

# Bericht zum 27. Chaos Communication Congress

27.12. - 30.12.2010 in Berlin, Deutschland



Der Chaos Communication Congress ( CCC ) ist eine der wichtigsten Veranstaltungen zu den Themen Telekommunikations- und Computersicherheit im deutschsprachigen Raum. Er wird seit 1984 regelmässig vom Verein *Chaos Computer Club* veranstaltet. Dabei gibt es eine Vielzahl von Vorträgen und Workshops zu aktuellen technischen und gesellschaftspolitischen Themen.

Nachdem bereits der Vorverkauf nicht ganz glatt über die Bühne gehen wollte, gab es zu Beginn des Kongresses bereits wieder technische Probleme mit dem Vorverkaufssystem. Doch dank des tatkräftigen Einsatzes der freiwilligen Helfer und Techniker vor Ort konnte die Konferenz trotzdem pünktlich und wie geplant beginnen.

In der Keynote unter dem Titel - *We Come in Peace* – berichtet Rop Gonggrijp über den weltweiten Einsatz von Wahlcomputern und die zunehmende Überwachung der Bevölkerung in westlichen Ländern.

Gleich anschliessend folgte der Vortrag *Copyright Enforcement VS Freedoms* wobei unter anderem auf ACTA und IPRED3 eingegangen wurde.

Die Digitalisierung alter und neuer Werke ist an vielen Bibliotheken Europas bereits Realität und bringt den Beteiligten etliche Vorteile. Die technischen Abläufe der Digitalisierung sind mittlerweile schon recht erprobt, jedoch sind die rechtlichen und politischen Rahmenbedingungen noch aus dem „Analogen Zeitalter“. Die naive Strategie – sich über das geltende Urheberrecht hinwegzusetzen – wie Google dies einst tat, ist für

die Bibliotheken offensichtlich nicht gangbar. Bereits jetzt implementieren und nutzen Bibliotheken digitale Verleihprozesse, welche das Konzept, dass ein „Virtuelles Exemplar“ eines Buches auch nur einmal verliehen werden kann, und der nächste Nutzer auf die „Rückgabe“ warten muss abbilden.

In 3 Sälen gab es ein dicht gepacktes Vortragsprogramm von Mittags bis Mitternacht. Zusätzlich wurden noch Abseits dessen weitere Gesprächsrunden und Workshops zu verschiedensten Themen abgehalten. Bei manchen Vorträgen war allerdings ein derart grosser Ansturm, dass sich spätkommende Teilnehmer mit der Übertragung auf dem Monitor vor dem Saal oder am eigenen Laptop begnügen mussten. Dies war jedoch auch nicht immer ganz einfach zu bewerkstelligen, denn trotz aktuellster Technik namhafter Netzwerkhersteller, welche für den Kongress bereit gestellt wurde, konnte das WLAN der Belastung mehrerer tausend Endgeräte nicht standhalten. Nicht nur dass beinahe jeder Kongressteilnehmer einen Laptop nutzte sondern auch die immer weiter steigende Zahl von Smartphones überlasteten schliesslich diese essenzielle Infrastruktur. So sahen sich viele Nutzer gezwungen Kable auszupacken und sich um die vereinzelt Netzwerkdozen zu scharen.

Noch am selben Tag gab es einen intressanten Vortrag über Sicherheitsproblematiken in den aktuellen IPv6 Implementierungen verschiedener Betriebssysteme. Zwar ist mittlerweile jedes moderne Betriebssystem in der Lage mit diesem neuen Netzwerkprotokoll zurecht zu kommen, jedoch sind teilweise gravierende Mängel in der Standardkonfiguration gemacht worden.

Mit der guten Absicht, einen möglichst einfachen Umstieg vom bestehenden auf den neuen Standard zu ermöglichen, wird einem potentiellen Angreifer sehr leicht ermöglicht die Kontrolle über DHCP und DNS Server zu erlangen ohne dass dies für die Benutzer ersichtlich wäre. Mit Hilfe dieser beiden grundlegenden Netzwerkdiensten kann ein potentieller Angreifer dann auch relativ leicht beliebige andere Services angreifen oder sich auf die Jagd nach Benutzerdaten und Passwörtern machen.

Am zweiten Tag wird gleich auf ein weiteres Sicherheitsrisiko in Form der aktuellen SSL-Richtlinien eingegangen. Die damit verbundene Infrastruktur schützt einerseits die Privatsphäre des Nutzers, indem die Verbindung zwischen Server und Client verschlüsselt wird. Andererseits soll damit auch eine Authentifizierung des Servers erfolgen, um gegen „man in the middle“ Angriffe zu schützen. Beispielsweise um sicher zu gehen, dass die Online-Banking Seite auch wirklich von den Servern der eigenen Bank stammt, und nicht eine Immitation von böswilligen Betrügern ist.

Die technische Umsetzung ist aus heutiger Sicht ausreichend, und wird durch starke kryptographische Verfahren gewährleistet. Das Verfahren basiert allerdings auf dem absoluten Vertrauen in die Certificate Authorities. Dies sind Firmen, welche die Aufgabe haben, sich für die Identität ihrer Kunden gegenüber den Internet Nutzern zu verbürgen. Die gängigen Browser werden alle mit einer Liste von hunderten solcher über die ganze Welt verstreute Stellen ausgeliefert, und allen wird vollkommen vertraut. Neben der Möglichkeit einer böswilligen Ausstellung gefälschter Zertifikate, existiert auch die Gefahr dass die zur Ausstellung der Zertifikate verwendeten Computersysteme nicht ausreichend gesichert sind. Auf diesem Weg sind vor kurzer Zeit gefälschte Zertifikate für google.com, yahoo.com, skype.com und einige andere prominente Adressen erstellt worden.

Meinen persönlichen Höhepunkt dieses Tages bildete *The Concert* im grossen Saal. Die Live Aufführung von Corey Cerovsek (Violine) und Julien Quentin (Piano) welche gemeinsam mit Medienkünstler Alex Antener einen wunderbaren Bogen von Lennon über Mozart und Bizet bis hin zu Bach spannten und dies in Kombination mit modernen visuellen Techniken zu einem unvergleichlichem multimedialem Erlebniss machten.

Der dritte Tag bot neben vielen security Vorträgen, speziell zu den Themen RFID und GSM auch einen kurzen Vortrag über die Icelandic **M**odern **M**edia Initiative – eine Bemühung der isländischen Regierung zur Anpassung der derzeitigen Gesetzeslage an

das digitale Zeitalter. Dadurch sollen die Rechte aller Beteiligten freier und unabhängiger Berichterstattung gewährleistet werden. Angefangen bei den Journalisten und ihren Quellen, über die Betreiber der Server- und Netzwerkinfrastruktur bis hin zum Konsumenten sollen sowohl die Rechte, Privatsphäre und Kommunikation dieser Parteien durch legislative und technische Mittel nach bestem Vermögen gewährleistet werden. Bedingt durch das Medium Internet muss dies alles auch immer in einem internationalen Kontext betrachtet werden, wodurch diese Bemühungen noch ein Stück schwieriger und Konsequenzen teilweise unvorhersehbar werden.

OMG\_WTF\_PDF – der provokante Titel eines Vortrags über ein bis vor 3 Jahren proprietäres Format für Dokumente, welche ursprünglich von der Firma Adobe Systems geschaffen wurde. Dank einer schweren Veränderbarkeit und der Möglichkeit das Dokument auf unterschiedlichsten Betriebssystemen zu betrachten, hat dieses Format weltweite starke Verbreitung gefunden. Auch in vielen Bibliotheken werden PDF Dateien zu Speicherung von Digitalisaten zum Verleih als auch zur Langzeit-Archivierung (in Variante PDF/A) verwendet. In den letzten Jahren wurden - speziell in der Referenz Implementierung von Adobe – unglaublich viele Sicherheitslücken in den Betrachtungsprogrammen entdeckt. Oftmals wurde Adobe in diesem Zusammenhang sehr viel Fahrlässigkeit bei der Implementierung vorgeworfen, jedoch ist die Situation noch weitaus bedenklicher.

Das „**P**ortable **D**ocument **F**ormat“ wurde sehr nahe an dem **P**ostscript Format (welches vor allem bei Laserdruckern Unterstützung findet) angelehnt. Postscript galt als zu komplex und unsicher für den Austausch von Dokumenten, sodass ursprünglich viele Funktionen entfernt wurden, um ein möglichst einfaches Format zu bekommen. Allerdings wurde dieses Format dann über die Jahre immer wieder erweitert um beispielsweise Links einbetten zu können oder Formulare auszufüllen. Dieses schrittweise Erweitern artete zusehends aus, und mittlerweile können vollständige Applikationen oder sogar Audio und Video in einem Dokument enthalten sein. Durch solche Inhalte lässt sich das Dokument dann weder 1:1 ausdrucken, oder auf den meisten E-Readern und Smartphones nutzen.

Die Abschlussveranstaltung bestand nebst dem gerechtfertigten Dank an alle freiwilligen Helfer und Vortragenden, auch aus etlichen Statistiken rund um den diesjährigen Kongress. Von Daten über Besucherzahlen und deren Konsum bis hin zur Auslastung der Internetanbindung, wurden alle Statistikbegeisterten ordentlich versorgt.

Todmüde von vielen Tagen mit viel zu wenig Schlaf war es dann zu Silvester Zeit die Heimreise vom in eine tiefe Schneedecke gehüllten Berlin zu den grünen Wiesen in Tirol anzutreten.

Mein besonderer Dank gilt BI International, welche mir dank großzügiger finanzieller Unterstützung dieses Jahr die Teilnahme am Congress ermöglichten.