DLR Projektträger Berlin
Eingegangen am:
24. März 2020
Eingegangen:

Richtlinie zum „Software-Sprint“

Dark Crystal

Schlussbericht

Zuwendungsempfänger:

Pegasus GbR

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen **01IS19S06** gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor.

Kurze Darstellung der Aufgabenstellung und Motivation

Was war Deine Motivation? Welches Problem wolltest Du mit Deinem Projekt lösen? Wie war die geplante Vorgehensweise zur Problemlösung (auch Angabe der wichtigsten Meilensteine)?

Die zunehmende Internetverfügbarkeit hat eine Verschiebung hin zu leichten Geräten mit geringer Leistung bewirkt, macht Nutzende jedoch immer mehr von ressourcenintensiven Zentralinfrastrukturen abhängig.

Peer-to-Peer-Systeme mit niedriger Bandbreite bieten eine vielversprechende ressourcenschonende Alternative. Das Problem des Schlüsselmanagements ist jedoch ein Hindernis für ihre Akzeptanz. Nutzende heute sind es gewöhnt, diese Verantwortung an zentrale Anbieter abzugeben.

Damit sich dezentrale Architekturen durchsetzen können, braucht es Lösungen für Probleme wie Geräteverlust oder -fehler und vergessene Kennwörter.

Mit unserem Projekt planten wir:

- die Erarbeitung einer transportagnostischen Protokollspezifikation für ein System zur Wiederherstellung kryptographischer Schlüssel;
- die Erstellung eines Entwickler-Toolkit zur Integration von Dark Crystal in vorhandene Projekte – mit Anleitungen, Methodenteil und Code-Modulen;
- die Erweiterung von Dark Crystal um die Funktion des Widerrufs und der Neuausgabe von Schlüsseln.

Beitrag des Projektes zu den Zielen der Förderinitative „Software-Sprint“

Wer ist die Zielgruppe für Deine Lösung? Wie profitiert sie von den Ergebnissen Deines Projekts? Welche Bezüge gibt es zu den Themenfeldern und Zielen des Software Sprints?

Unsere Zielgruppe sind Entwickler_innen, die ein Schüsselverwaltungssystem in ihre Software implementieren wollen.

Im Speziellen wendet sich Dark Crystal an Projekte, in denen die Schlüsselintegrität eine wichtige Rolle spielt. Dies ist in der Regel bei „distributed Systems“ der Fall, da sie ohne einen authentifizierten Server auskommen.

Diese Systeme sind vorteilhaft hinsichtlich der Datensicherheit, da Anwendende die volle Kontrolle über ihre Daten behalten. Sie schneiden auch aus einer ökologischen Sicht sehr gut ab, weil sie kollaborative Anwendungen ohne energieintensive Datenzentren ermöglichen.

Dark Crystal macht diese Systeme sicherer und leichter nutzbar und unterstützt damit deren Verbreitung.

Entwickelnde profitieren von unserer Arbeit durch die Veröffentlichung unseres Werkzeugkastens für Entwickler_innen, den wir frei zugänglich veröffentlichen. Neben unseren Open Source- Modulen enthält dieser Werkzeugkasten auch eine umfangreiche Dokumentation mit Anleitungen, Empfehlungen und Anwendungsbeispielen.

Wir haben darauf geachtet, diesen Werkzeugkasten so flexibel wie möglich zu gestalten. Daher haben wir an Stelle von festen Codes vor allem 'Design Muster' entwickelt, die in vielfältgen Situationen anwendbar sind.

Entwickelnde, die Dark Crystal benutzen, können daher unsere Ideen so umbauen und implementieren, wie es für die Besonderheiten ihres Projektes passt.

Das macht unser Projekt zukunftssicher im Hinblick auf neue Programmiersprachen und Technologien.

Ausführliche Darstellung der Ergebnisse

Welche konkreten Ergebnisse hast Du erzielt? Konnten alle Meilensteine erreicht werden? Welche zusätzlichen Erkenntnisse hast Du aus der Projektarbeit gewonnen, auch im Hinblick auf die Begleitung durch die Open Knowledge Foundation?

Wir haben:

- unser Prinzip zur Generierung und Verschlüsselung von Shares in einer allgemeingültigen Form formuliert und vom Transportprotokoll unabhängige Module in NodeJS entwickelt;
- einen allgemeingültigen Standard für unser Protokoll erstellt;
- Berichte über die sozialen und technischen Herausforderungen des Modells zur Verfügung gestellt;
- das Protokoll um ein System zur Sperrung und Neuausgabe von Schlüsseln mit BLS-Threshold-Signaturen erweitert.
- eine allgemeine Einführung zu unserem Konzept und seinen Hintergründen geschrieben.
- Anwendungsvorlagen für die verschiedenen Nachrichtentypen, die wir im Protokoll benutzen, veröffentlicht;
- einfache Erklärungen zu den wichtigsten von uns benutzten Verschlüsselungstechniken erstellt.
- ein Anwendungsbeispiel zur Erstellung einer Benutzungsoberfläche für einen Email- Klienten zur Verfügung gestellt, in welchem das Dark Crystal-Protokoll zur Sicherung der Verschlüsselung und zum Zeichnen von Schlüsseln implementiert ist.

Mit Hilfe von Design-Coaching Sitzungen mit Simply Secure, die von der Open Knowledge Foundation organisiert wurden, haben wir ein Dokument mit Empfehlungen für das Designen von Benutzungsoberflächen erstellt. Simply Secure haben selbst erst kürzlich zu Herausforderungen im Design bei dezentralisierten Systemen geforscht. Dies ist genau das Thema, welchem sich unser Projekt widmet. Das Coaching durch Simple Secure war daher für uns äußerst hilfreich.

Zielgruppe, Nutzen und mögliche Weiterentwicklungen

Welcher Nutzen ergibt sich für die Zielgruppe aus den Ergebnissen Deines Projekts? Welche weiter-gehenden Effekte ergeben sich aus der Open-Source-Stellung der Ergebnisse? Gibt es Ideen für die Weiterentwicklung Deiner Lösung und Pläne zu deren Umsetzung? Hat die Arbeit in dem Projekt Dich in Deiner persönlichen, fachlichen Weiterentwicklung unterstützt?

Mehrere Softwareprojekte haben bereits ihr Interesse daran bekundet, unser System der Schlüsselwiederherstellung in ihrem Projekt zu verwenden.

In unserem nächsten Projekt, welches in Kürze beginnt, werden wir mit „Briar“ zusammen arbeiten, einer mobilen Nachrichten-App mit Schwerpunkt auf Datenschutz und Schutz der Privatssphäre, um ein System zur

Schlüsselwiederherstellung und „remote Wipe“ in deren Anwendung einzubringen. „Briar“ wurden in der Vergangenheit ebenfalls durch Software-Sprint unterstützt.

Wir haben durch das Projekt viel dazugelernt, vor allem über Aspekte des Designs durch die von der Open Knowledge Foundation organisierten Coaching-Sessions.

Wir haben auch durch das Schreiben des Berichtes und der Module zu den Treshold-Signaturen viel gelernt. Dies war der stärker experimentelle Teil des Projektes, welcher aus einem Anfang 2019 veröffentlichten Forschungspapier entstanden ist, an dem wir mitgeschrieben haben. Dieser Teil beinhaltete die Arbeit an einem für uns neuen Verschlüsselungssystem und die Zusammenarbeit mit Entwickelnden, mit denen wir bisher noch keinen direkten Kontakt hatten. Dieser Teil des Projektes war für unsere persönliche Entwicklung besonders spannend und förderlich.

Kurze Darstellung der Arbeiten, die zu keiner Lösung geführt haben

Gab es Arbeiten bzw. Lösungsansätze, die nicht weiter verfolgt wurden? Was waren die Hinter-gründe, und wie bist Du alternativ vorgegangen?

Das Schlüsselneuausgabesystem auf der Basis von Threshold-Signaturen war der eher experimentelle Teil dieses Projektes und wir sind sehr dankbar für die Möglichkeit, daran zu arbeiten. Wir haben im geförderten Zeitraum dazu ein funktionierendes Modell entwickelt und eine Beschreibung geschrieben. Dennoch ist dieser Teil des Projektes weiterhin weniger stabil und befindet sich in der Testphase. Hier ist noch Arbeit nötig, bevor es einem breiteren Publikum empfohlen werden kann.

Kurze Angabe von Präsentationsmöglichkeiten für mögliche Nutzer

Wo können sich Interessenten detailliert über Deine Projektergebnisse informieren (z.B. Webseite, GHitHub, Veröffentlichungen)?

Die schriftliche Komponente des Werkzeugkastens für Entwickelnde ist über eine einfache Webseite unter folgendem Link verfügbar:

https://dark-crystal.gitlab.io/

Der Quellcode aller unserer Code- Module und unsere verschriftlichtlichten Forschungsergebnisse, alle veröffentlicht unter der Affero General Public License version 3, finden sich unter folgendem Link:

https://gitlab.com/dark-crystal

Kurze Erläuterung zur Einhaltung der Arbeits- und Kostenplanung

Gab es im Projektverlauf Ereignisse, die eine Anpassung der Planung erforderlich machten – z.B. Mehr- oder Minderaufwand bei der Bearbeitung von Teilaufgaben?

Natürlich ist es immer der Fall, dass bestimmte Dinge länger dauern als geplant etwa aufgrund von Fehlern im Code oder anderen Schwierigkeiten.

Aufgrund unserer personellen Verfügbarkeit und aus sonstigen persönlichen Gründen haben wir die Abfolge der Teile unseres Projektes gegenüber dem ursprünglichen Ablauf verändert. Wir haben die Arbeit an den Threshold-Signaturen zuerst abgeschlossen und anschließend an der Schlüsselwiederherstellungskomponente gearbeitet.

Die regelmäßigen Anrufe und die Unterstützung durch die Open Knowledge Foundation waren sehr hilfreich, um ein gutes Projekt Managment zu etablieren und haben uns die Möglichkeit zum Dialog und Erfahrungsaustausch mit den Angehörigen anderer Projekte gegeben.

Kurze Darstellung von etwaigen Ergebnissen bei anderen Stellen

Gab es Entwicklungen anderer Personen oder Institutionen, die Einfluss auf Deine Arbeiten und die Zielsetzung hatten? Wenn ja, worin bestand dieser und wie bist Du damit umgegangen?

Ein Teil der Grundlagenarbeit, auf der Dark Crystal aufbaut, wurde mit Unterstützung der Etherium Foundation erarbeitet. Dieses Projekt endete jedoch bereits in 2018.