

# 21C3 - the usual suspects

# Fahrplan Day 3, 10:00-18:00

v1.0.2

10  
10.5  
11  
11.5  
12  
12.5  
13  
13.5  
14  
14.5  
15  
15.5  
16  
16.5  
17  
17.5

Saal 1	Saal 2	Saal 3	Saal 4	Workshop	Haecksen	AVIT	Lockpicking
						286: AVIT Breakfast Day Three ( <i>Toby-spark</i> ) · Breakfastmeeting as daily introduction. There will be free Brötchen, Kaffee and Tee for the attending VJs.	
133: <b>How To Herd Cats</b> ( <i>Druid</i> ) · Despite the hacker ethic of free information real life frameworks for constructive dialogue are sadly lacking. Interestingly a number of systems, from socratic dialogue to parliamentary procedure already exist for structuring conversation toward a goal. In this talk we will look at hacker workgroups from open source developers to CTf teams ...	250: <b>Lightning Talks: Day 3</b> ( <i>Hanno Wagner</i> ) · Lightning Talks are your chance to give introductory talks for your projects, interesting technologies and evolving developments and other things that might be interesting to the 21C3 audience.	46: <b>Toll Collect</b> – Verpeilen im industriellen Maßstab ( <i>Volker Birk</i> ) · Technik und juristischer Hintergrund des Mautsystems ausgeleuchtet nach Stärken, Schwächen und dem Überwachungsauftrag.	127: <b>Security Frameworks</b> – An enterprise approach to security ( <i>Robert Frazier</i> ) · The presentation looks at security from a framework approach, using the OSI 7 layer model to map security tools across the enterprise. The discussion centers on how security tools map to the OSI model to provide end-to-end security.	256: <b>On finding the score to visuals</b> ( <i>codeep: Ros Roca, codeep: Seex</i> ) · To find a standard which can be used as a medium that can persevere the work of a vj for institutional conservation and later use, we must first define the form of art that it is. Visuals are determined by several crucial factors that we try to shine light on.	305: <b>(K)lein Anschluss unter dieser Nummer</b> – Die Informationsgesellschaft: Neue Chancen und Hemmnisse für geschlechtergerechte Entwicklung ( <i>Heike Jensen</i> ) · Dr. Heike Jensen (HU Berlin und terre des femmes) ist mit Olga Drossou in der einzigen Frauengruppe für die WSIS und hat sich auf Frauen-NGOs spezialisiert. Geplant ist ein Workshop zu WSIS und Computer-Frauen: was können / wollen die Haecksen für Forderungen einbringen?		231: <b>Lockpicking von Meisterhand</b> – Für Anfänger und Fortgeschrittene · Zu jeder vollen Stunde beginnt ein Lockpicking-Workshop. Traditionell werden die ersten Workshops von den neuen Deutschen Meistern gehalten.
135: <b>Voting Machine Technology</b> ( <i>Tom Trumpbour</i> ) · The talk will be about voting machine technology, a short history, its vulnerabilities and overall reliability. There will be a concentration about the Diebold e-voting code and its limitations.	15: <b>Sicherheit bei VoIP-Systemen, eine Einführung</b> – Welche Standards gibt es, was wird de-facto wo genutzt? ( <i>Christian Louis</i> ) · Der Vortrag beschäftigt sich mit Sicherheit von VoIP, einem Stiefkind der Entwicklung rund um diese neue Killerapplikation. Es wird versucht, einen Überblick über bestehende Produkte und Lösungen zu geben und aufzuzeigen, welche Sicherheit heute ...	111: <b>The Kernel Accelerator Device</b> – Reconfigurable computing for the kernel ( <i>Ludwig Jaffé</i> ) · KAD is an interdisciplinary development project which consists of kernel driver programming, fpga programming (VHDL/Verilog) and hardware development. There is no working KAD at the moment, but our aim is to develop such a device under the GPL with much support from everyone who ...	126: <b>Apache Security</b> – Improving the security of your web server by breaking into it ( <i>Sebastian Wolfgarten</i> ) · While apparently being quite secure out of the box the Apache web server is still a well-liked target for hackers. This talk will help system administrators to improve the security of their site and will also cover techniques on attacking a web server.	253: <b>Pixels want to be many</b> – High definition video and reasons for using it in a VJ context ( <i>4YourEye:Eva, 4YourEye:Gery</i> ) · Technics and Ideas for VJing in high resolutions made possible by the new consumer video format HDV.			
138: <b>Protesting in the new Millenium</b> – The Use of Electronic Communications to Protest ( <i>Emmanuel Goldstein</i> ) · Emmanuel Goldstein describes the changing times in the United States. While hackers were always looked upon with suspicion, they are now seen as a very definite threat on the order of terrorists. Add activism into the mix and there's no end to the potential for ...	122: <b>Enforcement of Intellectual Property Rights under German Private Law</b> – An outline in view of the European Directive on the Enforcement of Intellectual Property Rights (2004/48/EC) ( <i>Ulrike Mahlmann</i> ) · The objective of the European Directive "on the Enforcement of Intellectual Property Rights" is to help prevent intellectual property infringements and to ...	163: <b>SPAM Workshop</b> – SPAM- und Zombie-Abwehr bei hohem Mail-Volumen am Beispiel von gmail ( <i>Sirko Zidlewitz</i> ) · SPAM-Mails und virenverseuchte Mails von Zombie-Rechnern stellen für kleine und große Provider eine dauerhafte Herausforderung dar. Am Beispiel von gmail wird die Integration von einem mehrstufigem, modularen Anti-SPAM-Konzept erläutert. An welcher Stelle des "Qmail-Big-Picture" setzt welches Verfahren an, und warum ist dies alles nur Flickwerk? Bewußt werden eventuelle zukünftige Standards noch nicht berücksichtigt, sondern nur derzeit umsetzbare Möglichkeiten zur Kombination verschiedener Verfahren erklärt.	11: <b>xDash</b> – Wie integriere ich meine Applikationen mittels Instant Messaging? ( <i>Jerzy Wachowiak</i> ) · In praktisch jeder Firma existieren Applikationen nebeneinander, die auf unterschiedlichen Betriebssystemen und Datenbanken laufen. Das Rückgrat der Integration von IT-Systemen nach dem Muster "Publish/Subscribe" bildet der "Asynchronous Messaging ...	254: <b>AVIT`C3 MIDI Lab</b> – MIDIFY · DONT MYSTIFY ( <i>Elektraschroeder, Hamageddon</i> ) · in this workshop we will explore different methods of controlling vj applications with dedicated midi hardware.	140: <b>A Fat Girl's Intimate Perspective on Hacker Culture and Spaces</b> – How to Survive a Cock Fight, without a Cock ( <i>b9punk</i> ) · Despite her gender handicap, "b9punk" has managed to chill out in the American Hacker scenes and retain her self-respect. Her contemporaries think that's a pretty big accomplishment and would like her to talk to you about her (pending) patented formula for what she crudely calls "putting up with the bullpucky, and getting something out of the hacker scene besides sex." She's also conducted a extensive survey with ...		
308: <b>MD5 To Be Considered Harmful So-meday</b> ( <i>Dan Kaminsky</i> ) · Joux and Wang's multicollision attack has yielded collisions for several one-way hash algorithms. Of these, MD5 is the most problematic due to its heavy deployment, but there exists a perception that the flaws identified have no applied implications. We show that the appendability of Merkle-Damgard allows us to ...	278: <b>TKÜV · Das Ohr am Draht</b> – Recht, Regulierung und Realität der Telekommunikationsüberwachung in Deutschland ( <i>Jörg Müller-Kind</i> ) · Rund 200 Verpflichtete müssen bis zum 31.12.2004 Konzepte für die Überwachung von E-Mail bei der RegTP eingereicht haben. Über Breitband-IP-Access (xDSL, Cable, Wireless) und VoIP wird heftig ...	218: <b>Practical Mac OS X Insecurity</b> – Security Concepts, Problems, and Exploits on Your Mac ( <i>Angelo Laub</i> ) · Some recent security problems with Mac OS X stem from the fact that Apple tries to combine the Unix security model with easy and convient usability and closed source. Showing examples from our own research we will take you on a pleasant journey to get root on almost any ...	17: <b>Next-Generation Peer-to-Peer Systems</b> ( <i>Magnus Kolwey</i> ) · A significant paradigm for the Internet are Peer-to-Peer Systems. Those networks form new types of distributed information platforms. The lecture will discuss concepts for Next-Generation Peer-to-Peer Systems that range beyond the scope of todays filesharing applications.	73: <b>Coden auf dem Info-Layer</b> – Die Hierarchie der Online-Kommunikation oder: Warum der Titel die Botschaft ist ( <i>Erich Mächel</i> ) · Im Zentrum von Vortrag/Workshop stehen Auswahl, Analyse und Produktion von Nachrichten für News/sites, Weblogs, Mailing/lists etc. Definition der eigenen Ziele und der möglichen Dialog-Gruppen. Zusammenstellen der Quellen und Brauen der eigenen Nachrichten/mixtur. Wie man aus Texten unbekannter Autor/innen Ideologien, Meinungen und Werte herausfiltert. Die gnadenlose Hierarchie der Online-Kommunikation oder: Weshalb der Titel die Botschaft ist. Sowie weitere bisher bekannt gewordene Faustregeln der E-Kommunikation anhand von praktischen Beispielen. Produktion eines Nachrichtentexts, der am Ende des Workshops auch publiziert wird.	259: <b>Apple Motion on the Workbench</b> – Introduction and Working with Apple Motion ( <i>lAlk</i> ) · Meant as a short introduction into Apple Motion as a very fast tool for preparing VJ loops. This will be a collaborative exploration of the program for everyone to have a look at this marvelous tool.		
134: <b>Secure Instant Messaging</b> – Suppression of secure communications by governments ( <i>phar</i> ) · The talk describes some of the current practices of Instant Messaging providers, and go over what makes some of the design choices better or worse, describing possible and known attacks against messaging protocols and suggest possible solutions to those problems. If possible a live ...	168: <b>Spam-Politik</b> – Politisch-rechtliche Bekämpfung unerwünschter Information ( <i>Dirk Schmidt</i> ) · Spam ist ein nicht einfach zu fassender Begriff. Unterschiedliche Perspektiven auf die spam-Phänomene, entgegenstehende Interessen und die Historie führen zu unterschiedlichen Problemendarstellung und schließlich Lösungsvorschlägen für die spam-Bekämpfung. Dieser widmet sich der ...	107: <b>Embedded devices as an attack vector</b> ( <i>Stephen Lewis</i> ) · Although attacking embedded devices is not a new idea, little work has been done on using these devices for attack. Here I present work on the insertion of custom code into a network switch in order to carry out attacks on a network.	40: <b>Firewall Piercing</b> – Creative exploitation of valid Internet protocols to get your data through obstacles ( <i>Alien8, Maik Hentsche</i> ) · IT will be shown how IPv4 based protocols can be used to tunnel data through Firewalls while maintaining RFC compatibility. The goal is to show a broad spectrum of techniques. However, a few examples are presented in more detail.	273: <b>Crashkurs Mathematik am Beispiel Biometrie</b> ( <i>Jule P. Riede</i> ) · Dieser Vortrag ist ein Crashkurs in Mathematik am Beispiel Biometrie. Ausgehend von dem Problem, eine Iris in einem Foto zu lokalisieren, fangen wir bei der Definition einer Funktion an und landen via Trigonometrie, Differential- und Integralrechnung, sowie ein wenig linearer Algebra bei Vektoranalysis und Statistik.	328: <b>Pure Data and Gem for VJs</b> – hacking with pure data: the VJ edition ( <i>Asli Serbest, Peter Plessas</i> ) · An introduction to the open source alternative to the widely used PD graphical programming environment with special emphasis on GEM the Pure Data Open GL engine		
158: <b>How to find "anything" on the Web</b> – Advanced internet searching strategies & "wizard seeking" tips ( <i>Fravia</i> ) · Participants will be trained to become good "seekers". Techniques and tricks used for efficiently searching through the world wide web will be taught and search engines will be reviewed in short: the hacker's approach to ...	164: <b>Barrierefreies Internet</b> – Aspekte der Minimierung der Unmöglichkeit ( <i>Petra Berndt, Ralf Roltschek</i> ) · Menschen mit Behinderungen sind überdurchschnittlich häufig im Internet aktiv weil dies eine Kommunikationsmöglichkeit darstellt die sie im 'real live' nicht oder nur eingeschränkt haben. Der Vortrag soll zeigen welche Barrieren sich im Internet für Behinderte beim ...		72: <b>The Reality of Network Address Translators</b> – Dealing with NAT ( <i>Harald Welte</i> ) · NAT's are ubiquitous in todays Internet. Unfortunately the IETF missed to recognize this reality. Due to this lack of standardization, NAT's pose an enormous threat to the paradigm shift from client-server to peer-to-peer. The presentation covers proposed solutions.		262: <b>Pixels don't need no money</b> – Ethics of a corporate sponsored VJ scene ( <i>lAlk</i> ) · With the recent push of large corporations (like Motorola and BMW) or mass media (like MTV) into the VJ scene questions are raised of how we can sustain a community driven scene without capitalistic influence and its main focus on the artistic side of our craft.		

	Saal 1	Saal 2	Saal 3	Saal 4	Workshop	Haecksen	AVIT	Lockpicking
18	125: Old Skewl Hacking: Infra Red – MMir-DA (Major Malfunction's Infra Red Discovery Application) ( <i>Major Malfunction</i> ) · This talk will cover methods for discovering the hidden capabilities of Infra-Red remote controls, as well as brute forcing single function controls such as garage door openers or car alarm systems. It will look at the 'why' as well as the 'how', and opens ...	19: Verdeckte Netzwerkanalyse – Ich weiss, was Du weisst ( <i>Torsten Höfler</i> ) · Es gibt relativ viele Möglichkeiten passiv festzustellen, mit welchem Betriebssystem man sich gerade "unterhält". Die theoretischen Grundlagen des Fingerprintings und einige Tools werden vorgestellt. Einige Tipps zur Abhilfe (hide myself) werden ebenfalls gegeben.	174: Lobbying für Nerds ( <i>Andreas Bogk, Andreas Dietl, Andy Müller-Maguhn, Markus Beckedahl</i> ) · Eine Vielzahl von politischen Direktiven und Gesetzen verändern den Umgang mit den neuen Medien. Viele einflussreiche Lobbygruppen nutzen die in diesem Themengebiet unerfahrenen Politiker, um ihre Interessen politisch durchzubringen. Idee dieses Vortrags ist es, politische Prozesse ...	83: Quanteninformationstheorie für Nicht-Physiker – Keiner hat's verstanden, aber alle basteln dran ( <i>Sandra Gaycken</i> ) · Die Quanteninformationstheorie prophezeit grundlegende Revolutionen für die Informationstechnologie. Ist zwar die alltägliche technische Anwendung noch fern, lassen sich doch anhand der Vielzahl aktueller Bemühungen bereits recht genaue Bilder davon ...	207: Amateurfunk · ein Hobby mit Hack-value!?! – Eine kurze Einführung mit Beleuchtung chaosrelevanter Aspekte ( <i>Marc Schneider, Thomas Rücker</i> ) · Der Amateurfunk hat eine lange Tradition im CCC. Wir werden interessante Gebiete aus dem breiten Themenspektrum des Afu betrachten und aktuelle Forschungsfelder vorstellen. Fehlen dürfen natürlich nicht diverse Hacks im und um den Amateurfunk (Mobiltelefonie, drahtlose Datenübertragung, etc.). Weiterhin werden wir die Aktivitäten der IG Chaoswelle / DARC OV D23 vorstellen. In Ihr sind die meisten Funkamateure im und um den CCC organisiert. Hier gibt es das ganze Jahr über interessante Veranstaltungen und es werden neue Ideen ausgebrütet. Man trifft sich täglich zum Chat im vom Internet (fast) ...	313: Biometrie als datenschutzrechtliches Problem ( <i>Elisa</i> ) · Je nach Art des Verfahrens, Einsatzort und den verwendeten Merkmalen kann Datenschutz eine große Rolle beim Einsatz biometrischer Verfahren spielen. Da sich die anfallenden Daten im privaten Bereich stark von denen im öffentlichen Bereich (Ausweise) unterscheiden, muss dieses Problem sehr differenziert betrachtet ...		
19	95: Security Nightmares 2005 – Oder: worüber wir nächstes Jahr lachen werden ( <i>Frank Rieger, Ronj</i> ) · Security Nightmares betrachtet die Vergangenheit, Gegenwart und Zukunft von Sicherheitsvorfällen in der IT. Wir machen eine Rückschau auf unsere Vorhersagen vom letzten Jahr, unterhalten uns darüber, was sonst noch passiert ist und wagen dann die Vorschau ins nächste Jahr.	13: The Art of Fingerprinting – Open your eyes on the network ( <i>Ilya van Sprundel, Maximilian Dornseif</i> ) · Fingerprinting is the art of extracting features from a resource and comparing it to a database to draw conclusions about the probed resource. We show the current state of the art of fingerprinting on all layers of the TCPstack, will evaluate existing tools and release ...						
20								
21								
21.5	173: Closing Event – So long and thanks for all the fish ( <i>Tim Pritlove</i> ) · The final get-together looking back at three days of genuine hacking experience at bcc. 21C3 tried to reinvent the Congress in a couple of ways. Did we succeed? Could we do better? Of course we can, but looking ahead to 22C3 should bring us finally on the road to a true international event that serves ...							