The SolarWinds Attack and Farm-to-table Methods in the Development Process: Review

Mitigating disasters through supply chain security

Felix Pojtinger

2022-02-19

Inhaltsverzeichnis

1 Einführung

Im Rahmen der Vorlesung wählte ich ein Thema, welches mich schon seit längerem beschäftigt: Supply Chain Security. Ich hoffte über meine Vorerfahrung durch einige Open-Source-Projekte im Bereich einen relativ einfachen Einstieg in das Thema zu haben und einige der Erkenntnisse auch auf diese anwenden zu können.

2 Feedback

Schon zuvor war mir bewusst, dass eines der Hauptprobleme beim Schreiben des Papers die Verfügbarkeit von Quellen sein würde. Der immer noch relativ junge Bereich der IT-Sicherheit baut stark auf das Veröffentlichen via Blogs, Repositories und Vorträge/Videos auf, welche schwer zu zitieren sind, obwohl sie Primärquellen darstellen. Eine weitere Hürde, welche ich zum Start sah, war das Schreiben in LaTeX bzw. Markdown; während ich zwar zuvor schon oft in Isolation mit diesen Tools gearbeitet hatte (LaTeX im Rahmen von Projektberichten, Markdown im Rahmen von Projektdokumentation) hatte ich die beiden zuvor noch nicht kombiniert, weshalb vor dem Start des Schreibens noch einige Dinge unklar waren.

Dementsprechend konnten viele neue Erfahrungen mittels des Schreibprozesses erlangt werden, insbesondere im Rahmen der Recherchephase. Ich hatte versucht mich stark an die Struktur der Vorlesung zu halten und startete daher mit einer Recherche im Web und in dort veröffentlichten Journals. Schnell bemerkte ich hierbei das erste große Problem: Speziell im Rahmen der IT-Sicherheit lassen sich (zitierbare) Quellen nur schwer finden. Blogposts und ähnlichen Medien fehlt das Peer-Review, und veröffentlichte Paper sind fast nie frei verfügbar. In anderen Worten: Ohne freie Plattformen wie Sci-Hub und Library Genesis ist, selbst wenn ein Zugang zu diesen unfreien Journals vorhanden ist, Recherche kaum möglich und stellt zudem auch ein ethisches Hindernis dar. In der Vorlesung wurde hierbei z.B. angesprochen, dass Artikel möglichst gesammelt und dann überflogen werden sollen - sind jedoch alle Artikel unfrei lizenziert und kaum zugänglich, so wird eine schnelle Bewertung der Nutzbarkeit von Artikeln natürlich deutlich schwerer. Dieser Kontrast ist besonders dann spürbar wenn man es mit der Recherche via nicht-zitierbaren Quellen (i.e. Blogposts) vergleicht; hier ist die Zeit, welche zum Finden von Informationen und suche nach weiteren Informationen mit z.B. Google notwendig ist, auf deren Basis drastisch reduziert. Eine weitere Hürde im Bereich der IT-Security speziell ist, dass viele Paper aus Forschungsstipendien des US-Militärs stammen und dementsprechend zwar oft in anderen Papern zitiert, jedoch (ohne Sci-Hub) nicht zugänglich sind. Neben dem Umgang mit diesen freien Methoden, um an Quellen zu gelangen, konnte aber auch vor allem der Umgang mit LaTeX/-BibTeX gut geschult werden. Im Paper hatte ich mich für eine Toolchain auf Basis von Markdown und LaTeX mittels Pandoc entschieden, wodurch viele der Komplexitäten von LaTeX durch den deutlich

einfacheren Syntax von Markdown entschärft werden konnten, ohne aber die Fähigkeiten von BibTeX usw. zu verlieren. Dieses System war zum Beginn ein wenig gewöhnungsbedürftig, führte jedoch nach relativ kurzer Zeit zu einer sehr zufriedenstellenden Produktivität.

Beim Recherche- und Schreibprozess ist mir mehrmals der "Writer's Block" zum Verhängnis geworden. Der Grund hierfür schien zumeist gewesen zu sein, dass ich zu wenige Quellen zu Verfügung hatte und versuchte zu "Dampfplaudern", was zumeist durch eine weitere Recherche gelöst werden konnte. Besonders bei den Kapiteln Abstract, Introduction und Summary jedoch fiel es mir sehr schwer mich nicht zu wiederholen; schließlich soll das Abstract bereits die Ergebnisse beinhalten, die Introduction aber nicht einfach nur das Abstract kopieren usw. Dies konnte ich jedoch schlussendlich relativ einfach lösen, indem ich diese Abschnitte bis zum Ende einfach ignorierte und dann in diesen über den Rest des Papers deutlich einfacher reflektieren konnte. Das Paper auf Englisch zu schreiben war eine weitere Erfahrung, welche ich in diesem Rahmen gut ausprobieren konnte. Rückblickend schien dies definitiv die richtige Entscheidung gewesen zu sein, da ansonsten sehr viele "unnötige" Übersetzungen notwendig gewesen wären, schließlich sind sämtliche Quellen und der Fachjargon auf Englisch.

Das Feedback zum Paper war durchaus positiv, dennoch aber gibt es mehrere Stellen an welchen man das Paper definitiv noch verbessert könnte. Das Thema scheint interessant gewesen zu sein, aber bei manchen Themen (wie z.B. die sozialen Aspekte von sicheren Lieferketten) hätte man definitiv noch weiter in die Tiefe gehen können. Angesprochen wurden zudem auch noch ein paar Aspekte, welche mit einer etwas kritischeren Betrachtung der externen Quellen auch zuvor schon aufgefallen wären. Auch eine ganzheitliche Betrachtung des Softwareentwicklungsprozesses hätte noch eine gute Erweiterung/Schlussfolgerung sein können; viele Probleme, welche die Lieferkette betreffen, scheinen sich auch in anderen Bereichen der Softwareentwicklung in Form der grundlegenden Ansätze, wie Probleme bearbeitet werden, wiederzufinden.

Beim Schreiben meiner nächsten wissenschaftlichen Arbeit möchte ich vor allem versuchen, aktiver Quellen während der Recherchephase zu notieren. Wie schon zuvor beschrieben ist es relativ schwer mit nicht frei verfügbaren Quellen wie Journals Artikel überhaupt zu finden, noch schwerer aber ist es die genauen Stellen, welche man las, wiederzufinden, da nicht einfach ein Link zur Textstelle gespeichert werden kann. Auch das frühere Notieren von Stichpunkten zum Thema hätte hilfreich sein können, auch da dies das detaillierte Auseinandersetzen mit dem Thema, welches man gerade liest, erfordert. Am Korrekturprozess gibt es ebenfalls Verbesserungsmöglichkeiten; hier hatten sich einige Grammatikfehler eingeschlichen, welche vermutlich durch ein früheres Korrekturlesen, sofern möglich von einem Native Speaker, hätten verhindert werden können.

3 Fazit

Zusammenfassend war zwar ein deutlicher zeitlicher Aufwand notwendig, um das Paper zu schreiben, jedoch wurden auch viele notwendigen Erfahrungen gesammelt und z.B. das freie Build-System, mit welchem das Paper erstellt wurde, auch schon in anderen Projekten verwendet. Auch der Prozess der Recherche hat viele neue Quellen und Plattformen gezeigt, deren Relevanz mir zuvor nicht so stark wie jetzt bewusst war, wodurch ich hoffe bei meinem nächsten Paper die noch vorhandenen Probleme zu verbessern.