thus will not be focus of this talk.

Instead further techniques will be discussed which can be used to bypass the additional per-process protections of EMET. To apply these techniques a vulnerability which allows code execution as well as leaking information (to bypass ASLR) is required. These requirements are satisfied per default because otherwise writing an exploit for a not-EMET protected application would be impossible.

The aim of this talk is to demonstrate new and more reliable exploitation techniques as well as discussing in which situations already existing techniques can be applied in a reliable way.

An important approach of exploit developers is to write bypasses in a way that they can easily be ported to other exploits. For example, if a technique requires jumping to already existing code a dumb approach would be to build it application specific. Instead the technique can be built on top of the EMET library which gets injected into all protected applications and thus is a good target to minimize work load because the code for the bypass must only be written one time. To apply such techniques various methods to identify the presence, retrieving the imagebase as well as the version of EMET will be shown.

EMET also supports none memory corruption related protection techniques (like Attack Surface Reduction ASR and certificate pinning), however these will not be discussed during the talk because the focus of the talk is on memory corruption exploitation (e.g. buffer overflows, use-after-free bugs, type confusion attacks and so on).

All techniques are implemented and demonstrated in a real-world Firefox exploit. Even if the vulnerability is older (we at SEC Consult don't want to publish reliable working exploit code for applications which are still in-use these days) it is a very interesting vulnerability to study and together with a highly configurable exploit it's easy to see the different techniques in action. The exploit works reliable against any Windows operating system (Windows XP, Windows Vista, Windows 7, Windows 8, Server 2003, Server 2008, Server 2012, ...), on 32-bit as well as on 64-bit architectures and is able to bypass EMET in all versions (EMET 4.1, 5.0 and 5.1) with all protections enabled.

Microsoft as well as other vendors typically suggest as a workaround for new memory corruption vulnerabilities to install EMET to protect the application. The aim of the presentation is to show the audience that attackers can still exploit such protected applications by using one of the many existing techniques.

We at SEC Consult do not believe in putting additional security layers like EMET, DEP, ASLR, application firewalls and so on on top of applications. Rather we demand from software developers and especially from the software industry itself to focus on secure software development instead of forcing their customers to create a chain of security layers to protect their software product.

Protections such as EMET, DEP and ASLR are useful to add an additional hurdle for attackers but are not unbreakable.</description>

<persons>

<person id="4988">René Freingruber</person>

</persons>

<links/>

</event>

<event guid="uMGv2XJJqkQodKm0\_Mtr\_A" id="6121">

<date>2014-12-29T17:15:00+01:00</date>

<start>17:15</start>

<duration>01:00</duration>

<room>Saal 2</room>

<slug>31c3\_-\_6121\_-\_en\_-\_saal\_2\_-\_201412291715\_-\_what\_ever\_happened\_to\_nuclear\_weapons\_-\_michael\_buker</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>What Ever Happened to Nuclear Weapons?</title>

<subtitle>Politics and Physics of a Problem That's Not Going Away</subtitle>

<track>Ethics, Society &amp; Politics</track>

<type>lecture</type>

<language>en</language>

<abstract>An overview of 70 years of nuclear weapons, focusing on some of the underlying physics, the international politics that surround the topic, modern technology for nuclear weapons detection and monitoring, and what everyone can do to help nuclear disarmament.</abstract>

<description>With the end of the Cold War, the sense of imminent danger from nuclear weapons quickly faded. But the weapons never went away: Today, half the world's population lives in countries with nuclear weapons. Roughly 15,000 nuclear warheads, each powerful enough to destroy a city, are in the hands of nine countries.

The most important international treaty on nuclear weapons states that only five countries can ‘legally’ have them. But over the last 50 years, eight other countries have come into their posession, four of which are established nuclear powers today. How did that happen?

Moreover, nuclear tests of different kinds are banned by a multitude of international treaties. An impressive global measurement network of hundreds of seismic, hydroacoustic, infrasound and radionuclide measurement stations has been set up to detect nuclear tests. However, a treaty to finally ban all sorts of nuclear explosions, signed by 183 countries, is on the brink of failing. What is up with that?

This talk aims to provide a broad physical, technical and historical overview of the topic of nuclear weapons, and explain where international politics and verification technology stand today.</description>

<persons>

<person id="4920">Michael Büker</person>

</persons>

<links/>

</event>

<event guid="p6g2YacbVEfuPkJ01kvHAw" id="6043">

<date>2014-12-29T18:30:00+01:00</date>

<start>18:30</start>

<duration>01:00</duration>

<room>Saal 2</room>

<slug>31c3\_-\_6043\_-\_en\_-\_saal\_2\_-\_201412291830\_-\_the\_maker\_movement\_meets\_patent\_law\_-\_natalia\_lukaszewicz</slug>

<recording>

<license>CC-BY-3.0</license>

<optout>false</optout>

</recording>

<title>The Maker movement meets patent law</title>

<subtitle>How many windows are open in the patent fortress</subtitle>

<track>Hardware &amp; Making</track>

<type>lecture</type>

<language>en</language>

<abstract>The Maker movement and patent law are like two planets moving on the orbit of innovations. Occasionally, they collide … because the Maker planet moves too fast.

But, back on the Earth. Encounters with patent law can be of many reasons, e.g. filing a patent application or being blocked in making by a patent (or much worse, being accused of a patent infringement). The latter motivated the question of the permissible uses of patented inventions. The talk explains which activities on patents are lawful and keep Makers safe in their making.

</abstract>

<description>The Maker Movement does not need to be presented. Even the White House has expressed its gratitude and admiration for individual inventors – single heroes; and the World Bank has recognised their potential.

But the daily life of Makers is not (always) that sweet and victorious. As they get more technologically advanced, they face new challenges: financial, resource-related or legal.

The project focuses on the legal aspects, specifically on patent law. There are two ways Makers meet with patents: 1) they want to obtain a patent for their solution, 2) they get confronted with a patent infringement claim. The latter led to the question of the efficacy of patent flexibilities (“patent windows”) that reduce the patent exclusivity over the use of an invention. They provide both the freedom to operate and enable defence in patent infringement lawsuits.

The project also contributes to the ongoing discussion on the reform of patent law, and suggests the re-consideration of certain legal tools in the light of the Maker phenomenon.

Beyond any doubt, Makers deserve special attention in the legal field for a number of reasons:

1) their technological contributions,

2) popularisation of democratic ideas: participation, trust and responsibility,

3) for making a part of this world better.

(The patent system shared once the same principles … before it has changed into a money-making machine.)

The reference point for the research is collective making: when an idea leaves the safe private harbour (adverbial basements and garages) and enters open waters of knowledge dissemination and commercialisation, where a patent infringement may easily occur. Against this background I analyse the scope of patent windows (statutory provisions and doctrines) stipulated in four legal systems: Germany, the UK, the USA, and Japan. I present the main construction lines and apply them to the Maker environment. There are measures, e.g. private and non-commercial use or experimental use, that work in “making” but under certain reservations.

The talk serves advising and increasing the awareness of the scope of the permissible uses on patented solutions.

</description>

<persons>

<person id="4843">Natalia Lukaszewicz</person>

</persons>

<links/>

</event>

<event guid="4f9TGtkPJafH9LU7RqsZnw" id="6275">

<date>2014-12-29T20:30:00+01:00</date>

<start>20:30</start>

<duration>00:30</duration>

<room>Saal 2</room>

<slug>31c3\_-\_6275\_-\_en\_-\_saal\_2\_-\_201412292030\_-\_living\_drones\_-\_anja\_drephal</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Living Drones</title>

<subtitle>From war pigeons in 1914 to cyborg moths in 2014</subtitle>

<track>Science</track>

<type>lecture</type>

<language>en</language>

<abstract>During World War I, homing pigeons were used to carry messages and take photographs over enemy territory. Today, experiments are being conducted to remote-control insects for similar purposes.

This talk intends to give an overview of 100 years of living drones, speculate on future developments in the field, and question the ethical implications of the practice.</abstract>

<description>Long before man-made aerial vehicles were invented and perfected, pigeons have been employed to carry messages over long distances. Their homing instinct, the ability to find their way back to their home loft from as far as 1,000 miles away, has been known and used by mankind since ancient times. While regular pigeon post had been established since the Middle Ages, it was during World War I that pigeons were used extensively for military purposes: radio communication was still crude and unreliable, but pigeons were fast and dependable means of delivering messages from behind enemy lines. With the advancement of photography, they were even employed as aerial surveillance drones, equipped with small automatic cameras.

Although the US and British armies disbanded their pigeon sections in the 1950s, carrier pigeons are being used for communication purposes until today.

Taking the idea of connecting flying animals with communication technology one step further, as of 2014, experiments are being conducted in wiring and remote-controlling moths, effectively turning them into biobots to be used for search and rescue missions – and possibly for military and surveillance purposes?</description>

<persons>

<person id="4221">Anja Drephal</person>

</persons>

<links>

<link href="http://www.computerworld.com/article/2598546/emerging-technology/cyborg-moths-could-act-like-living-drones-in-search-and-rescue.html">Cyborg Moths</link>

</links>

</event>

<event guid="iU5CnqxotZz\_KK2P-uVMsQ" id="6253">

<date>2014-12-29T21:15:00+01:00</date>

<start>21:15</start>

<duration>00:30</duration>

<room>Saal 2</room>

<slug>31c3\_-\_6253\_-\_en\_-\_saal\_2\_-\_201412292115\_-\_computer\_science\_in\_the\_dprk\_-\_will\_scott</slug>

<recording>

<license>CC BY 3.0</license>

<optout>false</optout>

</recording>

<title>Computer Science in the DPRK</title>

<subtitle>A view into technology on the other side of the world</subtitle>

<track>Ethics, Society &amp; Politics</track>

<type>lecture</type>

<language>en</language>

<abstract>This talk will reflect on teaching Computer Science in Pyongyang over the last two years, and look at how technology has been integrated into civilian life in the DPRK. Remaining an extremely isolated country, many people would be surprised to hear that cellphones have become commonplace within the capitol, let alone that the country invests in custom hardware and software. I'll talk through the current state of desktop and mobile technology in pyongyang, and what's changing.</abstract>

<description>From redstar OS, a custom redhat-derived linux desktop and server environment, to the arirang cellphone and tablet, technology in the DPRK is different from what you are likely to see anywhere else in the world. Most systems are not widely available, and exist as much in rumor as reality. Partially from language barrier, and partially due to restrictive import, export, and communication policies, there are large gaps and large amounts of misinformation around most aspects of the country.

I've spent the last two falls teaching Computer Science, specifically Operating Systems and Databases, to undergraduates at the Pyongyang University of Science and Technology. In the course of life in Pyongyang, I've been able to observe the growing prevalence of mobile technology, and get a firsthand look at the state of consumer technology in the country.

In this talk I'll provide a demonstration of redstar 3.0, the current generation of the desktop operating system, and offer the caveat that it is seldom used in practice. I will also bring a samjiyong android tablet, to demonstrate the state of mobile technology. I'll focus the talk on discussing what international technology is and isn't applicable to the country, and the opportunities going forwards.</description>

<persons>

<person id="4821">Will Scott</person>

</persons>

<links>

<link href="https://www.reddit.com/r/IAmA/comments/1ucl11/iama\_american\_who\_spent\_the\_fall\_teaching/">Reddit AMA from first trip</link>

</links>

</event>

<event guid="SNW-UDgMBlqvbRHVTwhxpg" id="6299">

<date>2014-12-29T22:00:00+01:00</date>

<start>22:00</start>

<duration>00:30</duration>

<room>Saal 2</room>

<slug>31c3\_-\_6299\_-\_en\_-\_saal\_2\_-\_201412292200\_-\_trackography\_-\_maria\_xynou\_-\_claudio\_vecna</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Trackography</title>

<subtitle>You never read alone</subtitle>

<track>Ethics, Society &amp; Politics</track>

<type>lecture</type>

<language>en</language>

<abstract>Have you ever wondered who is watching while you are reading your favourite media online?

Whether we are reading the Guardian, the New York Times, the Hindu or any other news website, third party trackers are collecting data about our online behaviour.

This lecture will present Tactical Tech's new project, Trackography, which shows that we are all part of a global tracking business. </abstract>

<description>When we access websites, third parties are able to track our online behaviour, aggregate our data, link it to other data collected about us and subsequently create profiles. These profiles tell a story about us – which may or may not be true - and can include our political beliefs, gender, sexual orientation, economic status, habits, interests, affiliations and much more.

And while this might all appear to be harmless, we largely have very little control over how and when our data is collected, how our profiles are created, whether they are accurate, who they are subsequently shared with, who has access to them, what they are used for, where they are stored and for how long.

The global data industry has been very opaque... until now.

Trackography illustrates which companies track our data when we read the news online, which countries our data travels to and how our data is handled everytime we access a media website within a period of time.

We developed Trackography to increase transparency about the data collection industry. We hope it will start a discussion on unseen and unconsented data collection and on the politics of data.

Come to our lecture, learn about Trackography and help us track the trackers! </description>

<persons>

<person id="5037">Maria Xynou</person>

<person id="4912">Claudio ࿓ vecna</person>

</persons>

<links>

<link href="https://github.com/vecna/trackmap">Trackography project on github</link>

</links>

</event>

<event guid="ejFaY7sUr4WTs1tajM9JOQ" id="6462">

<date>2014-12-29T22:45:00+01:00</date>

<start>22:45</start>

<duration>00:30</duration>

<room>Saal 2</room>

<slug>31c3\_-\_6462\_-\_en\_-\_saal\_2\_-\_201412292245\_-\_megacode\_to\_facility\_gates\_-\_kevin\_redon</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>MegaCode to facility gates</title>

<subtitle/>

<track>Hardware &amp; Making</track>

<type>lecture</type>

<language>en</language>

<abstract>How do garage gate remotes work?

It turns out the ones from MegaCode simply send a individual fixed code.

And with little efforts if was possibly to clone them, send arbitrary codes, and record them all.</abstract>

<description>Garage gate remotes are not particularly well known for their security. And cloning them generally isn't a difficult task.

The MegaCode system from Linear LLC is no exception to it.

It did not take long to find out each remote sends a unique but fixed code over the radio interface. The rest was straight forward: record the signal using a Software Defined Radio, decode the signal, modify another remote to send this code, modify a receiver to collect even more codes, and record even more codes.

In this talk I will show how this simple system was reverse engineered. If you always wanted to play with software defined radio, electronics, micro-controllers, or solder components but you had no idea where to start, or thought that it would be to complicated because these are unknown grounds, this should motivate you. The tools and techniques are accessible for newcomers and should motivate you to also start playing with hardware.

</description>

<persons>

<person id="5126">Kévin Redon</person>

</persons>

<links/>

</event>

<event guid="z84bCyzZ-xiYlyM83L5dig" id="6455">

<date>2014-12-29T23:30:00+01:00</date>

<start>23:30</start>

<duration>00:30</duration>

<room>Saal 2</room>

<slug>31c3\_-\_6455\_-\_de\_-\_saal\_2\_-\_201412292330\_-\_snowden\_effect\_vs\_privacy\_paradox\_-\_matthias\_herz\_-\_michael\_johann</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Snowden Effect vs. Privacy Paradox</title>

<subtitle>Einstellungen und Internetnutzungsverhalten im Kontext des NSA-Skandals am Beispiel von Facebook</subtitle>

<track>Ethics, Society &amp; Politics</track>

<type>lecture</type>

<language>de</language>

<abstract>&quot;Vertrauen ist gut - Kontrolle ist besser.&quot; Dieses Idiom gilt mehr denn je, sofern man die Aktivitäten von Geheimdiensten bewerten mag. Wie seit einiger Zeit bekannt ist, ist die Mär der massenhaften Überwachung des Einzelnen Realität. Ob und inwieweit dies Auswirkungen auf die Realität des Einzelnen hat, steht im Fokus der vorliegenden Studie.</abstract>

<description>Der NSA-Skandal hat gerade in der jüngeren Vergangenheit gezeigt, dass konkrete Einstellungen zu Überwachung, Internetnutzung und Datensicherheit globale Themen sind, die gerade im Lichte der Enthüllungen Edward Snowdens vielfach eine Neubewertung erfahren. Aktuelle Studien zeigen, dass der NSA-Skandal die Einstellung von Internetnutzern zu diesen Themen, insbesondere in den Bereichen Online-Shopping, Cloud-Computing, E-Government und Sozialen Online-Netzwerken verändert hat. (BITKOM, 2013; Fittkau &amp; Maaß, 2013; Fritz, 2013; Krempl, 2013; Wilkens, 2013).

Die vorliegende Studie nutzt ein Multimethoden-Design, um Einstellungen hierzu und um das Nutzungsverhalten von Facebook-Nutzern zu analysieren. Dabei stehen u.a. generationale Effekte und unterschiedliche Nutzertypen im Fokus. Ziel der Studie ist es zu ermitteln, ob mit zunehmendem Wissen über Überwachungspraktiken eine Veränderung des Nutzungsverhaltens in Sozialen Online-Netzwerken einhergeht, oder: Ob gegenwärtig der Snowden-Effekt oder die Manifestation des Privacy Paradox zu beobachten ist. </description>

<persons>

<person id="4711">Matthias Herz</person>

<person id="5357">Michael Johann</person>

</persons>

<links/>

</event>

</room>

<room name="Saal G">

<event guid="hl9yD87mkTYvOY5J2BIQwQ" id="6332">

<date>2014-12-29T11:30:00+01:00</date>

<start>11:30</start>

<duration>01:00</duration>

<room>Saal G</room>

<slug>31c3\_-\_6332\_-\_en\_-\_saal\_g\_-\_201412291130\_-\_security\_analysis\_of\_a\_full-body\_x-ray\_scanner\_-\_eric\_wustrow\_-\_hovav\_shacham</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Security Analysis of a Full-Body X-Ray Scanner</title>

<subtitle/>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>Full-body scanners, also known as &quot;naked scanners&quot;, are used in airports and other government facilities to detect metallic and nonmetallic objects hidden beneath people's clothes. In many countries, they play a critical part in airline security, but they have also been criticized for being unsafe, ineffective, and an invasion of privacy. To shed scientific lights on these questions, we conducted the first rigorous, independent security evaluation of such a system. We bought a government-surplus Rapiscan Secure 1000 full-body scanner on eBay and extensively tested it in our lab. We found that it's possible to conceal knives, guns, and explosives from detection by exploiting properties of the device's backscatter X-ray technology. We also investigated computer security threats: malicious software and hardware that can compromise the effectiveness, safety, and privacy of the machine. In this talk, we'll explain how full-body scanners work, describe the results of our experiments, and draw lessons to inform transportation security, embedded systems security, and the public debate over secretive and privacy invasive government technologies.</abstract>

<description>In response to evolving terrorist threats, including non-metallic explosive devices and weapons, the U.S. TSA has adopted full-body scanners as the primary passenger screening method at nearly 160 airports nationwide at a cost exceeding $1 billion. Although full-body scanners play a critical role in transportation security, they have generated considerable controversy, including claims that the devices are unsafe, violate privacy and civil liberties, and are

ineffective. Furthermore, these scanners are complex embedded systems that raise important computer security questions.

Despite such concerns, neither the manufacturers nor the government have disclosed enough technical details to allow for rigorous independent evaluation, on the grounds that such information could benefit attackers, or is a trade secret. To help advance the public debate, we purchased a government-surplus Rapiscan Secure 1000 full-body scanner and performed a detailed security evaluation of its hardware and software.

We tested the Secure 1000's effectiveness by experimenting with different methods of concealing contraband. While the device performs well against naive attackers, fundamental limitations of its backscatter X-ray technology allow more clever attackers to defeat it. We show that an adaptive adversary can confidently smuggle contraband past the scanner by carefully arranging it on his body, obscuring it with other materials, or properly shaping it. Using these techniques, we are able to hide firearms, knives, plastic explosive simulants, and detonators in our tests. These attacks suggest a failure on the part of the Secure 1000's designers and the TSA to think adversarially.

We also evaluated the security of the Secure 1000 as a cyberphysical system. We show how malware infecting the operator's console could selectively render contraband invisible to screeners. We also attempt (with limited success) to use software-based attacks to bypass the scanner's safety interlocks and deliver an elevated X-ray radiation dose. Lastly, we show how an external device carried by an attacker can capture naked images of the subject being scanned.

Our results suggest that the Secure 1000 is not able to guarantee effectiveness or privacy against attackers who are knowledgeable about its inner workings, and that such knowledge is easy to obtain for an attacker with modest resources. We believe this study reinforces the message that security systems must be subjected to testing that is rigorous, adversarial, and public before they can be deemed safe for critical applications.

Warning: Nudity. We plan to show unmodified scanner images in order to demonstrate the privacy implications of full-body scanning.

</description>

<persons>

<person id="5283">Eric Wustrow</person>

<person id="5336">Hovav Shacham</person>

</persons>

<links>

<link href="https://radsec.org">Website about our study</link>

<link href="https://www.radsec.org/paper.html">Full research paper</link>

</links>

</event>

<event guid="e46101e6-3114-4d5a-a09a-c70d4bfb4fec" id="6579">

<date>2014-12-29T12:45:00+01:00</date>

<start>12:45</start>

<duration>02:15</duration>

<room>Saal G</room>

<slug>31c3\_-\_6579\_-\_en\_-\_saal\_g\_-\_201412291245\_-\_lightning\_talks\_day\_3\_-\_theresa</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Lightning Talks Day 3</title>

<subtitle/>

<track>Other</track>

<type>lecture</type>

<language>en</language>

<abstract>Lightning Talks are short lectures (almost) any congress participant may give! Bring your infectious enthusiasm to an audience with a short attention span! Discuss a program, system or technique! Pitch your projects and ideas or try to rally a crew of people to your party or assembly! Whatever you bring, make it quick!</abstract>

<description/>

<persons>

<person id="5269">Theresa</person>

</persons>

<links>

<link href="https://events.ccc.de/congress/2014/wiki/Static:Lightning\_Talks">31C3 Wiki: Lightning Talks</link>

</links>

</event>

<event guid="5gpaE5FLmfxMjTlbSDJkWw" id="6137">

<date>2014-12-29T16:00:00+01:00</date>

<start>16:00</start>

<duration>01:00</duration>

<room>Saal G</room>

<slug>31c3\_-\_6137\_-\_en\_-\_saal\_g\_-\_201412291600\_-\_caesar\_and\_norx\_-\_philipp\_jovanovic\_-\_aumasson</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>CAESAR and NORX</title>

<subtitle>Developing the Future of Authenticated Encryption</subtitle>

<track>Science</track>

<type>lecture</type>

<language>en</language>

<abstract>&quot;Nearly all of the symmetric encryption modes you learned about in school, textbooks, and Wikipedia are (potentially) insecure.&quot; -- Matthew Green

In recent history, we saw time and again (to some extent catastrophic) failures of cryptographic constructions for authenticated encryption (AE) due to bad design choices, implementation errors and a lack of reliable standards. After an introduction providing some background information on these topics, we present CAESAR, a new cryptographic competition which aims to find solutions to the problems mentioned above. In the second part of the talk, we introduce NORX, a new and next-generation AE scheme and our candidate for CAESAR.</abstract>

<description>&lt;div style=&quot;width:600px&quot;&gt;

&lt;p&gt;&lt;strong&gt;CAESAR&lt;/strong&gt; is the &lt;strong&gt;C&lt;/strong&gt;ompetition for &lt;strong&gt;A&lt;/strong&gt;uthenticated &lt;strong&gt;E&lt;/strong&gt;ncryption: &lt;strong&gt;S&lt;/strong&gt;ecurity, &lt;strong&gt;A&lt;/strong&gt;pplicapility, and

&lt;strong&gt;R&lt;/strong&gt;obustness, and the latest crypto contest after AES, eSTREAM, SHA-3, and PHC. CAESAR aims to identify a portfolio of authenticated encryption (AE) schemes with support for associated data (AD). Compared to ciphers like AES-CBC or Salsa20, protects not only confidentiality, but also authenticity and integrity of the processed data. Before we give an introduction to CAESAR, we present the motivations behind the competition, like the importance to protect in-transit data, a lack of reliable AE(AD) standards or the repeated crypto failures in recent history that led, for example, to the cracking of WEP (aircrackng), and to attacks on (D)TLS, like BEAST and Lucky13.&lt;/p&gt;

&lt;p&gt;In the second part, we talk about &lt;strong&gt;NORX&lt;/strong&gt;, our CAESAR candidate: NORX is a user-oriented cipher, engineered to take advantage of modern CPUs and to scale to different levels of parallelism. NORX relies on trusted building blocks, adapted to meet our design goals:

&lt;ul&gt;

&lt;li&gt;the sponge construction (as used in Keccak/SHA-3) is tuned to provide parallel processing&lt;/li&gt;

&lt;li&gt;the core of NORX is inspired by the ciphers Salsa20 and ChaCha (by DJB), and the hash function BLAKE(2) (by Aumasson et al.)&lt;/li&gt;

&lt;/ul&gt;

We explain how we selected NORX's operations and parameters to achieve maximized security and efficiency in both soft- and hardware. We also report on detailed benchmark results showing that NORX is among the fastest CAESAR candidates on various platforms, from ARM and x86 to ASICs. For example, on Intel's Haswell microarchitecture, NORX achieves 2.51 cycles per byte (more than 1 gigabyte per second), exploiting local parallelism provided by AVX2 instructions.&lt;/p&gt;

&lt;/div&gt;</description>

<persons>

<person id="4745">Philipp Jovanovic</person>

<person id="3622">aumasson</person>

</persons>

<links>

<link href="https://norx.io/">Official website of NORX</link>

<link href="https://github.com/norx/NORX">NORX on GitHub</link>

<link href="http://competitions.cr.yp.to/caesar.html">CAESAR</link>

</links>

</event>

<event guid="xnYRHWIRybr3subP-h\_1Wg" id="6173">

<date>2014-12-29T17:15:00+01:00</date>

<start>17:15</start>

<duration>01:00</duration>

<room>Saal G</room>

<slug>31c3\_-\_6173\_-\_en\_-\_saal\_g\_-\_201412291715\_-\_source\_code\_and\_cross-domain\_authorship\_attribution\_-\_aylin\_-\_greenie\_-\_rebekah\_overdorf</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Source Code and Cross-Domain Authorship Attribution</title>

<subtitle>The Role of Stylometry in Privacy</subtitle>

<track>Science</track>

<type>lecture</type>

<language>en</language>

<abstract>Stylometry is the study of linguistic style found in text. Stylometry existed long before computers but now the field is dominated by artificial intelligence techniques.

Writing style is a marker of identity that can be found in a document through linguistic information to perform authorship recognition. Authorship recognition is a threat to anonymity but knowing ways to identify authors provides methods for anonymizing authors as well. Even basic stylometry systems reach high accuracy in classifying authors correctly. Stylometry can also be used in source code to identify the author of a program. In this talk, we investigate methods to de-anonymize source code authors of C++ and authors across different domains. Source code authorship attribution could provide proof of authorship in court, automate the process of finding a cyber criminal from the source code left in an infected system, or aid in resolving copyright, copyleft and plagiarism issues in the programming fields. Programmers can obfuscate their variable or function names, but not the structures they subconsciously prefer to use or their favorite increment operators. Following this intuition, we create a new feature set that reflects coding style from properties derived from abstract syntax trees. We reach 99% accuracy in attributing 36 authors each with ten files. We experiment with many different sized datasets leading to high true positive rates. Such a unique representation of coding style has not been used as a machine learning feature to attribute authors and therefore this is a valuable contribution to the field.

We also examine the need for cross-domain stylometry, where the documents of known authorship and the documents in question are written in different contexts. Specifically, we look at blogs, Twitter feeds, and Reddit comments. While traditional methods in stylometry that work well within one domain fail to identify authors across domains, we are able to improve the accuracy of cross-domain stylometry to as high as 80%. Being able to identify authors across domains facilitates linking identities across the Internet making this a key privacy concern; users can take other measures to ensure their anonymity, but due to their unique writing style, they may not be as anonymous as they believe. </abstract>

<description>Anonymity is a topic researched in detail at the Privacy, Security, and Automation Lab at Drexel University. We study how to effectively identify the author of text with unknown authors and how to anonymize text of known authorship. In our previous talks at CCC, we have presented methods to identify authors of regular text, translated text and users a.k.a cyber-criminals of online underground forums. We introduced our authorship anonymization framework ‘Anonymouth’. Many times, we received questions on how applying de-anonymization techniques would work on source code and different domains. In this year’s talk, we will focus on identifying the authors of source code and cross-domain stylometry.

Can the authors of source code be identified automatically through features of their programming style? Do they leave coding “footprints”? Holding important implications for protecting intellectual property as well as for identifying malware authors and tracking how malware spreads and evolves, this question spurred a cross-cutting research project involving NLP and machine learning. Code stylometry requires features unique to coding and to the programming language. Source code has different properties than common writing, such as the lineage, keywords, comments, the way functions and variables are created, and the grammar of the program.

Aware that methods from text analytics can strengthen cyber analytics, this project sought to advance the potential of automated linguistic-type analysis, or stylometry, for authorship attribution of source code. A corpus of tens of thousands of users was built by scraping Google Code Jam Competition dataset. Specifically investigated were new ways of representing coding style through NLP-inspired syntactic, lexical and layout features. Random forests with 300 hundred trees were used along with less than ten decision features per tree. The main dataset had 173 authors each with six source code files with less then 100 lines of C++ code. A series of experiments was performed to discover the feature set that yielded the highest recognition accuracy: 91%. 57% of the features with information gain were syntactic and the rest were lexical and layout features. Tests on a validation dataset of exact same size showed 86% accuracy with the same features. The features that had information gain in the validation experiments all had information gain in the original dataset, which shows that the method and feature set are robust and abstract syntax trees show best promise.

Source code is just one domain studied in authorship attribution. We also study the problem of domain adaption in stylometry. Can we identify the author of an anonymous blog from a suspect group of Twitter accounts? The ability to do so would lead to the ability to link accounts and identities across the Internet. We can achieve high accuracy at identifying authors of documents within the same domain, including blogs, Twitter feeds, and Reddit comments, even when classifying with up to 200 authors. Identifying the author of a group of tweets from among 200 tweeters yields an accuracy of 94% and identifying the author of a blog entry from among 200 bloggers yields an accuracy of 71%. When we try to identify to author of a collection of tweets based on a collection of blogs from 200 authors, however, accuracy drops to 7% using the same method and features.

We are able to increase the accuracy, however, by applying an augmented version of doppelganger finder, a stylometric approach for multiple account detection that can handle small stylistic changes. This provides significant improvements in each of the cross-domain cases.

Advances in authorship attribution offer both positive and negative repercussions for security. However, it is important to understand the assumptions that underlie these results. Blind application of stylometric methods could be dangerous if the domain is not understood. This work shows that stylometric methods are domain dependent. Whether used defensively or offensively, this is certain to impact user account security. </description>

<persons>

<person id="3596">Aylin</person>

<person id="2101">greenie</person>

<person id="5302">Rebekah Overdorf</person>

</persons>

<links/>

</event>

<event guid="0hwHwiTLCTkE94bpOBOcVg" id="6547">

<date>2014-12-29T18:30:00+01:00</date>

<start>18:30</start>

<duration>01:00</duration>

<room>Saal G</room>

<slug>31c3\_-\_6547\_-\_en\_-\_saal\_g\_-\_201412291830\_-\_exploit\_in\_theater\_-\_cyphunk\_nathan\_fain</slug>

<recording>

<license>CC-BY-3.0</license>

<optout>false</optout>

</recording>

<title>&quot;Exploit&quot; in theater</title>

<subtitle>post-existentialism is the question, not post-privacy</subtitle>

<track>Art &amp; Culture</track>

<type>lecture</type>

<language>en</language>

<abstract>3 theater projects that illustrate the false &quot;California Ideology&quot; and ask us to look at our slip into neoliberalism through the backdoor of technology and to consider the ethics in the protocol. </abstract>

<description>We are moving the responsibility for the construction of social behaviour and good citizenry from the hands of policy makers to the hands of engineers. Trading spaces of the commons for those of market will. And the architects (standards bodies) are hardly concerned. Followers of the &quot;California Ideology&quot; present as their argument fluid consensus, provided through technology, as a reason to trust this neoliberal future. I will present 3 collaborations in theater that I feel question this ideology.

&lt;ul&gt;

&lt;li&gt;&lt;a href=&quot;http://www.politikimfreientheater.de/anonymus-p/&quot;&gt;Anonymous-P&lt;/a&gt; (with Chris Kondek &amp; Christiane Kühl)&lt;br&gt;

The question is &quot;post-existentialism&quot; not &quot;post-privacy&quot;&lt;/li&gt;

&lt;li&gt;&lt;a href=&quot;http://www.rimini-protokoll.de/website/en/project\_5194.html&quot;&gt;Hermann's Battle&lt;/a&gt; (with Rimini Protokoll)&lt;br&gt;

Cypherpunks, Heinrich von Kleist, &quot;Absolute Democracy&quot;&lt;/li&gt;

&lt;li&gt;&lt;a href=&quot;http://14.diskursfestival.de/?p=179&quot;&gt;Right of Might&lt;/a&gt; (self &amp; Maria Rößler)&lt;br&gt;

Competitive Assassination Markets (e.g. Assange v. Assad)&lt;/li&gt;

&lt;/ul&gt;</description>

<persons>

<person id="2682">cyphunk / nathan fain</person>

</persons>

<links>

<link href="https://vimeo.com/99041398">Anonymous-P trailer</link>

<link href="http://www.politikimfreientheater.de/anonymus-p/">Anonymous-P description @ festival Politik im Freien Theater </link>

</links>

</event>

<event guid="wyL8OVhv0Y6VczeYR3K\_jQ" id="6402">

<date>2014-12-29T20:30:00+01:00</date>

<start>20:30</start>

<duration>00:30</duration>

<room>Saal G</room>

<slug>31c3\_-\_6402\_-\_en\_-\_saal\_g\_-\_201412292030\_-\_axoloti\_-\_johannes\_taelman</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Axoloti</title>

<subtitle>DIY audio signal processing</subtitle>

<track>Hardware &amp; Making</track>

<type>lecture</type>

<language>en</language>

<abstract>Axoloti is an integrated platform for digital audio: its graphical editor is an easy-to-use toolbox for creating sound synthesis or processing algorithms. The audio processing runs on a microcontroller board, and runs standalone after editing. </abstract>

<description>Axoloti creates compilable c++ code from a graphical network of objects and connections, and automates the compilation, upload and execution of the resulting code on the target hardware. While running, parameters (presented as controls on objects in the document) can be tweaked from the host computer, and variables are read back (presented as numbers, virtual LEDs, graphs...) on the objects, in real time.

The Axoloti hardware has standard audio and MIDI in- and output, but also general purpose I/O, enabling easy development of custom &quot;new&quot; musical instruments.</description>

<persons>

<person id="4203">Johannes Taelman</person>

</persons>

<links>

<link href="www.axoloti.be">Axoloti</link>

</links>

</event>

<event guid="aowmh\_BVhxN\_YNmkQomweQ" id="6460">

<date>2014-12-29T21:15:00+01:00</date>

<start>21:15</start>

<duration>00:30</duration>

<room>Saal G</room>

<slug>31c3\_-\_6460\_-\_en\_-\_saal\_g\_-\_201412292115\_-\_eye\_wear\_computing\_-\_kai\_kunze</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Eye Wear Computing</title>

<subtitle>Augmenting the Human Mind</subtitle>

<track>Science</track>

<type>lecture</type>

<language>en</language>

<abstract>The talk gives an overview about the emerging field of smart glasses and how they can be used to augment our mind (e.g. how to improve our brain with technology). The talk will focus mostly on how to quantify cognitive tasks in real world environments. I also present a first application scenarios on how to use smart eyewear (e.g. google glass or JINS MEME) for short term memory augmentation and cognitive activity recognition.

</abstract>

<description>Considering the last centuries, major scientific breakthroughs aimed at overcoming our pyhsical limitations (faster transportation, higher buildings,

longer, more comfortable lifes).

Yet, I believe the coming big scientific

breakthroughs will focus on

overcoming our cognitive limitations.

Smart glasses can play a vital role in

1. understanding our cognitive actions and limitations

by quantifying them

2. helping us design interventions to improve our mind.

The talk will focus mostly on the first point,

what kind of cognitve tasks can we track already

with the smart glasses that are available in the

market and what will happen in the near future.

I will discuss application examples for

Google Glass and J!NS MEME. J!NS MEME is the first consumer level device measuring eye movements using electrodes also called Electrooculography (EOG). The MEME glasses not a general computing platform. They can only stream sensor data to a computer (e.g. smart phone, laptop, desktop) using Bluetooth LE. Sensor data includes vertical and horizontal EOG channels and accelerometer + gyroscope data. The runtime of the device is 8 hours enabling long term recording and, more important, long term real-time streaming of eye and head movement. They are unobtrusive and look mostly like normal glasses.

For Google Glass I present an open sensor-logging platform (including the infrared sensor to count eye blinks) and a fast interface to do lifelogging.

We will discuss which eye movements correlate with

brain functions and how this fact can be used

to estimate the cognitive task a user is performing,

from fatigue detection, over reading segmentation

to cognitive workload and the advances to track attention and concentration. Challenges discussed in the talk include how to get ground truth and how to evaluate performance in general.

</description>

<persons>

<person id="1891">Kai Kunze</person>

</persons>

<links>

<link href="https://www.jins-jp.com/jinsmeme/en/">J!NS MEME</link>

<link href="http://kaikunze.de/posts/google-glass-for-eldery/">Google Glass applications for Elderly</link>

<link href="http://www.dagstuhl.de/wiki/index.php?title=14362">Dagstuhl Seminar on Augmenting Human Memory</link>

</links>

</event>

<event guid="7dt2PzyGxZI8i0QQysCZ6Q" id="6554">

<date>2014-12-29T22:00:00+01:00</date>

<start>22:00</start>

<duration>00:30</duration>

<room>Saal G</room>

<slug>31c3\_-\_6554\_-\_en\_-\_saal\_g\_-\_201412292200\_-\_automatically\_subtitling\_the\_c3\_-\_timobaumann\_-\_arne\_kohn</slug>

<recording>

<license>CC-BY-3.0</license>

<optout>false</optout>

</recording>

<title>Automatically Subtitling the C3</title>

<subtitle>How speech processing helps the CCC subtitle project, and vice-versa.</subtitle>

<track>Science</track>

<type>lecture</type>

<language>en</language>

<abstract>Transcribing a talk comes relatively easy to fast typists, whereas turning a transcript into time-aligned subtitles for a video requires a much larger human effort. In contrast, speech recognition performance (especially for open-source-based solutions), is still poor on open-domain topics, but speech technology is able to align a given text to the corresponding speech with high accuracy. Let's join forces to generate superior subtitling with little effort, and to improve future open-source-based speech recognizers, at the same time!

</abstract>

<description>We present the ongoing work of an student project in informatics at Universität Hamburg in which we combine the strengths of human transcription performance and automatic alignment of these transcriptions to produce high quality video subtitles.

We believe that our work can help the C3 community in generating video subtitles with less manual effort, and we hope to provide subtitles for all 31C3 talks (as long as you provide the transcriptions).

However, we're not just a service provider to the C3. There is a shortage of training material for free and open-source speech recognizers and the acoustic models they employ. Thus, we plan to prepare an aligned audio corpus of C3 talks which will help to advance open-source speech recognition.

Be a part of this by helping us with your transcriptions -- we'll repay with subtitlings and better open-source speech recognition in the future!</description>

<persons>

<person id="5226">timobaumann</person>

<person id="5360">Arne Köhn</person>

</persons>

<links>

<link href="http://nats-www.informatik.uni-hamburg.de/ProSub1415/">Project Homepage</link>

<link href="https://bitbucket.org/natsuhh/prosub/">Source Repository</link>

</links>

</event>

<event guid="n2e6vsWynbgJeu2GC6FpnA" id="6385">

<date>2014-12-29T22:45:00+01:00</date>

<start>22:45</start>

<duration>00:30</duration>

<room>Saal G</room>

<slug>31c3\_-\_6385\_-\_en\_-\_saal\_g\_-\_201412292245\_-\_the\_machine\_to\_be\_another\_-\_beanotherlab</slug>

<recording>

<license>CC attribution non-commercial share-alike.</license>

<optout>false</optout>

</recording>

<title>The Machine To Be Another</title>

<subtitle>Exploring identity and empathy through neuroscience, embodiment, VR and storytelling</subtitle>

<track>Art &amp; Culture</track>

<type>lecture</type>

<language>en</language>

<abstract>The Machine To Be Another is an open-source interactive system designed to explore the relationship between identity and empathy through interdisciplinary performance-experiments drawing from neuroscience, VR, storytelling and art. Through research collaborations we have been developing applications in contexts of conflict resolution, the arts and healthcare.</abstract>

<description>Imagine the possibility of creating stories that can be felt through the audience's own body as something real. For example, what would it mean for the world if citizens from opposite sides of a war could swap bodies and feel what it is like to be part of the family of their own enemy? What if every school child could experience, in full immersion, the life of another young person half way around the world? How would this impact our ability to share our pain, address the challenges we share, resolve conflicts and build empathy, or even improve our emotional resilience as individuals?

We developed a system that allows users to enter the body of a different person and inhabit each other’s experiences in a radically different way; a way of sharing that transports us to a place of preverbal, embodied empathy. The Machine to Be Another is a Creative Commons interactive system designed as a tool for embodied-immersive storytelling. We merge interaction protocols from neuroscience research in embodiment with performance, storytelling and virtual reality hardware to create in users the illusion of feeling themselves in the body of another person. Embodied simulation mechanisms, in particular of actions, emotions and corporeal sensations have been recently proposed as having deep implications in the understanding of empathy and social cognition, perception of one’s body, neural plasticity but also in the formation of concepts .For example, studies conducted by EventLab in Barcelona suggest the effectiveness of inducing body ownership for reducing implicit racial bias. This “body swap illusion” is so strong that a person can experience being in another’s body when facing her own body and shaking hands with “themselves”.

For two years we have been working with an extended community of researchers, artists, activists and members of the public to create performance-experiments related to the understanding of the other and the self. Through this processes we have explored issues such as mutual respect, immigration and physical disability bias, gender identity, conflict resolution, body extension and embodied dance performances.

</description>

<persons>

<person id="5000">BeAnotherLab</person>

</persons>

<links>

<link href="themachinetobeanother.org">The Machine To Be Another</link>

<link href="https://vimeo.com/89556173">Video</link>

</links>

</event>

<event guid="V\_yKfMGBUgnu6g90YF-iBA" id="6072">

<date>2014-12-29T23:30:00+01:00</date>

<start>23:30</start>

<duration>00:30</duration>

<room>Saal G</room>

<slug>31c3\_-\_6072\_-\_en\_-\_saal\_g\_-\_201412292330\_-\_higher-dimensional\_geometry\_and\_fractals\_-\_magnus</slug>

<recording>

<license>CC-BY-3.0</license>

<optout>false</optout>

</recording>

<title>Higher-Dimensional Geometry and Fractals</title>

<subtitle/>

<track>Science</track>

<type>lecture</type>

<language>en</language>

<abstract>Extending the common 3-space-to-2-space projections to 4D and higher and how certain types of fractals can be presented using these expansions. After that we'll have a closer look at Fractal Flames as used in Electric Sheep.</abstract>

<description>This talk will be split into 3 parts; first: extending the common 3D-to-2D projections - used by libraries such as OpenGL - to also allow projecting hypothetical 4D or higher constructs to a 2D screen.

Second: making pretty fractal pictures by rendering iterated function systems with affine transformations in 4D and higher. This part explains how the chaos game works and how to do an alternate, discrete render which works better in higher dimensions than 2D.

The third and final part takes a look at the Fractal Flames by Scott Draves, a different kind of iterated function system used in the Electric Sheep screen saver. The original algorithm for this is inherently 2D, but parts of it can be extended to higher dimensions, producing interesting results.

Due to time constraints, it is assumed that the audience is already roughly familiar with - or willing to believe in - the general method for 3D projections, including vector and matrix maths. There will also be pretty pictures.

The presentation will have live demo segments mixed in, which make use of a F/OSS 4D+ primitive and fractal renderer called &quot;Topologic&quot; (see links, below).</description>

<persons>

<person id="4892">Magnus</person>

</persons>

<links>

<link href="https://ef.gy/31c3">Slides (Preliminary)</link>

<link href="https://github.com/ef-gy/topologic">Topologic</link>

</links>

</event>

</room>

<room name="Saal 6">

<event guid="nH8WWBIPmElTIWVCbrjcrg" id="6158">

<date>2014-12-29T11:30:00+01:00</date>

<start>11:30</start>

<duration>01:00</duration>

<room>Saal 6</room>

<slug>31c3\_-\_6158\_-\_en\_-\_saal\_6\_-\_201412291130\_-\_why\_do\_we\_need\_an\_open\_food\_information\_platform\_-\_alexis</slug>

<recording>

<license>cc-by-sa</license>

<optout>false</optout>

</recording>

<title>Why do we need an open food information platform</title>

<subtitle>We want all data about food to be linked and public</subtitle>

<track>Hardware &amp; Making</track>

<type>lecture</type>

<language>en</language>

<abstract>We from EveryCook are building an open source computerized cooking device. At 29c3 I presented the idea of digital cooking and people gave me an awesome feedback. Now, 2 years later the industry giants have realised that connecting computers and kitchen devices can do awesome things. But do they create open standards? Of course not! They create little black boxes speaking strange languages that you can't integrate in an ecosystem that wasn't designed by the manufacturers themselves. We still want an open ecosystem for free exchange of information about food and recipes. We came closer to our goal. Let me tell you...</abstract>

<description>There are bluetooth thermometers for meat. Can I use them with my computer? Nope, because they only talk to one dedicated app.

There are cooking devices with touch screen, built-in recipes and sometimes even networking capabilities. But do we know how to talk to them?

We seem to be the only ones believing in the power of open standards. EveryCook is open source since the beginnings. Because we look at the large picture. We want to use ALL available data for cooking. Even data from WWF about sustainability or data from scientific research about nutrients.

And we want to show how we treat this data. We want our database open for all useful input.

As we do for our Hardware. If you see a weak part in our designs you can tell us and we'll change it if needed.

I will tell you what we learned making 4 generations of digital cooking devices. And I would like to explain you why we believe that there should be open standards for cooking software.

What is now done &quot;in the market&quot; is that many companies develop many, many apps and some kitchen devices and none of them is made to interact with it's neighbors. Why? &quot;because my data is my data!&quot; and &quot;my hardware design is mine!&quot;

Isn't that a huge waste of resources? Everyone re-inventing the wheel and then adding some little special sauce to claim the whole thing as &quot;unique&quot;.

Having all data about food available is not a need, it is a human right. Having additional data on how to prepare food in machine readable form is a nice extra. Having both together in a database is the technically best solution because of the many synergies.

Let's form the future of digital cooking before someone else does!</description>

<persons>

<person id="4986">Alexis</person>

</persons>

<links>

<link href="http://everycook.org/">EveryCook Website</link>

</links>

</event>

<event guid="SkWIxKKgQFunVQAJT\_oagA" id="6463">

<date>2014-12-29T12:45:00+01:00</date>

<start>12:45</start>

<duration>01:00</duration>

<room>Saal 6</room>

<slug>31c3\_-\_6463\_-\_en\_-\_saal\_6\_-\_201412291245\_-\_damn\_vulnerable\_chemical\_process\_-\_marmusha</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Damn Vulnerable Chemical Process</title>

<subtitle>Exploitation in a new media</subtitle>

<track>Hardware &amp; Making</track>

<type>lecture</type>

<language>en</language>

<abstract>So you want to author a next Stuxnet (or even cooler than that). Here is the success recipe: forget what you have known about cyber security. When an attack transitions from control of a digital system to control of a physical process, physics and time become controlling factors instead of the digital rules encoded into your microcontroller.

The holly CIA trinity is meaningless in the physical world. The uncontrollable but still running process is not really available; process dynamics does not stop simply because the controlling equipment is DoSed; electronically segregated components can still communicate over physical media (the process) and a physical phenomenon can be measured terribly wrongly (so that the wrong measurement will be proudly delivered to the digital application in a totally secure way). Where physics plays a governing role, IT security concepts are rendered useless.

Please welcome a new arrival in the &quot;damn&quot;-frameworks series - Damn Vulnerable Chemical Process. Come to the lecture and learn what it takes to exploit a physical process: how to find vulnerabilities and how to exploit them with minimal cost and maximum impact. Get astonished about the gazillion of uncertainties you will have to face on your way to disruptive goal and realize that the TIME is ONLY what matters while designing your attack .

Make sure to visit local library and refresh your knowledge on physics, chemistry, mechanics, control theory, signal processing and algorithms. The lecture will teach you how to apply this knowledge in the exciting world of cyber-physical exploitation.

</abstract>

<description>Attackers and researchers have shown numerous ways to compromise and control the digital systems involved in process control (plants, grids, cars). Little information is available what to actually do with those controls. A single bit flip can engage the burner under a tank of chemicals, but the reaction will still take hours to complete regardless of the state of the controller outputs. Changing the state of the outputs does not immediately put the process into a vulnerable state. An attacker needs to take into account the timing and state of the system and act when the process is in the vulnerable state.

Designing an attack on a cyber-physical systems leads to unconventional hacking and interesting computer science challenges. Thus, DoS attacks on controlls in the physical domain do not deny process dynamics. In fact, if timed wisely, DoS attack allow manipulation of the process at will. Whoever thinks that cryptography will safe the world is wrong. Due to the specifics of controll principles and their implementation in the equipment, DoS attacks allow manipulation of process controls even if the communication is authenticated.

On the example of the DoS attacks on controller inputs and outputs at the level of communication links the lecture will take the audience through all the stages and details of (i) designing and (ii) implementing such attacks to cause physical damage. The experiments are conducted on the realistic model of a chemical plant used in process engineering research.</description>

<persons>

<person id="4111">Marmusha</person>

</persons>

<links/>

</event>

<event guid="H1GEe9l64eUbo1oZXtLkEg" id="5930">

<date>2014-12-29T14:00:00+01:00</date>

<start>14:00</start>

<duration>01:00</duration>

<room>Saal 6</room>

<slug>31c3\_-\_5930\_-\_en\_-\_saal\_6\_-\_201412291400\_-\_funky\_file\_formats\_-\_ange\_albertini</slug>

<recording>

<license>CC-BY-3.0</license>

<optout>false</optout>

</recording>

<title>Funky File Formats</title>

<subtitle>Advanced binary tricks</subtitle>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>Binary tricks to evade identification, detection, to exploit encryption and hash collisions.</abstract>

<description>\* artistic binaries - why they are possible, how they work.

- quines

- polyglots &amp; chimeras

- schizophrenic

- AngeCryption

- hash collisions

\* challenges and failures</description>

<persons>

<person id="4585">Ange Albertini</person>

</persons>

<links/>

</event>

<event guid="vw7sldBf\_2ldlwNWTOF93A" id="6373">

<date>2014-12-29T16:00:00+01:00</date>

<start>16:00</start>

<duration>01:00</duration>

<room>Saal 6</room>

<slug>31c3\_-\_6373\_-\_en\_-\_saal\_6\_-\_201412291600\_-\_the\_only\_thing\_we\_know\_about\_cyberspace\_is\_that\_its\_640x480\_-\_olia\_lialina</slug>

<recording>

<license>CC-BY-3.0</license>

<optout>false</optout>

</recording>

<title>The Only Thing We Know About Cyberspace Is That Its 640x480</title>

<subtitle>One Terabyte of Kilobyte Age</subtitle>

<track>Art &amp; Culture</track>

<type>lecture</type>

<language>en</language>

<abstract>Since 10 years I write about Vernacular Web and Digital Folklore, about early days of the web and web design before it became a profession. It is not that easy to find pages that were made in 93-97 and are still online or look the same. Things changed in 2009, when Yahoo announced that they are closing Geocities, number one free hosting service of the last century, &quot;myspace of the 90es&quot;, first home for many web users and a jest for &quot;professional web&quot;

In half a year yahoo gave its users to copy their data, Archive Team managed to partly rescue the pages and release one terabyte torrent of it. In 2010 my partner Dragan Espenschied and I started to download the files. In the middle of 2011 Dragan restored the archive and we started to go through the profiles: collecting, tagging, comparing, analyzing. One Terabyte of Kilobyte Age project started.

We don't only collect and restore but bring this culture of the 90es back to the web, using contemporary infrastructure. It is http://oneterabyteofkilobyteage.tumblr.com/ that posts a screenshot of a page every 20 minutes since February 2013. Or my channel on Vine, that allows to see those pages animated and with sound. And of course the blog http://contemporary-home-computing.org/1tb/ where we describe the findings.

In my HIGHLY ILLUSTRATED talk I'd like to introduce to the audience pearls of the early web culture, going much deeper than usual Under Construction signs and animated GIFs nostalgia. Will show what did it mean to make a web page technically, philosophically and ideologically. Will also talk about our unique technical setting for emulating the pages and what digital preservation really means. And last but not least will talk about newer cases of deleted social networks and social services.</abstract>

<description/>

<persons>

<person id="3832">olia lialina</person>

</persons>

<links/>

</event>

<event guid="L9rFWciMu\_GVpHLIhPT9Qg" id="6381">

<date>2014-12-29T17:15:00+01:00</date>

<start>17:15</start>

<duration>01:00</duration>

<room>Saal 6</room>

<slug>31c3\_-\_6381\_-\_de\_-\_saal\_6\_-\_201412291715\_-\_die\_krise\_der\_bilder\_ist\_die\_krise\_der\_politik\_-\_mareike\_foecking</slug>

<recording>

<license>CC-BY-3.0</license>

<optout>false</optout>

</recording>

<title>Die Krise der Bilder ist die Krise der Politik</title>

<subtitle>Die Krise der Politik ist die Krise der Bilder</subtitle>

<track>Art &amp; Culture</track>

<type>lecture</type>

<language>de</language>

<abstract>Im Rahmen meiner Forschungsarbeit &quot;Das Bild im digitalen Wandel&quot; beschätige ich mich mit der Veränderung der Bilder im Rahmen der Veränderung der medialen Anwendung und Vermittlung von Bildern.

Darüber würde ich gerne sprechen.</abstract>

<description>Mit welchen Bildern wird die Zukunft beschrieben, mit welchen Bildern wird Wahlkampf gemacht, mit welchen Bildern werden Nachrichten vermittelt und visualisiert?

Bilder kommunizieren oft direkter als Texte und aus ihnen entstehen wiederum neue Bilder.

Inwieweit ist das Selfie ein gesellschaftliches Dispositiv, das zu einem kollektiv verordneten Handeln aufruft und Menschen vereinheitlicht?

Wieso gibt es für die Überwachung keine wirklichen Bilder und warum bedient Angela Merkel nicht nur ein Bild, sondern viele?

Inwieweit ist die Politik eine Inszenierung oder die Inszenierung selbst die Politik bezüglich der Bilder, mit denen sie kommuniziert?

In einer essayartigen Aneinanderreihung von visuellen Beispielen wird sich dieser Vortrag mit verschiedenen Fragen beschäftigen, die zum Teil beantwortet werden, zum Teil selbst wiederum neue Fragen stellen.</description>

<persons>

<person id="4177">Mareike Foecking</person>

</persons>

<links/>

</event>

<event guid="-fw4u4HgOtFUvdKnF7Xrbw" id="6124">

<date>2014-12-29T18:30:00+01:00</date>

<start>18:30</start>

<duration>01:00</duration>

<room>Saal 6</room>

<slug>31c3\_-\_6124\_-\_de\_-\_saal\_6\_-\_201412291830\_-\_es\_gibt\_viel\_zu\_tun\_-\_hau\_n\_wir\_ab\_-\_robert\_verch\_-\_eva\_olivin</slug>

<recording>

<license>CC-BY-3.0</license>

<optout>false</optout>

</recording>

<title>ES GIBT VIEL ZU TUN - HAU'N WIR AB.</title>

<subtitle>[Die Untersuchung]</subtitle>

<track>Art &amp; Culture</track>

<type>lecture</type>

<language>de</language>

<abstract>Eine Mietwohnung ist seit circa 20 Jahren verlassen, ihr Bewohner nicht auffindbar. Unveränderte Möblierung, Ausstattung und persönliche Hinterlassenschaften sind jedoch noch vorhanden und unberührt.

</abstract>

<description>Anhand dieser Situation verhandeln Besucher\*innen in einem künstlerisch-technischem Reallabor die Grenzen von Neugier und Voyeurismus. Ihr Verhalten wird für die Öffentlichkeit künstlerisch reflektiert und inszeniert. Auf dieser Grundlage wird die Frage nach der Möglichkeit empathischer Wahrnehmung über digitale Kanäle aufgeworfen und zur Diskussion gebracht.</description>

<persons>

<person id="4946">Robert Verch</person>

<person id="5326">Eva Olivin</person>

</persons>

<links>

<link href="http://dieuntersuchung.de">ES GIBT VIEL ZU TUN - HAU'N WIR AB.</link>

</links>

</event>

<event guid="lE9xGxC7-9DQGljZOWg\_Sw" id="6135">

<date>2014-12-29T20:30:00+01:00</date>

<start>20:30</start>

<duration>00:30</duration>

<room>Saal 6</room>

<slug>31c3\_-\_6135\_-\_en\_-\_saal\_6\_-\_201412292030\_-\_agri-tech\_and\_the\_arts\_from\_barns\_to\_d-space\_-\_richard\_marggraf\_turley</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Agri-tech and the Arts: From Barns to D-Space</title>

<subtitle/>

<track>Ethics, Society &amp; Politics</track>

<type>lecture</type>

<language>en</language>

<abstract>What do the arts and literature have to contribute to urgent debates about the technization of food production? What can a play from 1605 tell us about fairer distribution of natural resources today? Equally, how might a cyber thriller from 2011 help us debate contentious issues such as gene-based technologies and utopian visions of knowledge-led society? This talk considers agri-tech and food security across a wide sweep of social and political terrain, from the Arab Spring to the European horsemeat scandal, from Shakespeare to Daniel Suarez. It argues that the arts and sciences need to cooperate to deepen understanding about, and define actions on, the big challenges facing a needy world. Finally, it suggests ways in which the arts and technology can assist us in arriving at a model of society in which resources are distributed not only more efficiently, but also more equitably.</abstract>

<description>We are facing a crisis of food that threatens to overwhelm households, communities and even entire states. Inequality of access to sustenance has been exacerbated by soaring prices, corporate sharp practice and wide “food fraud” – including 2013’s UK horsemeat scandal, and Europol’s exposé of “fake” and “substandard” food in Europe in 2013-14. Riots and political unrest that appear to have little connection with food, on closer inspection turn out to have dimensions associated with sustenance. For example, the first shop to be looted in 2011’s London Uprising was not a branded trainers outlet or flat-screen TV centre, but the Clarence Convenience Store, raided for chocolate bars and bottled water. In its first moments, then, the unrest in Britain’s capital took the form of a traditional “food riot”. Similarly, the first wave of protest that gave rise to the Arab Spring was initiated by the self-immolation of a street vendor who made his living selling fruit and vegetables from a cart in Tunis. As a result of food-related political unrest, food security has risen on the agendas of governments and international agencies around the world.

Agri-tech has come to be regarded as the panacea to food constraint. MEP Julie Girling is not alone in arguing that “technological advancement will be the only way that we can meet the coming growth in demand”. Certainly, the technization of food production and distribution – advances in gene-based technologies, synthetic biology, agri-robots, remote sensing, agri-infomatics and just-in-time (JIT) algorithms – offers a compelling vision of knowledge-led development. However, as this talk argues, technology is only one part of the story. Until the quality of public engagement is improved around agri-tech, the nature of our food, where it comes from, and the conditions in which it is produced, programmes aimed at establishing a more equitable, ethical, sustainable future society worth living will be compromised. In this regard, the arts can open a shared spae of imagination.

This talk develops findings from my forthcoming interdisciplinary book, co-authored with literary scholar Dr Jayne Archer and plant scientist Professor Howard Thomas, Food and the Literary Imagination. Our argument is that vital, deep knowledge about food, technology and society is to be found in art and literature, both historical and contemporary. In this talk, I explore what art and literature, as heuristic media, can tell us about our relation to food technology, what they can contribute to global debates about the ethics and mechanics of food production, and their role in helping us to imagine a society in which resources are distributed not only more efficiently, but also more equitably.

Part 1 considers former systems consultant Daniel Suarez’s 2011 novel Freedom TM (German title, Darknet), popular among hacker communities for its kinetic scenes of “D-space” cyber combat. At the novel’s radical centre, however, is a vivid portrait of an utopian agricultural society founded on tech-led solutions to food supply. Suarez’s “darknet farms” of the future represent a serious intervention into the politics of C21 agri-tech and food security. In this respect, Freedom TM belongs to a long tradition of the arts exploring contemporary food politics, stretching back to include Shakespeare’s play King Lear (c. 1605), key sections of which are set – modern directors often forget – in a wheatfield, and John Constable’s The Hay Wain (1821), widely misunderstood as a themepark fantasy of rural life and the origins of food, regularly voted Britain’s “best loved” painting.

Part 2 discusses three projects in which I am involved, each aimed at improving public dialogue around food and food politics at local and regional levels: (1) a creative commons project, “Edible Wales” (funded by CEWN/AHRC); (2) the Welsh Govt/EU-funded “Food Engagement Wales”; and (3) a project being developed with a major UK supermarket to examine practical ways in which literature can be used to promote public understanding of food as we search for a sustainable, resilient, more equitable future society.</description>

<persons>

<person id="4951">Richard Marggraf Turley</person>

</persons>

<links>

<link href="http://www.palgrave.com/page/detail/food-and-the-literary-imagination-jayne-elisabeth-archer/?K=9781137406361">Food and the Literary Imagination</link>

<link href="http://richardmarggrafturley.weebly.com/blog">Richard Marggraf Turley blog</link>

<link href="http://www.historytoday.com/blog/2013/04/“making-famine-where-abundance-lies”-shakespeare-hoarder">History Today feature</link>

</links>

</event>

<event guid="35vPpFdywfzrf36\_zbn6zA" id="6543">

<date>2014-12-29T21:15:00+01:00</date>

<start>21:15</start>

<duration>02:15</duration>

<room>Saal 6</room>

<slug>31c3\_-\_6543\_-\_de\_-\_saal\_6\_-\_201412292115\_-\_the\_time\_is\_right\_-\_c-atre</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>The Time is Right</title>

<subtitle>Ein Science-Fiction-Theaterstück</subtitle>

<track>Entertainment</track>

<type>other</type>

<language>de</language>

<abstract>Das c-atre collectivdrama präsentiert THE TIME IS RIGHT, ein Science-Fiction-Theaterstück nach einer Idee von yetzt.

„Es geht um das große Ganze! Die Bewahrung von freiem Wissen, freier Kultur – ohne Copyright-Mafiosi, die jeden Pups, der dir entfleucht, lizenzieren wollen!“ (Jo)

Als die Aktivisten Mo und Jo bei einer ihrer geheim-gefährlichen Widerstandsaktionen gegen die drohende Allmacht der Verwertungsgesellschaften von dieser sonderbaren jungen Frau, die wie aus dem Nichts erscheint, überrascht werden, ahnt noch niemand, welche weitreichenden Folgen diese Begegnung im Kampf für die Kunst der Zukunft gehabt haben wird.</abstract>

<description>THE TIME IS RIGHT

Schauspieler/innen:

Carolin Meyer

Gero Nagel

Jens Ohlig

Josefine Matthey

Martine „authmillenon“ Lenders

Mirko „macro“ Fichtner

Pierre Pronchery

Sebastian „epunc“ Marg

Sigi Oepke

Merle von Wittich

Elisabeth Krüger

Carolina Rocha

Schauspielerische Leitung:

Josefine Matthey

Dramaturgie:

Carolin Meyer

Text:

das c-atre in Zusammenarbeit mit yetzt

Musik/Sound/Komposition:

Dirk Geier

Bühnenbild:

Peter Stoltz

Sebastian Marg

Kostüm:

das c-atre

Maske:

Vivien Pöltl

Technik:

Sven Wagner

UA: 03. Juli 2014, c-base Berlin</description>

<persons>

<person id="5262">c-atre</person>

</persons>

<links/>

</event>

</room>

</day>

<day date="2014-12-30" end="2014-12-31T04:00:00+01:00" index="4" start="2014-12-30T11:30:00+01:00">

<room name="Saal 1">

<event guid="6b94aab7-5909-4662-99f8-1a990c247bb1" id="6602">

<date>2014-12-30T11:30:00+01:00</date>

<start>11:30</start>

<duration>01:00</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6602\_-\_en\_-\_saal\_1\_-\_201412301130\_-\_the\_case\_of\_chelsea\_manning\_-\_alexa\_o\_brien\_-\_nancy\_hollander\_-\_ahmed\_ghappour\_-\_chase\_strangio</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>The case of Chelsea Manning</title>

<subtitle/>

<track>Ethics, Society &amp; Politics</track>

<type>lecture</type>

<language>en</language>

<abstract>A discussion with U.S. Army private Chelsea Manning's attorneys Nanny Hollander, Ahmed Ghappour, and Chase Strangio.

Moderated by journalist Alexa O'Brien.</abstract>

<description>In the Summer of 2013, Manning was convicted under the Espionage and Computer Fraud and Abuse Acts and sentenced to 35 years in prison for disclosing battlefield reports from the wars in Iraq and Afghanistan, Guantanamo prison camp detainee profiles, and U.S. diplomatic correspondence. She currently is imprisoned at the U.S. Disciplinary Barracks at Fort Leavenworth, Kansas.

During her pretrial confinement before her trial, the U.N. Special Rapporteur on Torture ruled Manning'treatment at Quantico Brig was cruel and unusual.

She is now suing the Department of Defense to provide adequate medical care for her gender dysphoria, which she was diagnoised with four years ago before her arrest by a U.S. Army doctor.

Manning is now appealing her conviction in the U.S. Army Court of Criminal Appeals.

This discussion will explain Manning's current situation and legal fights and how you can help this brave military whistleblower.</description>

<persons>

<person id="5303">Alexa O´Brien</person>

<person id="5304">Nancy Hollander</person>

<person id="5364">Ahmed Ghappour</person>

<person id="5366">Chase Strangio</person>

</persons>

<links/>

</event>

<event guid="ad722522-5817-4317-8f3d-bb443b4e6c77" id="6574">

<date>2014-12-30T12:45:00+01:00</date>

<start>12:45</start>

<duration>01:00</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6574\_-\_en\_-\_saal\_1\_-\_201412301245\_-\_why\_are\_computers\_so\_and\_what\_can\_we\_do\_about\_it\_-\_peter\_sewell</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Why are computers so @#!\*, and what can we do about it?</title>

<subtitle/>

<track>Science</track>

<type>lecture</type>

<language>en</language>

<abstract>Computers have become ubiquitous and essential, but they remain massively error-prone and insecure - as if we were back in the early days of the industrial revolution, with steam engines exploding left, right, and centre. Why is this, and can we do better? Is it science, engineering, craft, or bodgery?

I'll talk about attempts to mix better engineering methods from a cocktail of empiricism and logic, with examples from network protocols, programming languages, and (especially) the concurrency behaviour of programming languages and multiprocessors (from the ARMs in your phone to x86 and IBM Power servers), together with dealings with architects and language standards groups.

</abstract>

<description>For more details of the underlying research and the many people who have contributed, see: http://www.cl.cam.ac.uk/~pes20/

</description>

<persons>

<person id="5247">Peter Sewell</person>

</persons>

<links/>

</event>

<event guid="XGhOde-ujLyDS1gsvpebMg" id="6251">

<date>2014-12-30T14:00:00+01:00</date>

<start>14:00</start>

<duration>01:00</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6251\_-\_en\_-\_saal\_1\_-\_201412301400\_-\_state\_of\_the\_onion\_-\_jacob\_-\_arma</slug>

<recording>

<license>CC-BY-3.0</license>

<optout>false</optout>

</recording>

<title>State of the Onion</title>

<subtitle>Neuland</subtitle>

<track>Ethics, Society &amp; Politics</track>

<type>lecture</type>

<language>en</language>

<abstract>The current state of the Tor network and community, covering important updates, discussions of the ecosystem of software, and include a longer Q&amp;A than previous CCC talks!</abstract>

<description>The State of the Onion covers technical, social, economic, political and cultural issues pertaining to anonymity, the Tor Project and the ecosystem surrounding our communities.

Important topics include the following issues:

- XKEYSCORE rules

- The shift from 3 guards to 1 guard

- Blackhat / cert talk and responsible Tor research in general

- Russian funding for Tor research

- Heartbleed

- New hidden service R&amp;D funding

- Helping Internet services accept anonymous users

- Meek and new pluggable transports

- Tor Browser integration

- Tor and EFF Tor relay challenge

- OrFox

- Incentives to relay

- Spoiled onions paper amongst others

- A summary and fact checking of important media coverage

- Tor Weekly news

- Art and anonymity in culture</description>

<persons>

<person id="1083">Jacob</person>

<person id="1785">arma</person>

</persons>

<links/>

</event>

<event guid="TvC3Zh1wVU8NotOjslV57Q" id="6377">

<date>2014-12-30T16:00:00+01:00</date>

<start>16:00</start>

<duration>01:00</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6377\_-\_en\_-\_saal\_1\_-\_201412301600\_-\_paypals\_war\_on\_terror\_-\_the\_no\_-\_absolem</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Paypals War on Terror</title>

<subtitle>A Historical Re-Enactment of the PayPal14</subtitle>

<track>Ethics, Society &amp; Politics</track>

<type>podium</type>

<language>en</language>

<abstract>We are the PayPal 14. For the last several years we've been restricted in what we could or couldn't say about our court case. Our sentencing is on December 4th, ending the legal restrictions on what we can share about our story.</abstract>

<description>The panel will consist of four PayPal 14 defendants: Mercedes &quot;no&quot; Haefer, Josh &quot;Absolem&quot; &quot;t0x1c&quot; Covelli, and an unyet decided attorney.

We will be discussing the legal, political, and ethical issues surrounding the PayPal14 courtcase.

</description>

<persons>

<person id="5031">the\_no</person>

<person id="5351">absolem</person>

</persons>

<links>

<link href="http://thepaypal14.com/">Paypal 14 Official Website</link>

<link href="http://en.wikipedia.org/wiki/PayPal\_14">Paypal 14 Wiki Page</link>

</links>

</event>

<event guid="38ea922b-5b2d-4290-8c79-da0c891edd7a" id="6572">

<date>2014-12-30T17:15:00+01:00</date>

<start>17:15</start>

<duration>01:00</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6572\_-\_de\_-\_saal\_1\_-\_201412301715\_-\_security\_nightmares\_-\_frank\_-\_ron</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Security Nightmares</title>

<subtitle>Damit Sie auch morgen schlecht von Ihrem Computer träumen.</subtitle>

<track>Entertainment</track>

<type>lecture</type>

<language>de</language>

<abstract>Was hat sich im letzten Jahr im Bereich IT-Sicherheit getan? Welche neuen Entwicklungen haben sich ergeben? Welche neuen Buzzwords und Trends waren zu sehen?

</abstract>

<description>Wie immer wagen wir den IT-Security-Alptraum-Ausblick auf das Jahr 2015 und darüberhinaus. Denn was wir wirklich wissen wollen, ist ja schließlich: Was kriecht, krabbelt und fliegt in Zukunft auf uns zu und in unseren digitalen Implants herum? Im Zuge von noch mehr Transparenz, Kritik &amp; Selbstkritik und kontinuierlicher nachhaltiger Optimierung aller Prozesse werden wir außerdem frühere Voraussagen hinsichtlich des Eintreffens unserer Weissagungen prüfen.</description>

<persons>

<person id="1633">frank</person>

<person id="384">Ron</person>

</persons>

<links/>

</event>

<event guid="eddb2328-37c3-4e86-86cc-c8541d14b4d7" id="6562">

<date>2014-12-30T18:30:00+01:00</date>

<start>18:30</start>

<duration>01:00</duration>

<room>Saal 1</room>

<slug>31c3\_-\_6562\_-\_en\_-\_saal\_1\_-\_201412301830\_-\_31c3\_closing\_event\_-\_tomate\_-\_dodger</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>31C3 Closing Event</title>

<subtitle/>

<track>CCC</track>

<type>lecture</type>

<language>en</language>

<abstract/>

<description/>

<persons>

<person id="2929">tomate</person>

<person id="1111">dodger</person>

</persons>

<links/>

</event>

</room>

<room name="Saal 2">

<event guid="uJGVeWdNzwr\_8AvAXa2DKA" id="5943">

<date>2014-12-30T11:30:00+01:00</date>

<start>11:30</start>

<duration>01:00</duration>

<room>Saal 2</room>

<slug>31c3\_-\_5943\_-\_en\_-\_saal\_2\_-\_201412301130\_-\_low\_cost\_high\_speed\_photography\_-\_polygon</slug>

<recording>

<license>CC-BY-3.0</license>

<optout>false</optout>

</recording>

<title>Low Cost High Speed Photography</title>

<subtitle>Using microcontrollers to capture the blink of an eye for cheap</subtitle>

<track>Hardware &amp; Making</track>

<type>lecture</type>

<language>en</language>

<abstract>Capturing the splash of a water balloon, the snap of a mouse trap or the impact of a bullet results in exciting pictures. Best of all, it doesn't require expensive equipment. This talk covers the theory of high speed photography, the required hardware, microcontroller hacking and setting up an improvised studio in the shower.</abstract>

<description>A camera, a flash, a microcontroller and a soldering iron is all it takes to create high speed photos of splashing water balloons and other fast moving action. This talk gives a walkthrough from zero to final results.

Starting with initial thoughts on the speed limits of common cameras and how to circumvent them, then going over the configuration of camera and flash. I explain how to use a microcontroller for precise timing of the exposure and how to wire it up to the rest of the setup. Using the example of a splashing water balloon I'll share ideas on using black fabric and duct tape to turn a shower into an improvised studio and finally take that shot.</description>

<persons>

<person id="4689">polygon</person>

</persons>

<links>

<link href="flickr.com/derpoly">Flickr Gallery</link>

<link href="twitter.com/ploynog">Twitter</link>

</links>

</event>

<event guid="aUcSuwZ2iMoJQMEL40opIw" id="6214">

<date>2014-12-30T12:45:00+01:00</date>

<start>12:45</start>

<duration>01:00</duration>

<room>Saal 2</room>

<slug>31c3\_-\_6214\_-\_en\_-\_saal\_2\_-\_201412301245\_-\_attribution\_revolution\_-\_jonas\_oberg</slug>

<recording>

<license>CC-BY-3.0</license>

<optout>false</optout>

</recording>

<title>Attribution revolution</title>

<subtitle>Turning copyright upside-down with metadata</subtitle>

<track>Art &amp; Culture</track>

<type>lecture</type>

<language>en</language>

<abstract>Re-using works licensed under Creative Commons seems pretty simple, but it can often be quite time consuming. One image might be okay, but keeping track of the license and attribution of a thousand images in your mashup, or when quoting from massively crowdsourced data sets such as Wikipedia? Whoah! Don’t we have computers to do that for us!? We do – but there’s no widespread support for including licensing or author information when sharing or reusing digital works. This session will discuss how this should work in the open knowledge environment.</abstract>

<description>Re-using works licensed under Creative Commons seems pretty simple, but it can often be quite time consuming. One image might be okay, but keeping track of the license and attribution of a thousand images in your mashup, or when quoting from massively crowdsourced data sets such as Wikipedia? Whoah! Don’t we have computers to do that for us!? We do – but there’s no widespread support for including licensing or author information when sharing or reusing digital works. This session will discuss how this should work in the open knowledge environment, and could it be that many problems regarding copyright and &quot;piracy&quot; in our digital society could be solved with the right technology?

Let's take a step back and consider how we perceive photographs that we see, online and offline. Didn't you ever want to know who took that awesome photo that you scrolled past in a blog? Or find out more about where that image on Twitter or Facebook comes from? Finding this information for digital photographs can be a daunting task! Sometimes I don't even remember myself where a photograph I took was taken!

Most people have a drawer of black and white photographs at home, a collection of the family history. A very natural reaction when you take a photo, which most people can also relate to, is to turn it over and look at the back of it, hoping that someone -- a parent or grandparent perhaps -- have written on the back of the photo when it was taken, where and who's pictured. The information scribbled on the back represent the context of a piece of art; it's what gives the photograph meaning and value. Metadata is the digital equivalent of your grandmothers handwriting -- giving meaning to pieces of art. By persistently associating the metadata of a photograph with the photograph itself -- making the metadata &quot;stick&quot; -- we can even make sure that your grandmothers handwriting stays with the photograph, even when someone photocopies just one side of it. Assuming the technology makes this easy, of course.

Very recently, we've seen the emergence of technology enabling someone to copy a photograph from a web site, insert it into an editor, and have that editor automatically pick up the associated metadata and provide the correct attribution and licensing information. This has been made possible with the Creative Commons Rights Expression Language (CC-REL), other RDFa metadata, and a clever way of passing information between applications on the clipboard.

In order to relate effectively to the digital works we see online, attribution (who made or built something) matters. It is obvious that proper attribution is the currency of the information age, and it's the start of being able to explore digital works online in their right context. This talk will focus on the philosophical background of why attribution matters, the benefits that technology can bring to the way we work with pieces of art (lolcats and Shakespeare alike), and where we're heading in the future.</description>

<persons>

<person id="5022">Jonas Öberg</person>

</persons>

<links>

<link href="http://elog.io">Elog.io</link>

</links>

</event>

<event guid="4\_Q4s48yg8FV08kvf9lbpQ" id="6397">

<date>2014-12-30T14:00:00+01:00</date>

<start>14:00</start>

<duration>01:00</duration>

<room>Saal 2</room>

<slug>31c3\_-\_6397\_-\_en\_-\_saal\_2\_-\_201412301400\_-\_let\_s\_encrypt\_-\_seth\_schoen</slug>

<recording>

<license>CC-BY-3.0</license>

<optout>false</optout>

</recording>

<title>Let's Encrypt</title>

<subtitle>A Free Robotic Certificate Authority</subtitle>

<track>Ethics, Society &amp; Politics</track>

<type>lecture</type>

<language>en</language>

<abstract>As we've called for widespread use of HTTPS, the cost and complexity of the certificate system has been an obstacle.</abstract>

<description>In 2015, a certificate authority, trusted by mainstream web browsers, will issue certificates for web servers automatically at no charge in under a minute. This CA will automatically perform Domain Validation (DV) to verify applicants' control over domain names. The associated software can optionally reconfigure their web servers and deploy the new certificates immediately.

We'll take a look at how the Let's Encrypt CA works, our ACME protocol for requesting and issuing certs, and the client software that can automate the process. And we'll demonstrate what the experience of getting a cert from the new CA may look like for webmasters (don't look away, or you might miss it!). We'll also talk about who's behind Let's Encrypt and some of the measures we're considering for preventing misissuance of certs. Of course, you're invited to test and help perfect the process.</description>

<persons>

<person id="51">Seth Schoen</person>

</persons>

<links>

<link href="https://www.letsencrypt.org/">Let’s Encrypt</link>

</links>

</event>

<event guid="87b8f1ba-1f05-46c2-93ac-b575bbc9fb4f" id="6597">

<date>2014-12-30T16:00:00+01:00</date>

<start>16:00</start>

<duration>01:00</duration>

<room>Saal 2</room>

<slug>31c3\_-\_6597\_-\_en\_-\_saal\_2\_-\_201412301600\_-\_now\_i\_sprinkle\_thee\_with\_crypto\_dust\_-\_ryan\_lackey\_-\_andres\_erbsen\_-\_jurre\_van\_bergen\_-\_ladar\_levison\_-\_equinox\_-\_daniel\_ziegler\_-\_gedsic</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Now I sprinkle thee with crypto dust</title>

<subtitle>Internet reengineering session</subtitle>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>When the Internet was designed, it was thought to be meadows full of daisies. As we now know, it's a dark place, where communication is monitored and subverted. This session presents both developments in known solutions, as well as novel suggestions, to liberally apply crypto to improve the foundations of Internet communications.</abstract>

<description>&lt;b&gt;Trusting servers you can't touch&lt;/b&gt; by Ryan Lackey:

Servers for Internet applications are usually deployed at a distance from both the end users of the service and the administrators of the system, often controlled by third parties. Even when they're hardware vs. virtualized/cloud, it's rare for admins to have direct physical control of the servers. Yet, most applications require a high degree of trust in the integrity of servers. We describe a variety of technologies and solutions to this problem, and a framework to best protect your applications and your users.

&lt;b&gt;dename: decentralized, secure, usable PKI&lt;/b&gt; by Andreas Erbsen:

A major challenge for private online communication is public key distribution. Trusted authorities have failed to be secure, and the web of trust has failed to build the network effect it gravely requires to be usable. This talk proposes a new PKI system built on a cryptographic consensus protocol. A set of directory servers updates and signs a mapping from public keys to names. Anyone can run their own server, strengthening the security guarantee for all clients that know it. We have an open-source implementation that can be easily integrated with systems that currently rely on manual key verification, including secure

messaging, host authentication, and software distribution.

&lt;b&gt;New development in OTR&lt;/b&gt; by Jurre van Bergen

Jurre van Bergen will speak about new developments in the world of `off-the-record` messaging. What is going on? Where are we going? In addition we will address frequently answered questions by developers and users.

&lt;b&gt;Secure email communication - LEAP Encryption Access Project &amp;

Pixelated Your Right to&lt;/b&gt; by Varac

This presentation will introduce two new secure communication tools under development that help guarantee the right to digitally whisper – LEAP and Pixelated.

&lt;b&gt;Dark Mail&lt;/b&gt; by Ladar Levision

Since Ladar Levison shuttered Lavabit during the summer of 2013, he has been working to solve the email privacy problems that made it technologically possible for an American court to demand unfettered access to the email messages for all of Lavabit’s worldwide customers. After a year of hard work, the Dark Internet Mail Environment (DIME) is a standards based, collaborative effort to create an elegant technical solution capable of protecting the privacy of everyone’s email. It is focused on making end-to-end email encryption automatic, while providing message confidentiality, author verification, and minimizing the leakage of metadata. DIME capable systems reduce the amount of trust users must place in their service provider. Automating the key exchange process while keeping the system resistant to manipulation by sophisticated threats is an ongoing challenge. This talk offers a compressed discussion of the DIME standards, highlighting key portions and will be followed by a project update, where we hope to showcase a DIME capable client and server implementation.

&lt;b&gt;TLS ♥ DNS ♥ Tor&lt;/b&gt; by equinox

Replacing 100 CA hierarchies with the single DNS hierarchy, and how the bite reflex against the latter is coming at the cost of less secure identities.

</description>

<persons>

<person id="4190">Ryan Lackey</person>

<person id="5021">Andres Erbsen</person>

<person id="3519">Jurre van Bergen</person>

<person id="4933">Ladar Levison</person>

<person id="4730">equinox</person>

<person id="5081">Daniel Ziegler</person>

<person id="5263">gedsic</person>

</persons>

<links/>

</event>

<event guid="C4w30id6HpMnzKM2xcrT4g" id="6112">

<date>2014-12-30T17:15:00+01:00</date>

<start>17:15</start>

<duration>01:00</duration>

<room>Saal 2</room>

<slug>31c3\_-\_6112\_-\_en\_-\_saal\_2\_-\_201412301715\_-\_tor\_hidden\_services\_and\_deanonymisation\_-\_dr\_gareth\_owen</slug>

<recording>

<license>CC BY 3.0</license>

<optout>false</optout>

</recording>

<title>Tor: Hidden Services and Deanonymisation</title>

<subtitle/>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>This talk presents the results from what we believe to be one of the largest studies into Tor Hidden Services (The Darknet) to date. </abstract>

<description>There is no public list of onion addresses available; instead, over a period of 6 months, we ran a large number of Tor relays to infiltrate the Distributed Hash Table which Hidden Services publish to. From this, we were able to collect the list of Tor onion addresses AND the number of requests for each site (e.g. loosely analogous to the number of visitors).

We then used a custom web crawler to crawl all the hidden services and pull a large set of information from each. From this, in this talk, we present a the information we found, from the list of the top onion addresses by content type and by popularity to estimates on size and turnover. We will also present what the largest proportion of Tor Hidden Service traffic is (it isn't pretty, and it's not drugs/silk road!).

Finally, I will explain the main classes of attacks useful for deanonymising the Hidden Services and Tor users. Sadly, it's easier than the Tor user-base at large think and thus far, there have been no patches or fixes for these attacks and there isn't likely to be because they exploit fundamental weaknesses in the way Tor works.

</description>

<persons>

<person id="4665">Dr Gareth Owen</person>

</persons>

<links>

<link href="https://www.youtube.com/watch?v=rwawq8PsozU">My previous BSides talk (early results)</link>

</links>

</event>

</room>

<room name="Saal G">

<event guid="f69efb76-d030-4371-83e1-d7b2b8d408b9" id="6580">

<date>2014-12-30T12:45:00+01:00</date>

<start>12:45</start>

<duration>02:15</duration>

<room>Saal G</room>

<slug>31c3\_-\_6580\_-\_en\_-\_saal\_g\_-\_201412301245\_-\_lightning\_talks\_day\_4\_-\_breakthesystem</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Lightning Talks Day 4</title>

<subtitle/>

<track>Other</track>

<type>lecture</type>

<language>en</language>

<abstract>Lightning Talks are short lectures (almost) any congress participant may give! Bring your infectious enthusiasm to an audience with a short attention span! Discuss a program, system or technique! Pitch your projects and ideas or try to rally a crew of people to your party or assembly! Whatever you bring, make it quick!</abstract>

<description/>

<persons>

<person id="5268">breakthesystem</person>

</persons>

<links>

<link href="https://events.ccc.de/congress/2014/wiki/Static:Lightning\_Talks">31C3 Wiki: Lightning Talks</link>

</links>

</event>

<event guid="e192e98a-90ca-44c8-9cfd-86b94a79f4d1" id="6557">

<date>2014-12-30T16:00:00+01:00</date>

<start>16:00</start>

<duration>01:00</duration>

<room>Saal G</room>

<slug>31c3\_-\_6557\_-\_en\_-\_saal\_g\_-\_201412301600\_-\_31c3\_infrastructure\_review\_-\_leon</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>31C3 Infrastructure Review</title>

<subtitle/>

<track>CCC</track>

<type>lecture</type>

<language>en</language>

<abstract/>

<description/>

<persons>

<person id="2042">Leon</person>

</persons>

<links/>

</event>

<event guid="hYXcWw5YzxirnRJZDuYiSQ" id="5931">

<date>2014-12-30T17:15:00+01:00</date>

<start>17:15</start>

<duration>01:00</duration>

<room>Saal G</room>

<slug>31c3\_-\_5931\_-\_en\_-\_saal\_g\_-\_201412301715\_-\_telescope\_making\_-\_madonius</slug>

<recording>

<license>CC-SA 4.0</license>

<optout>false</optout>

</recording>

<title>Telescope Making</title>

<subtitle>How to make your own telescope</subtitle>

<track>Hardware &amp; Making</track>

<type>lecture</type>

<language>en</language>

<abstract>In this talk an introduction to amateur telescope making (ATM) will be provided. Starting from grinding the mirror, testing it and building the telescope around it.</abstract>

<description>Why to take the effort to make your own telescope? Because it's custom and many times even cheaper.

How-To grind your own mirror, lens, test its optical properties and build the telescope around that optics. The focus will be on newtonian telescopes but other types will be outlined as well.

Grinding the optical components is the trickiest part, here the techniques and methods are explained, especially how to make high precission optics with your own hands.

Testing those is very critical especially in the late manufaturing process, but optical testbenches can be made for as much as 30-50€

The most time consuming part is the building of the telescope itself, here many aspects have to be considered and taken into account.</description>

<persons>

<person id="4660">Madonius</person>

</persons>

<links/>

</event>

</room>

<room name="Saal 6">

<event guid="EN5SvbzMs0D7iCFyfK1Ubw" id="6213">

<date>2014-12-30T11:30:00+01:00</date>

<start>11:30</start>

<duration>01:00</duration>

<room>Saal 6</room>

<slug>31c3\_-\_6213\_-\_en\_-\_saal\_6\_-\_201412301130\_-\_the\_rise\_and\_fall\_of\_internet\_voting\_in\_norway\_-\_tor\_e\_bjorstad</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>The rise and fall of Internet voting in Norway</title>

<subtitle>Evaluating a complex cryptographic implementation</subtitle>

<track>Ethics, Society &amp; Politics</track>

<type>lecture</type>

<language>en</language>

<abstract>In the parliamentary elections of September 2013, more than 250 000 Norwegians in selected municipalities were able to vote from home. They were taking part in a national trial of Internet voting, building on an advanced cryptographic protocol.</abstract>

<description>The Norwegian e-vote project started in 2008, and was used for live election trials in 2011 and 2013. By using cutting-edge cryptography and committing to a high degree of openness in all parts of the execution, the project aimed to overcome public concerns about security risks and lack of verifiability.

To promote security, the entire voting system was implemented using a complex and verifiable cryptographic protocol, with no assumed trust between different system functions. To promote openness, the entire election system source code is publicly available, as well as most project documentation. The voting system would published the SHA-256 hashes of encrypted ballots on GitHub every hour, and detailed instructions were provided to voters on how to verify that their vote had been submitted.

In the run-up to the 2013 elections, the author audited the cryptographic Java implementation of the back-end election system, making a number of surprising findings. During the actual elections, a major encryption bug was discovered in the Javascript frontend code, potentially revealing the preferences of a large number of voters.

Most hackers and cryptographers are highly sceptical of Internet voting, due to legitimate security concerns. Even so, insufficient technical security, or even the perception of such, does not appear to be a main reason for why the project was discontinued.

The aim of this talk is twofold. First, we shall look at Norway's Internet voting project in its social and political context, highlighting the reasons why it came to be, and some of the key forces shaping the project throughout. Secondly, we discuss the findings, experiences and lessons learned from attempting to audit a large, public, complex and security-critical code base.</description>

<persons>

<person id="4973">Tor E. Bjørstad</person>

</persons>

<links>

<link href="https://www.regjeringen.no/en/dep/kmd/prosjekter/e-vote-trial/id597658/">The Norwegian e-vote trial</link>

</links>

</event>

<event guid="yN\_BHtGEljjFHh2dl-Irug" id="6157">

<date>2014-12-30T12:45:00+01:00</date>

<start>12:45</start>

<duration>01:00</duration>

<room>Saal 6</room>

<slug>31c3\_-\_6157\_-\_en\_-\_saal\_6\_-\_201412301245\_-\_diamonds\_are\_a\_quantum\_computer\_s\_best\_friend\_-\_nicolas\_wohrl</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Diamonds are a quantum computer’s best friend</title>

<subtitle/>

<track>Science</track>

<type>lecture</type>

<language>en</language>

<abstract>The next revolution in data processing is Quantum computing.

This talk is an entertaining “tour de force” starting with a brief introduction to the fascinating yet strange theories of quantum physics, the concepts of using these in quantum computing and the latest results on qubits in devices made out of real diamonds.

If you want to learn about the machines that decrypt your passwords in the coming years and how you can actually grow diamonds in your microwave oven (and who wouldn’t?) this talk is for you!

</abstract>

<description>Quantum computing uses quantum phenomena directly such as superposition and entanglement to perform data processing. However, applying these quantum concepts to macroscopic devices such as computers is an enormous challenge for information scientists and physicists alike. What does it make so hard? Well, scientists have to find a material in which they are able to store and manipulate quantum bits (qubits). Since quantum states are very fickle and thus hard to abide the most important task is to find materials in which qubits can be stored for a sufficient long time. Surprisingly they found these properties in diamond. More specific, scientists are investigating defect centers in diamond to be used as qubits. Although quantum computing in 2014 is still in its infancy first experiments have already been carried out that give hope that these computational concepts will become reality.

This talk is an entertaining “tour de force” starting with a brief introduction to the fascinating yet strange theories of quantum physics, the concepts of using these in quantum computing and the latest results on qubits in devices made out of diamond. Moreover this presentation is given by a physicist who was working on diamond for various other applications for years - who suddenly realized that he has the material for the next IT revolution right in his lab.

If you want to learn about the machines that decrypt your passwords in the coming years and how you can actually grow diamonds in your microwave oven (and who wouldn’t?) this talk is for you!

</description>

<persons>

<person id="4984">Nicolas Wöhrl</person>

</persons>

<links>

<link href="http://youtu.be/TNgSxEE6wTk?t=10m29s">Presentation @ Republica2014</link>

<link href="http://241568.website.snafu.de/wordpress/">Podcast: Methodisch inkorrekt</link>

</links>

</event>

<event guid="9RncwfCW37x4dhs15BQqBQ" id="6297">

<date>2014-12-30T16:00:00+01:00</date>

<start>16:00</start>

<duration>01:00</duration>

<room>Saal 6</room>

<slug>31c3\_-\_6297\_-\_en\_-\_saal\_6\_-\_201412301600\_-\_virtual\_machine\_introspection\_-\_tamas\_k\_lengyel\_-\_thomas\_kittel</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Virtual Machine Introspection</title>

<subtitle>From the Outside Looking In</subtitle>

<track>Security &amp; Hacking</track>

<type>lecture</type>

<language>en</language>

<abstract>New methods and approaches for securing cloud environments are becoming increasingly more critical as traditional host security strategies are not well integrated into virtual environments. For example, antivirus scans are a critical component of layered defense-in-depth, but in the cloud they rapidly exhaust available CPU and memory. The cloud environment nevertheless offers a unique opportunity: the ability to peer into a running operating system from an outside perspective, known as virtual machine introspection (VMI). More interestingly, it is also possible to alter the behavior of the virtualized components to help protect virtual systems in real-time. In this talk we will explore the open-source LibVMI library which over the last year, as part of the DARPA Cyber Fast Track program, has been significantly extended to ease the process of developing cloud security solutions.</abstract>

<description>New methods and approaches for securing cloud environments are becoming increasingly more critical now that virtual environments are being widely adopted by the businesses sector. Despite the fact that virtualization itself is not inherently insecure, the majority of virtual systems are less secure than those physical systems they replace. This curious state arises primarily because traditional host security strategies are not well integrated into virtual environments: as an example, typical antivirus scans are a critical component of layered defense-in-depth, but they rapidly exhaust available CPU and memory when protecting a large number of virtual machines. Some antivirus vendors have taken a small step into virtualization by adapting their existing products to scan the disks of VMs from an external perspective, but this gain in efficiency does not fully realize the potential for protection and monitoring of a virtual environment. In addition, weakly implemented ”self-defense” techniques leave themselves vulnerable to being neutralized by undetected or zero-day attacks. This ”one opportunity” for success is a critical handicap for existing protective measures.

Virtualization nevertheless also offers a unique opportunity: the ability to peer into a running operating system from an outside perspective, known as introspection (VMI). It is possible to observe the memory, storage, CPUs, processes, and kernel of a running virtual machine from a safe vantage point. More interestingly, it is also possible to alter the behavior of all of these components to help protect virtual systems. The open-source LibVMI library has been designed specifically for this purpose, to look at 32-bit or 64-bit virtual machines, both on x86 and ARM. Over the last year, as part of DARPA's Cyber Fast Track program, LibVMI has been significantly extended by our team to ease the process of developing secure intrusion detection and intrusion prevention systems for the cloud. Utilizing Xen's advanced memory access system and the latest virtualization extensions available on Intel processors, LibVMI now offers unique capabilities for instrumenting, inspecting and controlling the execution of hosted guest operating systems and applications. Further combined with Xen's Security Modules, cloud security applications can be now tailored to provide a multi-tiered security environment required for multi-tenant cloud deployments.

In this talk we will explore the finer details how these features can be utilized for the detection of advanced rootkits techniques, while providing a stealthy, tamper resistant environment. Our talk will explore the disaggregation of Xen's trusted computed base (TCB) with the use of the FLASK policy engine, and the changes our team implemented and contributed to Xen and the Linux kernel, to make secure cross-domain introspection part of a coherent mandatory access control system. Diving deeper into the virtualization details of the x86 architecture we will discuss advanced instrumentation techniques via the Extended Page Tables and via software breakpoint injection, and how these features are now accessible via the LibVMI API.

We will also discuss critical details of live memory introspection and highlight common pitfalls in developing secure applications without relying on untrusted and potentially compromised data-sources. We will explore how mapping in-memory Linux and Windows kernels is performed by LibVMI, and compare it to other forensics tools, such as Volatility and Rekall. Our talk will further explore how to use existing forensics tools on live virtual machine to analyze modern malwares. At last, we will briefly discuss open challenges in virtualization security and some of the new CPU features proposed by Intel.</description>

<persons>

<person id="5060">Tamas K Lengyel</person>

<person id="5314">Thomas Kittel</person>

</persons>

<links/>

</event>

<event guid="78d34ebe-e910-4d26-98e3-71c0f07cedb6" id="6607">

<date>2014-12-30T17:15:00+01:00</date>

<start>17:15</start>

<duration>01:00</duration>

<room>Saal 6</room>

<slug>31c3\_-\_6607\_-\_de\_-\_saal\_6\_-\_201412301715\_-\_security\_nightmares\_stream\_-\_frank\_rieger\_-\_ron</slug>

<recording>

<license/>

<optout>false</optout>

</recording>

<title>Security Nightmares (Stream)</title>

<subtitle>Damit Sie auch morgen schlecht von Ihrem Computer träumen.</subtitle>

<track>Entertainment</track>

<type>lecture</type>

<language>de</language>

<abstract>Was hat sich im letzten Jahr im Bereich IT-Sicherheit getan? Welche neuen Entwicklungen haben sich ergeben? Welche neuen Buzzwords und Trends waren zu sehen?</abstract>

<description>Wie immer wagen wir den IT-Security-Alptraum-Ausblick auf das Jahr 2015 und darüberhinaus. Denn was wir wirklich wissen wollen, ist ja schließlich: Was kriecht, krabbelt und fliegt in Zukunft auf uns zu und in unseren digitalen Implants herum? Im Zuge von noch mehr Transparenz, Kritik &amp; Selbstkritik und kontinuierlicher nachhaltiger Optimierung aller Prozesse werden wir außerdem frühere Voraussagen hinsichtlich des Eintreffens unserer Weissagungen prüfen.</description>

<persons>

<person id="5183">Frank Rieger</person>

<person id="384">Ron</person>

</persons>

<links/>

</event>

</room>

</day>

</schedule>