

3/2009

www.dud.de

DuD

Datenschutz und Datensicherheit

Recht und Sicherheit in
Informationsverarbeitung
und Kommunikation

Schwerpunkt:
Open Source

Christoph Wegener

Verinice

Alexander Koderman

Datenschutzkontrolle durch
Open-Source

Jan Schallaböck

CrypTool – Ein Open-Source-Projekt
in der Praxis

Bernhard Esslinger

Bernhard Esslinger

CrypTool – Ein Open-Source-Projekt in der Praxis

Erfahrungsbericht eines erfolgreichen Open-Source-Projektes

Nur wenige Open-Source-Projekte können auf einen Entwicklungszeitraum von mehr als 10 Jahren zurückblicken. CrypTool ist ein solches Projekt und hat das gesamte Spektrum von unternehmensinterner Entwicklung über Freeware zu Open-Source erlebt. Wie hat sich CrypTool zu einem erfolgreichen Open-Source-Projekt entwickelt?

Hintergrund

Open-Source-Software hat sich in den letzten Jahren auch im Unternehmenskontext immer mehr zu einer ernstzunehmenden Alternative gegenüber kommerziellen Produkten oder Eigenentwicklungen etabliert.

Die Anzahl an Projekten sowie Codezeilen aus Open-Source-Projekten weisen ein exponentielles Wachstum auf [Deshpande, Riehle 2008]. Bekannte Beispiele wie der Apache Webserver, der Internet Browser Mozilla Firefox oder das Betriebssystem Linux verdeutlichen, dass auch komplexe und zugleich qualitativ hochwertige IT-Systeme als Open-Source-Projekte kontinuierlich von einer Vielzahl von Entwicklern weiterentwickelt und verbessert werden.

Die Vorteile von Open-Source-Projekten sind offensichtlich: Einsatz freiwilliger Entwickler sowie eine oftmals höhere Qualität der Ergebnisse durch hohe Eigenmotivation der Beteiligten und der fortwährenden Einbeziehung von Benutzern bei der Entwicklung.

Daher erscheint es speziell vor dem Hintergrund immer kostenintensiverer interner Entwicklungsprojekte oftmals sehr attraktiv, einzelne Applikationen als Open-Source-Projekt durch- bzw. weiterzuführen.

Doch bei all den genannten Vorteilen sollte nicht außer Acht gelassen werden, dass der überwiegende Teil von Open-Source-Projekten schon nach einigen Monaten stark vernachlässigt wird. Mit Ausnahme der bekannten Großprojekte sind viele Open-Source-Projekte inaktiv oder verlaufen wenig erfolgreich [Chengalur-Smith, Sidorova 2003].

Denn verteilte Open-Source-Projekte stellen besondere Anforderungen bezüglich Motivation der Teilnehmer. Der Kommunikations- und Koordinationsaufwand eines Open-Source-Projektes ist daher in der Regel deutlich höher als bei vergleichbaren Eigenentwicklungen.

Welche Faktoren führen zu einem erfolgreichen Open-Source-Projekt? Hierzu werden im Folgenden die Erfahrungen aus dem Open-Source-Projekt CrypTool näher betrachtet. Es wird aufgezeigt, welche Kriterien im Rahmen des CrypTool-Projektes als erfolgskritisch angesehen werden.

Verfahren anwenden und analysieren, um dem Anwender grundlegende und fortgeschrittene Konzepte der Kryptologie praktisch zu verdeutlichen.

Die Entwicklung von CrypTool begann 1998 im Rahmen einer IT-Sicherheits-Initiative zur betrieblichen Ausbildung bei der Deutschen Bank. Ab 2000 wurde CrypTool als Freeware zur Verfügung gestellt und beispielsweise 2002 auf der Bürger-CD des Bundesamts für Sicherheit in der Informationstechnik (BSI) „Sicher ins Internet“ verteilt [Esslinger, DuD 2002]. Heruntergeladen werden kann CrypTool auch von der BSI-Seite zur Internetsicherheit [BSI für Bürger]. Erst 2003 erfolgt der Übergang zu einem internationalen Open-Source-Projekt [Südmeyer, Esslinger 2008].

CrypTool ist somit nicht als ein reines Open-Source-Projekt gestartet, sondern wurde von einer unternehmensinternen Entwicklung über den Freeware-Status in ein Open-Source-Projekt überführt [CrypToolPräs 2008]. Durch diesen Übergang ließen sich die Unterschiede sowie die Vor- und Nachteile bei Entwicklung sehr genau beobachten.



Prof. Bernhard Esslinger

Direktor Deutsche Bank, Professor für IT Security und Kryptologie,

Universität Siegen

E-Mail: esslinger@fb5.uni-siegen.de

Das CrypTool-Projekt

Ziel des CrypTool-Projektes ist die Entwicklung der E-Learning Applikation CrypTool für die Bereiche Kryptographie und Kryptoanalyse. Mit Hilfe von CrypTool lassen sich viele kryptographische

CrypTool im Überblick

- ◆ *Webseite:* www.cryptool.org
- ◆ *Anwendung:* Kryptologie-Ausbildung in Firmen und Universitäten weltweit
- ◆ *Ursprung:* 1998 als Awareness-Initiative und Kooperation der Deutschen Bank mit verschiedenen Universitäten

Abb. 1 | Einordnung von Kryptologie in den unternehmensbezogenen und wissenschaftlichen Kontext



- ◆ **Hauptsponsor:** Deutsche Bank
- ◆ **Hosting:** SourceForge, Universität Darmstadt, Universität Duisburg-Essen
- ◆ **Lokalisierung:** Universität Madrid, Universität Warschau
- ◆ **Verbreitung:** weltweit; mehr als 50.000 Downloads pro Jahr
- ◆ **Projekt-Mitwirkende momentan:** 45
- ◆ **Releaseversion:** CT 1.4.30 (C++)
- ◆ **Weiterentwicklung nur in**
 - ◆ JCT 1.0 (Java, Eclipse RCP, SWT)
 - ◆ CT 2.0 (C#, .NET, WPF)

Allgemeine Erfahrungen

CrypTool war zunächst Ergebnis eines unternehmensinternen Entwicklungsprojektes. Die Anwendung wurde von vielen Mitarbeitern genutzt, aber für die Einsatzzwecke innerhalb des Unternehmens war eine Weiterentwicklung nicht mehr erforderlich. Aufgrund des bisherigen Engagements der Entwickler wollte man CrypTool aber auch ohne finanzielle Unterstützung weiterleben lassen, und deshalb entschied man sich, CrypTool als Freeware der Öffentlichkeit zur Verfügung zu stellen.

Der Übergang zu Freeware gestaltete sich zunächst schwierig, denn es gab zahlreiche rechtliche Probleme, wie z.B. Exportrestriktionen für verschiedene kryptografische Verfahren. Zudem beinhaltet CrypTool eine Reihe von Bibliotheken von kommerziellen Anbietern (z.B. Secude

oder Cryptovision) sowie einzelne patentierte Verfahren (z.B. IDEA-Verschlüsselung). Auch die Qualität des Source-Codes sprach zunächst gegen einen Übergang zu Open-Source.

Die Erfahrungen nach dem Übergang zu Freeware waren durchweg positiv und belohnten den zusätzlichen Aufwand. Zahlreiche Anwender schickten Verbesserungsvorschläge oder informierten über Applikationsfehler, was zu einer kontinuierlichen Verbesserung von CrypTool durch die bis dahin weitgehend geschlossene Entwicklergruppe führte. Darüber hinaus stellte die Veröffentlichung auch für das Unternehmen einen Nutzen dar, denn neben dem Image-Gewinn wurden auch mehr IT-Experten auf den „ursprünglichen Sponsor“ aufmerksam.

Problem Open-Source-Lizenzen

- ◆ Die Unterschiede der Lizenzen sind für Nicht-Juristen nicht leicht nachvollziehbar. Aus Entwicklersicht gibt es zu viele verschiedene Lizenzen [Open-Source-Lizenzen].
- ◆ Bei CT1 wurde mit der GNU General Public License Version 2 (GPL 2) die damals verbreitetste und bekannteste Lizenz gewählt.
- ◆ CT2 nutzt die Apache 2-Lizenz. Diese Entscheidung fiel aus folgenden Gründen: Die GPL 2 hat den Nachteil, dass man die *.exe nur gegen solche Bibliotheken linken darf, die ihrerseits unter der GPL stehen. Das

hätte strenggenommen bedeutet, dass alle Plugins auch die GPL hätten verwenden müssen. Die Apache-Lizenz erlaubt es, auch Plugins anderer Lizenzen zu laden. Desweiteren darf zwar jeder den CrypTool-Code nach Belieben verändern und weiterverwenden, aber nur die ursprüngliche Version darf „CrypTool“ im Namen tragen. Sollte also jemand basierend auf dem bestehenden CrypTool-Code eine eigene Anwendung entwickeln, dann ist das erlaubt, aber das Programm darf keine Namensähnlichkeit mit „CrypTool“ haben. Die Apache 2-Lizenz wird von der Free Software Foundation (FSF) als Lizenz für freie Software anerkannt und ist zu der GPL Version 3 kompatibel.

- ◆ JCT (JCT) wurde ursprünglich auch unter der GPL 2 lizenziert. Mit Milestone 2 entschloss sich das Team, zur Eclipse Public License (EPL) Version 1.0 zu wechseln. Hauptgrund dafür war, eine möglichst hohe Konformität zu den Eclipse-Standards zu erzielen. Alle offiziellen Eclipse-Projekte (d.h. alle bei der Eclipse Foundation geführten Projekte) müssen unter der EPL veröffentlicht werden – eine Möglichkeit, die sich JCT für die Zukunft offen halten will. Ein Großteil der JCT-Plugins wird ebenfalls unter dieser Lizenz veröffentlicht. Die EPL ist sowohl von der Open Source Initiative (OSI) als auch von der Free Software Foundation (FSF) anerkannt.

Nach drei Jahren als Freeware wurde CrypTool 2003 schließlich zu einem Open-Source-Projekt. Während Firmen und Universitäten CrypTool bereits als Freeware einsetzten, wurde erst durch Open-Source die direkte Mitwirkung und Integration von freiwilligen Entwicklern möglich. Der Open-Source-Ansatz verbesserte insbesondere die Zusammenarbeit mit Universitäten, so dass im Rahmen von Seminar- oder Diplomarbeiten zahlreiche Erweiterungen für CrypTool entwickelt wurden. Auch das Hosting des Projektes wurde von der Universität Darmstadt übernommen. Des Weiteren lieferten Universitäten konkrete Vorschläge zur Verbesserung der Benutzerschnittstelle (z.B. experimentelle User-Interfaces von der Uni Koblenz und der FH Aachen). Die

kommerziellen Bibliotheken sind immer noch als Closed-Source in CrypTool 1.4.x enthalten (mit Ausnahme der notwendigerweise offenen Header-Dateien). Auch wenn dies nicht ganz dem Sinn des Open-Source-Gedankens entspricht, ist dies ein pragmatisches Vorgehen: Der Funktionsumfang lässt sich professionell erweitern und die Anbieter stellen die Dateien zur Nutzung in Verbindung mit CrypTool kostenlos zur Verfügung.

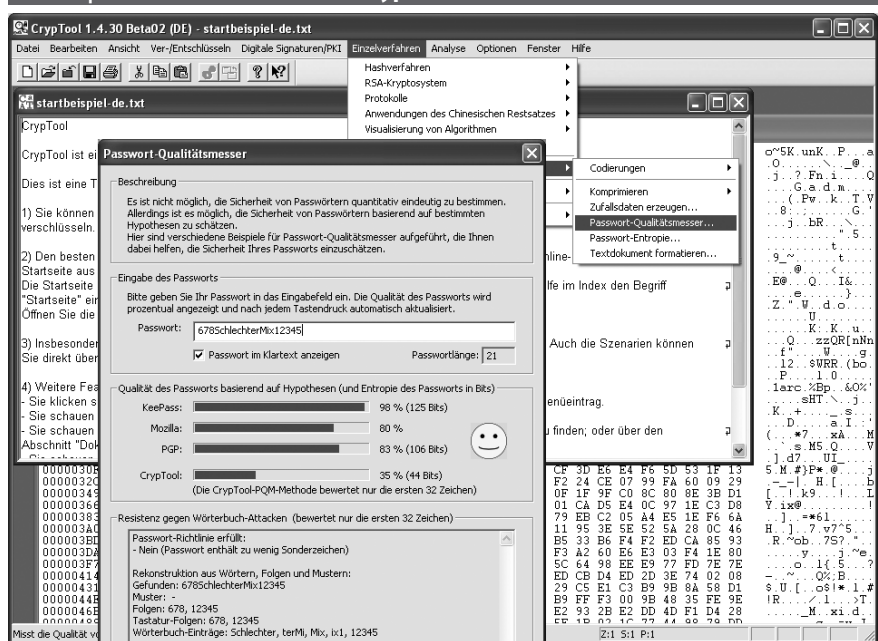
Die aktuelle CrypTool-Weiterentwicklung erfolgt in zwei parallelen Entwicklungsprojekten: JcrypTool (JCT, basierend auf Java, Eclipse RCP und SWT) sowie CrypTool 2 (CT2, basierend auf C#, Visual Studio 2008 Express und WPF) [JcrypTool][CrypTool 2].

Hintergrund der zwei Projekte war in erster Linie ein erforderlicher Technologiewechsel, denn CrypTool 1.4.x basierte auf der veralteten GUI-Bibliothek Microsoft Foundation Classes (MFC) und genügte nicht mehr den Anforderungen des Projektes. Daher wurde auf moderne Entwicklungsumgebungen gewechselt, die für die verteilte Entwicklung besser geeignet waren. Ferner konnte man sich durch den Wechsel auch an der aktuellen IT-Ausbildung in Unternehmen und an Universitäten ausrichten und somit mehr Entwickler ansprechen. Ein wichtiger Aspekt war die kostenlose Verfügbarkeit der Werkzeuge, um keine zusätzliche Barriere für Entwickler aufzubauen.

Zudem wurde über die CrypTool-Webseite eine Umfrage durchgeführt, bei der sich 40% der Befragten für C# und .NET und 40% für Java und Eclipse entschieden. Die Entscheidung deckt sich auch mit aktuellen Arbeitsmarktuntersuchungen (Januar 2009), die zeigen, dass vor allem Experten für Java und C#.NET gesucht sind [Heise-Meldung 2009].

Auch wenn die Spaltung in zwei Projekten zunächst problematisch erscheinen mag, haben sich durch die parallele Entwicklung viele gute Ideen ergeben, die häufig in den jeweils anderen Entwicklungsstrang übernommen werden konnten. Da die langfristigen CrypTool-Architekten in beiden Projekten aktiv sind, ist sichergestellt, dass insbesondere die konzeptionellen Verbesserungen auch zwischen den Entwicklungssträngen ausgetauscht werden. Außerdem waren die meisten freiwilligen Entwickler nur einer Entwicklungsumgebung zugeneigt, so dass die Wahl nur einer Plattform voraus-

Abb. 2 | Die aktuelle Version von CrypTool 1



sichtlich zu einem größeren Verlust von Entwicklern geführt hätte.

Wirtschaftlich gesehen wären zwei parallele Projekte im Unternehmenskontext schwer durchsetzbar; als Open-Source-Projekte aber sind sie eher gewinnbringend und ermöglichen es, mit verschiedenen Umgebungen und unterschiedlichen Ansätzen zu experimentieren.

Schätzung Mannjahre und Gesamtwert

- ♦ Laut <http://www.ohloh.net/p/8247> wird das bisherige Projekt CT1 anhand seiner Sourcen auf einen Wert von 8 Millionen USD und auf einen Aufwand von 146 Personenjahren geschätzt (überbewertet).
- ♦ Wie sehr man an solchen Schätzungen aufgrund der puren Source-Code-Betrachtung zweifeln kann, sieht man daran, dass in CrypTool 1 real bisher rund 40 Personenjahre flossen; und dass andererseits Projekte wie Firefox total unterbewertet sind.

Erfolgsfaktoren

Was hat dazu geführt, dass das CrypTool-Projekt immer noch aktiv ist? Was sind die kritischen Erfolgsfaktoren für ein erfolgreiches Open-Source-Projekt?

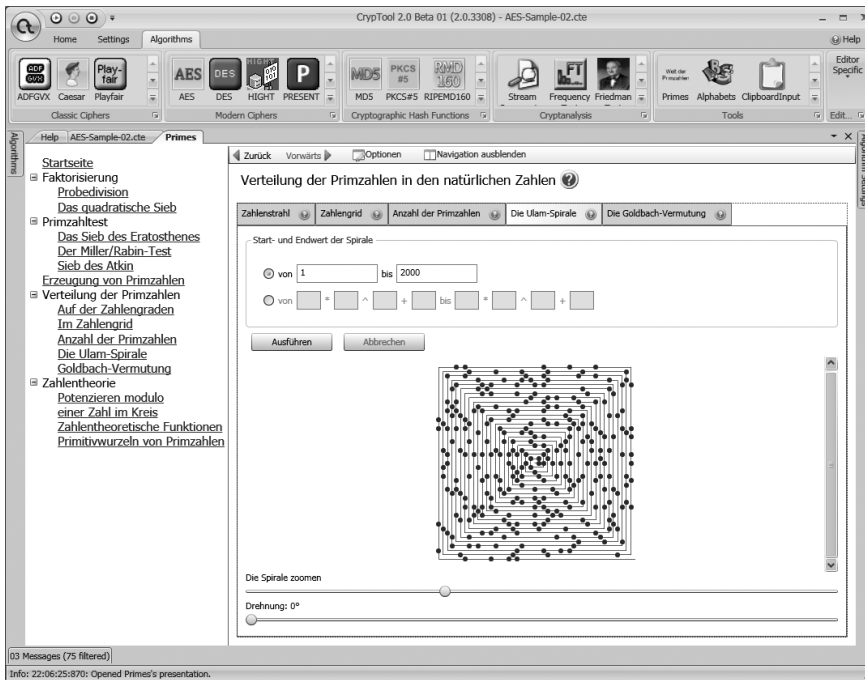
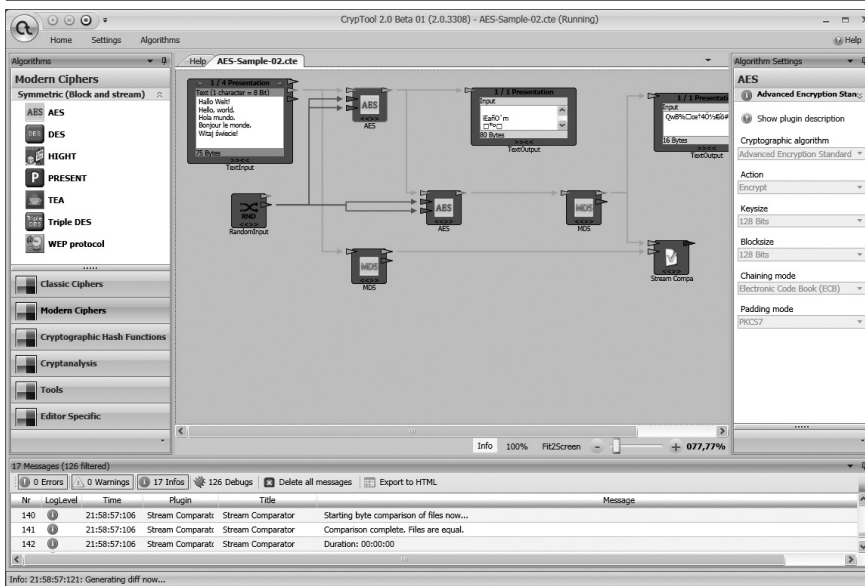
Generelle Motivation für das CrypTool-Projekt

Eine zentrale Fragestellung von Open-Source bezieht sich auf die Motivation, sich zumeist ehrenamtlich an einem Open-Source-Projekt zu beteiligen und daran nachhaltig mitzuwirken. In diesem Umfeld existieren bereits zahlreiche empirische Untersuchungen – eine Übersicht findet sich unter anderem in [Stoll 2006].

Als maßgebliche Motivation werden in den aufgeführten Studien zumeist der Erwerb und die Entwicklung von spezifischem Fachwissen genannt. Auch im Rahmen des CrypTool-Projektes steht das thematische Interesse an Kryptographie und Kryptoanalyse eindeutig im Vordergrund. Die Kryptologie umfasst eine Vielzahl von Verfahren und Methoden – von der klassischen Caesar-Verschlüsselung bis hin zu modernen Verfahren wie RSA, AES oder Gitterbasenreduktion. Die Kryptologie ist eine Basistechnologie für Datenschutz und Datensicherheit und somit eine wesentliche Komponente für das grundlegende Verständnis von IT-Sicherheit.

Für die Entwickler besteht die Herausforderung, die teils sehr komplexen Verfahren einerseits korrekt zu implementieren und andererseits geeignet zu visualisieren, um sie auch Laien verständlich zu machen. Bei der Implementierung der Verfahren wird das fachliche Wissen vertieft, wobei die zahlreichen Experten innerhalb des Projektes insbesondere bei

Abb. 3 | Die aktuelle Beta-Version von CrypTool 2



Software-Engineering-Problemen Hilfestellung leisten.

Ein weiterer wesentlicher Anreiz für neue Entwickler besteht in der freien Auswahl einer aktuellen Software-Entwicklungsumgebung. Einige Entwickler nutzen das CrypTool-Projekt, um sich mit einer der beiden aktuellen Entwicklungsumgebungen (in diesem Fall Microsoft Visual Studio oder Eclipse) vertraut zu machen. Die intrinsische Motivation „Freude am Programmieren“ wird dabei durch den Erwerb von Fachkenntnissen moderner verteilter Entwicklungssysteme

(verbunden mit entsprechenden Karriere-chancen) flankiert.

Zahlreiche Entwickler stoßen durch Diplom- oder Seminararbeiten zum CrypTool-Projekt. Hintergrund ist neben der praktischen Implementierung auch der Vorteil der Integration in eine bereits bestehende Umgebung sowie der Nutzen, dass die Ergebnisse der wissenschaftlichen Arbeit innerhalb des Projektes langfristig erhalten bleiben und weiterentwickelt werden.

Der zusätzliche Aufwand, sich in das Projekt einzuarbeiten, wird dabei durch das wertvolle Feedback von Experten be-

lohnt, wodurch die Qualität der eigenen Arbeit steigt. Oftmals ist ein gewisses Maß an Kritikfähigkeit seitens des Entwicklers erforderlich. Außerdem stellte sich heraus, dass solche wissenschaftlichen Arbeiten meist eine deutlich höhere Qualität und Relevanz hatten, so dass diese Studenten/Doktoranden danach sehr leicht eine entsprechende Anstellung fanden.

Freiheitsgrade versus Richtlinien

Ein wesentliches Motiv der Mitarbeit von freiwilligen Entwicklern an einem Open-Source-Projekt ist die Freiheit bei der Implementierung von Funktionalitäten, sowohl in technischer als auch in zeitlicher Hinsicht. Damit diese Freiheiten nicht zu einem kreativen Chaos führen und damit sich nach einer gewissen Zeit auch vorzeigbare Ergebnisse einstellen, sind Richtlinien unabdingbar.

Technologisch basiert CrypTool auf einem offenen Framework-Ansatz, der es den Entwicklern ermöglicht, so genannte Plugins zu entwickeln, die in die Gesamtanwendung relativ einfach aufgenommen werden können. Plugins stellen z.B. die Funktionen eines Verschlüsselungsverfahrens zur Verfügung. Dieser Ansatz ermöglicht es, spezifische Implementierungen von kryptographischen Verfahren unabhängig zu entwickeln und später in das Gesamtprojekt zu integrieren. Es hat sich gezeigt, dass hierdurch Entwickler mit relativ wenig Einarbeitungsaufwand an dem Projekt mitarbeiten können. Durch die Erfahrungen bei der Implementierung eines Plugins gewinnen die Entwickler zudem Verständnis für die Gesamtarchitektur und können sich dadurch für die Weiterentwicklung der eigentlichen Core-Anwendung qualifizieren. Der Plugin-Ansatz bietet darüber hinaus den Vorteil, die Implementierung unabhängig von der Entwicklung der Core-Anwendung zu planen, so dass die Release-Planung sich im Wesentlichen auf die Core-Anwendung bezieht und die zum Zeitpunkt verfügbaren Plugins in das Gesamtpaket integriert werden. Natürlich gibt es in den Projekt-Wikis Dokumente und Tabellen, die die gewünschten/fehlenden Funktionen auflisten und priorisieren.

Hat ein Anwender eine bestehende Core-Anwendung installiert, kann er mit Hilfe der eingebauten Update-Funktion neu entwickelte Plugins jederzeit nachladen.

Projektorganisation und Projektmanagement

Der organisatorische Aufbau ist in vielen Open-Source-Projekten sehr ähnlich und gleicht einem typischen Softwareentwicklungsprojekt.

Auch im CrypTool-Projekt besitzt der Projektleiter eine tragende Rolle. Da der Erfolg des Projektes maßgeblich von der Motivation der freiwilligen Entwickler abhängig ist, ist es die primäre Aufgabe der Projektleiter, die Projektmitarbeiter langfristig zu motivieren. Dazu ist es insbesondere notwendig, bei etwaigen Problemen oder Fragen verlässlich und zeitnah zu reagieren, damit keine Missverständnisse entstehen. Speziell für neue Mitglieder stellt das Projekt zunächst ein recht anonymes Konstrukt dar. Deshalb werden Anfragen schnell beantwortet, wodurch die Projektleitung eine hohe zeitliche Verfügbarkeit erbringen muss.

In den Anfängen als Open-Source-Projekt wurde versucht, Aufgaben möglichst stark zu dezentralisieren und Anfragen direkt an das gesamte Team weiterzuleiten. Allerdings wurden damit keine guten Erfahrungen gemacht, denn dieser sehr dezentrale Kommunikationsansatz führte oftmals zu verzögerten oder auch widersprüchlichen Antworten. Beim CrypTool-Projekt hat sich herausgestellt, dass der Projektleiter somit nicht nur einen guten Überblick über den Stand der Module sowie über die Kenntnisse der Entwickler haben muss, sondern auch bei technischen Fragestellungen als erste Anlaufstelle Auskunft erteilen kann.

Um die Aufgaben besser aufzuteilen bestehen derzeit Überlegungen, für einzelne Kategorien (z.B. klassische oder moderne Verschlüsselungsverfahren) Teilprojektleiter zu etablieren. Dies soll zum einen die Kommunikation und Entscheidungsfindung effizienter gestalten und zum anderen auch zur Motivation und Anerkennung der bisherigen Leistungen beitragen.

Ein wesentlicher Erfolgsfaktor im CrypTool-Projekt ist das Zusammenspiel verschiedener Talente. So finden sich neben Architekten und Entwicklern auch zahlreiche Experten in den Gebieten Mathematik, Kryptologie, Software-Engineering und Webdesign. Aufgabe des Projektleiters ist es eine effektive Kooperation der Projektmitarbeiter zu gewährleisten und dabei auch ehemalige Entwickler langfristig an das Projekt zu binden, um eine problemlose Fehlerbehebung zu ermöglichen.

Abb. 4 | Die aktuelle Beta-Version von JCrypTool



Im CrypTool-Projekt stehen zahlreiche ehemalige Entwickler dem Projekt weiterhin beratend zur Verfügung.

Eine besondere Herausforderung sind in vielen Projekten die eher unliebsamen Aufgaben. Hierzu zählt in erster Linie die Dokumentation der Ergebnisse. Hier hat sich gezeigt, dass eine klare Aufgabenzuordnung schon im Vorfeld helfen kann. So ist jeder Entwickler angehalten, seinen Code entsprechend zu dokumentieren.

Grundsätzlich lassen sich die Anforderungen hinsichtlich der Organisation so

wie des Managements eines Open-Source-Projektes wie CrypTool mit einem normalen größeren Softwareentwicklungsprojekt vergleichen. Vorhandene Erfahrungen im Bereich Projektmanagement erweisen sich auch bei Open-Source-Projekten als überaus wichtig, wobei die Aspekte Motivation und Kommunikation im Kontext von Open-Source eine noch zentralere Rolle spielen.

Agile Software

◆ Erfolgreiche verteilte Open-Source-Projekte haben meist auch eine agile Software-Entwicklung, ohne dies explizit mit Entwicklungswerkzeugen zu erzwingen: Der gesamte SW-Entwicklungsprozess wird immer wieder in kurzen Zyklen durchlaufen, um schnell neue Versionen lauffähiger Software bereit zu stellen, anhand deren sich überprüfen lässt, ob die Anforderungen erfüllt werden.

Interne und externe Kommunikation

Eine effektive und effiziente interne sowie externe Projektkommunikation ist ein kritischer Erfolgsfaktor für das CrypTool-Projekt.

Für die interne Kommunikation wird im JCrypTool-Projekt primär E-Mail verwendet. Das CrypTool2-Projekt hingegen hat mit einem offenen Skype-Chat-Kanal sehr gute Erfahrungen gemacht. Aufgrund der recht überschaubaren Projektgröße werden klassische Diskussionsforen nahezu gar nicht verwendet.

Darüber hinaus existieren auch ein Wiki sowie eine Projektwebseite: Diese dienen allerdings in erster Linie zur externen Kommunikation, um Anwendern und Entwicklern einen Überblick über das Projekt und das Team zu geben und um die Dokumentation (z.B. allgemeine FAQs oder Richtlinien für die Entwicklung) zentral zur Verfügung zu stellen [JCrypTool][CrypTool 2].

Als sehr effektiv haben sich Projekttreffen erwiesen. Allerdings ist es in der Regel sehr schwierig, einen Termin für das verteilte Team zu finden. Daher werden die Treffen primär dazu benutzt, um die Release-Planung und langfristige Architektur-Entscheidungen abzustimmen. Die Treffen sind aber auch sehr wichtig für die Förderung des Gemeinschaftsgefühls („Community Building“), da sich die Beteiligten ansonsten lediglich elektronisch miteinander austauschen.

Bei der internen Kommunikation hat sich, wie auch bei vielen anderen Open-Source-Projekten, Englisch als Projektsprache durchgesetzt, obgleich der Großteil der Entwickler aus Deutschland kommt.

Bei langfristigen Open-Source-Entwicklungsprojekten wie CrypTool ist es notwendig, kontinuierlich neue Projektmitarbeiter für das Projekt zu gewinnen

und möglichst dauerhaft zu binden. Eine erfolgreiche externe Kommunikation steht hierfür im Vordergrund.

Das Projekt versucht durch zahlreiche Veröffentlichungen und Vorträge, aber auch durch Mitarbeit bei Mathematik- und Informatik-Lehrgängen für interessierte und begabte Schüler, CrypTool bekannter zu machen und damit zusätzliche Anwender aber vor allem Entwickler anzusprechen. Wie erfolgreich die externe Kommunikation ist, lässt sich in der Regel an den Zugriffen auf der Webseite bzw. den Download-Zahlen messen. So steigen die Download-Zahlen beispielsweise nach einer Mitteilung der Verfügbarkeit einer neuen CrypTool-Version auf dem in der deutschen IT-Szene beliebten Heise Newsticker signifikant an und das Team erhält zahlreiches Feedback. Neben einer ansprechenden Webseite ist vor allem das zeitnahe Beantworten von Anfragen nicht nur für Entwickler, sondern natürlich auch für Anwender wichtig und sorgt für positive Mund-zu-Mund-Propaganda.

Das CrypTool-Projekt hat auch erfolgreich bei einer Reihe von Wettbewerben teilgenommen. So wurde CrypTool unter anderem mit dem European Information Security Award und dem NRW IT-Sicherheitspreis ausgezeichnet. Darüber hinaus wurde CrypTool im Rahmen der bundesweiten Initiative „Deutschland - Land der Ideen 2008“ als ausgewählter Ort geehrt.

Für die Rekrutierung neuer Entwickler sind die Auszeichnungen und Veröffentlichungen aber nur bedingt nützlich, da das Thema Kryptologie sehr spezifisch ist und in der Regel nur einen kleinen Anwenderkreis direkt anspricht.

Wichtiger ist dagegen, dass CrypTool an vielen Universitäten im Rahmen der Lehre eingesetzt wird, wie z.B. der Jahresbericht der London Royal Holloway University dokumentiert [RoyalHolloway 2008]. An Hochschulen erfolgt die primäre Rekrutierung von neuen Entwicklern über Seminar- oder Diplomarbeiten. In diesem Kontext lassen sich Verfahren als Plugin realisieren, wobei Entwickler auf eine vorhandene Infrastruktur bzw. Rahmenanwendung aufbauen können, um schneller zu nutzbaren Ergebnissen zu kommen und sich bei der Implementierung auf den eigentlichen Algorithmus fokussieren zu können. In Hinblick auf die erreichbare Zielgruppe hat es sich für das CrypTool-Projekt als sehr hilfreich erwiesen, Universitäten bzw. die entsprechenden Lehrstühle direkt anzusprechen und Koopera-

tionen anzubieten. So entstand die polnische CrypTool-Version durch die Universität Warschau und die spanische Version durch die Universität Madrid, wobei die Universitäten von sich aus auf das CrypTool-Projekt zukamen, um ihren Studenten eine bessere Lernumgebung auch in der Landessprache anbieten zu können.

Technische Infrastruktur

Wie bei jedem Open-Source-Projekt bedarf es einer technischen Infrastruktur, die eine effiziente verteilte Entwicklung ermöglicht.

Neben dem wohl bekanntesten Open-Source-Hosting bei SourceForge existieren zahlreiche kostenlose Alternativen –z.B. von Google (Google Code) oder Microsoft (CodePlex). Diese Anbieter stellen verschiedene Funktionalitäten zum Management der Projekte zur Verfügung [Open-Source-Hosting]. Hierzu zählen neben dem reinen Hosting des Source-Codes auch Dienste für Web-Hosting, Wiki, Tracker, Mailing-Lists oder Foren.

Die neuen CrypTool-Projekte werden bei SourceForge [JCrypTool] sowie bei der Universität Duisburg-Essen [CrypTool2] gehostet.

Als Versionskontrollsystem wird Subversion verwendet. Die Konfiguration des Systems ist bedingt offen gehalten (anonymer Lese- und Downloadzugriff für jedermann, Schreibzugriff nur für benannte Accounts), um einerseits möglichst unbürokratisch Änderungen zu übernehmen, aber andererseits die vorhandene Code-Basis nicht durch fehlerhafte Nutzung zu gefährden.

Ausblick

Der Übergang von einer unternehmensinternen Entwicklung zu einem Open-Source-Projekt ist für CrypTool sehr vorteilhaft gewesen. Durch die internationale Verfügbarkeit haben sich zahlreiche Kooperationen mit Universitäten im In- und Ausland entwickelt, und es konnten zusätzliche Entwickler für das Projekt gewonnen werden.

Doch die Übergabe der Entwicklung an die Open-Source-Gemeinschaft ist kein Selbstläufer. Für den langfristigen Erfolg eines Open-Source-Projektes gilt es neben der generellen Motivation auch eine geeignete Umgebung zu schaffen, in der das Projekt leben und sich entwickeln kann.

Der dazu notwendige Aufwand ist nicht zu unterschätzen, und es bedarf neben Engagement und Erfahrung auch einer gewissen Geduld und Beharrlichkeit. Letztendlich kommt es wie in nahezu jedem Projekt in erster Linie auf die beteiligten Menschen an.

Literatur

[BSI für Bürger] – <http://www.bsi-fuer-buerger.de/toolbox/tools.htm>

[Chengalur-Smith, Sidorova 2003] – “Success and Survival of Open-Source Projects: A Population Ecology Perspective”, in Proceedings of the 24th ICIS

Anmerkung 1: Von den rund 180.000 (Stand August 2008) in SourceForge (SF) enthaltenen Projekten sind 95 % „nahezu tot“ (eine etwas strenge Bezeichnung für Projekte, die eine oder mehrere der folgenden Bedingungen erfüllen: Software wird nicht mehr gewartet (stays-as-it-is); Erstellung und letzte Änderung innerhalb eines Jahres; kein Update mehr seit Ende 2007; Funktionalität im Umfang einer Übungsaufgabe; Development Status: „1 – Planning“ oder „2 – Pre-Alpha“; keine Reaktion unter der angegebenen Mailadresse).

Anmerkung 2: Leider wurden viele Projekte eröffnet, ohne zu schauen, ob es schon etwas Ähnliches gibt, ohne darauf zu referenzieren und ohne zu versuchen, mit vorhandenen Projekten zu fusionieren, um den Benutzern einen höheren Wert zu bieten.

Anmerkung 3: JCT liegt am 22.01.09 unter den 180.000 Projekten auf SF-Rang 992, was für eine relativ hohe Aktivität spricht. Hierbei gibt es aber starke Schwankungen.

Anmerkung 4: Zu dem Suchbegriff „Cryptography“ liefert SF am 22.01.09 genau 65 Projekte.

[CrypToolPräs 2008] – Präsentation über das Gesamtprojekt CrypTool und seine Möglichkeiten, verfügbar auf <http://www.cryptool.org>

[CrypTool 2] – CrypTool 2-Projekt, <http://cryptool2.vs.uni-due.de/>

[Deshpande, Riehle 2008] – “The Total Growth of Open Source”, in Proceedings of the Fourth Conference on Open Source Systems (OSS 2008). Springer Verlag, 2008, Seite 197-209.

[Esslinger, DuD 2002] – „CrypTool -- spielerischer Einstieg in klassische und moderne Kryptographie. Neue Version - fundierte Awareness in Deutsch und Englisch“, erschienen in „DuD Datenschutz und Datensicherheit“, Ausgabe 10/2002, S. 615-618,

<https://www.cryptool.org/images/esslinger-dud10-2002.pdf>

[Heise-Meldung 2009] – Meldung vom 13.01.2009 <http://www.heise.de/newsticker/Experten-fuer-Java-und-C-Net-langfristig-gefragt--meldung/121615>

[JCrypTool] – JCrypTool-Projekt, Allgemeine Homepage: <http://jcryptool.sourceforge.net>, Projektseite: <http://sourceforge.net/projects/jcryptool>.

[Open-Source-Hosting] – Übersicht von Anbietern für Open-Source-Hosting, http://en.wikipedia.org/wiki/Comparison_of_free_software_hosting_facilities

[Open-Source-Lizenzen] – Übersicht bei Wikipedia, <http://de.wikipedia.org/wiki/Open-Source-Lizenz>

[RoyalHolloway 2008] – “Information Security Group” (ISG) der London Royal Holloway University, Review 07/08, Seite 4, http://www.isg.rhul.ac.uk/files/ISG_WebNews08.pdf.

[Shadow 2008] – „Kryptisch gesagt...“, erschienen in Eclipse Magazin Vol. 16, Ausgabe 4, 2008, http://www.trivadis.com/fileadmin/user_upload/PDFs/Trivadis_in_der_Presse/EclipseMagazin_Kryptisch_gesagt_Shadow.pdf

[Stoll 2006] – „Spaß und Software-Entwicklung – Zur Motivation von Open-Source-Programmierern, Empirische Untersuchungen zu Open-Source“, Seite 37, Universität Zürich 2006, <http://www.dissertationen.unizh.ch/2006/luthigerstoll/diss.pdf>

[Südmeyer, Esslinger 2008] – „VerSchlüsselerlebnisse NG“, erschienen in <kes> 2008#3, Seite 62-65, <https://www.cryptool.org/images/kes-2008.pdf>