P3KI
trust yourself.

Quo vadis, Zertifikatsinfrastruktur

Graceful Degradation für resiliente, dezentrale Rechtedelegation

Version 1.5
2019-05-23

Gregor Jehle (gregor@p3ki.com)

Inhaltsverzeichnis

Version 1.5, 2019-05-23, Gregor Jehle (gregor@p3ki.com)
P3KI GmbH c/o Recurity Labs GmbH, Wrangelstr. 4, 10997 Berlin, Germany

1 Vorwort

Eine Version dieses Whitepapers erschien im Tagungsband[1] zum 16. Deutschen IT-Sicherheitskongress des Bundesamtes für Sicherheit in der Informationstechnik (BSI) welcher unter dem Titel "IT-Sicherheit als Voraussetzung für eine erfolgreiche Digitalisierung" vom 21. bis 23. Mai 2019 in Bad Godesberg stattfand.

2 Ein Traum von Sicherheit

Zertifikatsinfrastruktur und PKI sind nur in der Presse, wenn etwas passiert: Diginotar verliert Schlüssel[2] und verschweigt es, ein internationaler Sicherheitsanbieter wird mehrfach dabei erwischt Zertifikate[3] an unbekannte Dritte ausgestellt zu haben oder Zertifikate welche zur Authentifizierung einer Website gedacht waren signieren stattdessen bösartige Software. Die Aufregung ist heftig aber kurz. Das nächste Projekt setzt auf die gleiche Technologie. Alternativen gibt es keine.

Sicherheit ist lästig. Niemand will darüber reden und schon gar nicht bei der Benutzung von Services eingeschränkt werden.

Warum werden marktführende Datenbanksysteme ohne Absicherung durch Passwörter[4] und Zertifikate[5] installiert? Einfach: Die dafür notwendigen zwei bis drei Interaktionen senken die Conversion Rate signifikant. Die durch Wegfall der Absicherung gewonnene Zeit und reduzierte Komplexität erhöhen direkt die Wahrscheinlichkeit einen Kunden zu gewinnen. Steht das Testsetup erst einmal schaltet man es einfach Live. Die fehlende Absicherung ist längst vergessen. Die Aufgabe ist erfüllt und wir haben doch keine Zeit!

Gute Sicherheitstechnik ist unsichtbar. Verfügbarkeit und Verlässlichkeit sind Grundvoraussetzung. Eine verlässliche Absicherung gegenüber Angriffen muss ebenso gegeben sein wie eine hohe Fehlertoleranz und schnelle Korrekturmaßnahmen. Günstiger Betrieb und einfache Anpassbarkeit sind essentiell.

Existiert so etwas überhaupt? Welche technischen Eigenschaften muss ein solches System bieten? Nicht zuletzt stellt sich die Frage: Ist aktuelle Technologie den zukünftigen Entwicklungen bereits gewachsen?

3 Revolution mit Fußfessel

Das Internet der Dinge lebt von Dezentralisierung. Sein Ziel ist es, Sensoren und Aktoren, ohne die bisher notwendigen starren Hierarchien flexibel mit beliebigen Agentensystemen zu verknüpfen, um so maximale Flexibilität zu erreichen. Kernaspekt hierbei ist, dass jeder individuelle Sensor und Aktor nicht zwingend nur einem Agentensystem zugeordnet sein muss sondern zwischen vielen geteilt werden kann. So könnten sich einzelne, stark spezialisierte Agenten um ihre individuellen Aufgaben kümmern.

Betrachten wir eine moderne CNC-Fräsmaschine, welche mit einer Vielzahl Sensoren und Aktoren bestückt ist. Diese können unter anderem verwendet werden, um die Kräfte, welche auf die Frässpindeln wirken, anzuzeigen. Ein sehr einfacher und direkter Zusammenhang zwischen physischem Effekt, Messung und Indikation.

Erfasst man dazu noch weitere Werte, wie Stromaufnahme oder Laufruhe, sind die daraus resultierenden

[1] Nachdrucke der Tagungsversion des Whitepapers sind im Tagungsband ISBN 978-3-922746-82-9 über den Buchhandel erhältlich.
[2] https://threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112/77170/
[3] https://security.googleblog.com/2017/09/chromes-plan-to-distrust-symantec.html
[4] https://docs.mongodb.com/guides/server/auth/
[5] https://www.elastic.co/guide/en/elasticsearch/reference/current/security-settings.html

Informationen für sich gesehen sicherlich interessante Indikatoren für den Zustand der Maschine. Ein erheblicher Mehrwert ergibt sich jedoch erst aus der Zusammenführung dieser Datenpunkte mit einem Verschleißmodell, welches es erlaubt, subtile, graduelle Veränderungen aufzuzeigen und sie in einen zeitlichen Kontext im Lebenszyklus der Maschine zu setzen. Hierdurch kann ein Agent auftretende Fehler frühzeitig erkennen und Ersatzteilbestellungen auslösen bevor die Produktion zum Stillstand kommt. Dieses "Predictive Maintenance"[6] genannte Verfahren ist heutzutage bereits gang und gäbe.

Eine CNC-Fräsmaschine ist ein in sich geschlossenes System unter wohl definierter Kontrolle. Die wahre Revolution beginnt mit der Vernetzung über Systemgrenzen hinweg. Genau hier, bei Dezentralisierung von Sensor- und Aktornetzen, stoßen bestehende Technologien bei der Dezentralisierung an ihre Grenzen. Dabei sind die grundlegenden technischen Fragen zur Kommunikation, Datenerfassung und -aufbereitung bereits gelöst. Problematisch wird es, wenn es an die Beantwortung von Fragen geht die für den Menschen Alltag sind, die Maschinen aber vor große Probleme stellen. Das sind Fragen wie:

- "Darf der das?"
- "Ist die Datenquelle vertrauenswürdig?" oder
- "Darf dieser Agent diesen Aktor kontrollieren?"

Autonomes Fahren und Parken[7] ist ein weiteres Feld, welches vor dieser Herausforderung steht. Viele Automobilhersteller – mit jeweils Dutzenden Modellreihen – mit Millionen an Fahrzeugen weltweit müssen hierfür mit einer breiten Palette an heterogener Infrastruktur interagieren. Diese wiederum ist ein Zoo unterschiedlichster Systeme, Anforderungen, Hersteller und Betreiber: Smarte Straßen und Autobahnen, Parkhäuser, Ladestationen für eMobility, freie und Lizenzwerkstätten. Hinzu kommt unweigerlich die notwendige Interfahrzeugkommunikation.

Wenig anders stellt sich die Situation im Energiesektor dar. Die für die Aufrechterhaltung der Stromnetzstabilität notwendige zentrale Steuerung kämpft gegen die zunehmende Dezentralisierung der Energieerzeugung[8]. Egal ob Blockheizkraftwerke, Solar- oder Windkraftanlagen, längst gehören Stimmen, welche nach fernsteuerbaren Endverbrauchern rufen, zum Alltag.

Ist erst einmal alles untereinander vernetzt, kann jedoch jeder Netzteilnehmer auf alle Geräte zugreifen, sei es um Daten auszulesen oder Kontrolle auszuüben. Aber wie kann in einem solchen Szenario sichergestellt werden, dass Datenzugriffe und erhaltene Instruktionen genehmigt sind?

Offene, kryptografische Algorithmen sind hier die einzige verlässliche Möglichkeit Sicherheit zu schaffen, und auf diesen aufbauende Lösungen für Autorisierung bzw. Authentifizierung der Kommunikationspartner untereinander sind zwingend notwendig. Hierzu wurden Zertifikatstechnologien wie der bereits 1998 eingeführte X.509-Standard entwickelt. In ihm hängt Vertrauen an wenigen zentralen und als vertraut definierten Einheiten: sogenannten Certificate Authorities (CAs). Diese stellen Zertifikate an Dritte aus, welche über diese als vertrauenswürdig und "zugehörig" verifiziert werden können.

Aktuelle Zertifikatsinfrastruktur ist zwar ein verteiltes System und in verteilten Systemen einsetzbar, sie ist allerdings nicht dezentral. Essenzielle Bestandteile wie der Server für Zertifikatswiderruf und das Schlüsselmanagement sind hierbei zentralisiert. Daher verliert ein dezentrales System seine wesentlichen dezentralen Eigenschaften, sobald klassische Zertifikatsinfrastrukturen integriert werden. Neben diesem strukturellen Mangel bestehen noch weitere Mängel wie unzureichende Präzision, unflexible Delegation, aufwändige Schlüssel- und Zertifikatsverteilung und nicht zuletzt grobmotorisches Verhalten im Angriffs- und Fehlerfall.

[6] https://en.wikipedia.org/w/index.php?title=Predictive_maintenance&oldid=878934341
[7] https://www.mercedes-benz.com/en/mercedes-benz/innovation/avp-bosch-and-daimler-show-driverless-parking-in-real-life-traffic/
[8] https://derstandard.at/2000096185439/Europas-Stromnetz-stand-am-Rande-des-Totalausfalls

4 Herausforderung an die PKI der Zukunft

Die Praxis zeigt, dass sowohl das Internet of Things, als auch der Ansatz der Industrie 4.0 die klassischen Zertifikatsinfrastrukturen vor einzigartige Herausforderungen stellen. Hierbei stehen Interoperabilität, rechtliche und organisatorische Aspekte des Betriebs und Verhalten unter widrigen Umständen wie beispielsweise beim Ausfall von Kommunikationsinfrastruktur im Fokus.

Welche Anforderungen müssen wir somit an eine zukunftstaugliche Alternative zu bestehender PKI und Zertifikatsinfrastruktur stellen?

4.1 Feingranulare Rechtedelegation

Zertifikate auszustellen, welche lediglich auf ihre generelle Gültigkeit geprüft werden, kommt einem Blankoscheck gleich, ist aber nicht unüblich. Ebenso können vordefinierte Rollen und Berechtigungen zwar eine Vielzahl an Anwendungsfällen abdecken, aber niemals alle. Außerdem sind diese immer auch ein Kompromiss und ein Wettgeschäft auf zukünftige Entwicklungen.

Um die daraus resultierenden Probleme in Zukunft zu vermeiden, ist es zwingend notwendig, das Rechtesystem auf den Anwendungsfall anpassbar zu machen, statt die individuellen Anforderungen in das Rahmenwerk bestehender Systeme zu zwängen. So werden Mehrdeutigkeiten und unterschiedliche Interpretationen gleicher, vordefinierter Terme in verschiedenen Systemen vermieden.

Eine Lösung stellen hochflexible und mathematisch beweisbar korrekte Sprachen für Rechte- und Rollenvergabe dar. Mit ihnen kann das Vertrauensmodell eines gegebenen Szenarios perfekt passend modelliert werden, ohne durch einen vordefinierten Baukasten von Rechten und Rollen beschränkt zu sein.

Des Weiteren müssen Rechte und Rollen sowohl ganz als auch partiell zu delegieren sein. Je spezifischer eine solche Delegation beschrieben werden kann, umso genauer lässt sich das Betriebsrisiko abschätzen und der Umfang von Sicherheitsvorfällen eingrenzen.

4.2 Echte Dezentralisierung durch Web-of-Trust

Wie beschrieben ist ein streng hierarchisches Zertifikatsmodell den Anforderungen der bevorstehenden Dezentralisierung nicht gewachsen. Ein zukunftsfähiges System muss also zum einen vollständig dezentral betrieben werden, zum anderen aber auch flexible Vertrauensmodelle jenseits strenger Hierarchien modellieren können.

Es wird unweigerlich ein Wechsel hin zu Web-of-Trust Strukturen notwendig sein, hin zu Strukturen, in denen ein Gerät multiplen Parteien vertrauen kann, ohne das dieses Vertrauen über eine oder einige wenige zentrale Certificate Authorities ausgedrückt werden muss. Vertrauen und Rechte-Delegation müssen auch lokal, direkt zwischen Geräten, auf Ebene eines Haushalts, einer Abteilung, einer Firma oder eines beliebigen Szenarios möglich sein.

Dies ermöglicht eine erhöhte Flexibilität in der Modellierung, reduziert die Abhängigkeit von Dritten und minimiert Risiken. Wenige, zentrale Certificate Authorities, welche als Opfer eines Hackerangriffs industrieweite bzw. weltweite Effekte nach sich ziehen, müssen der Vergangenheit angehören.

Version 1.5, 2019-05-23, Gregor Jehle (gregor@p3ki.com)
P3KI GmbH c/o Recurity Labs GmbH, Wrangelstr. 4, 10997 Berlin, Germany

4.3 Risikomanagement als Kernaspekt

Ein struktureller Aspekt der Risikominimierung wurde bereits in der Dezentralisierung identifiziert. Darüber hinaus ist auch die eingangs beschriebene Granularität der Rechtedelegation ein nicht zu unterschätzender Punkt. Je konkreter ausgedrückt werden kann welche Rechte im Rahmen einer Delegation übertragen werden, umso geringer sind die Möglichkeiten die ein Angreifer ausnutzen kann wenn er die Kontrolle über den Empfänger dieser Rechte erhalten kann.

Mit bestehenden X.509 Zertifikatsinfrastrukturen ist der Verlust eines Zertifikats oft mit weitreichenden Berechtigungen für den Angreifer verbunden. Ließe sich jedoch genau ausdrücken, dass eine Berechtigung im Rahmen dieses Zertifikats sich beispielsweise lediglich auf das Auslesen von Sensorwerten oder das Einspielen eines konkret definierten Firmwareupdates beschränkt, so könnte ein Angreifer eben genau diese Aktionen ausführen und keine anderen, wodurch die Risikobewertung von Systemen, gerade im Umfeld Kritischer Infrastruktur (KRITIS), deutlich einfacher greifbar und nachvollziehbar wäre.

4.4 Schnelle Provisionierbarkeit

Neue Geräte in ein Vertrauensnetzwerk zu integrieren sowie die Delegation von Rechten und Rollen an selbige muss ohne zentrale Instanzen lokal oder föderiert bewerkstelligt werden können. Dabei muss eine Lösung effizient genug sein, um auch auf schwächeren eingebetteten Systemen benutzbar zu sein, ohne den Grad der Sicherheit zu beeinträchtigen.

Die Anforderungen an ein solches System sind mehrschichtig:

- Kryptografische Algorithmen mit geringer Entropieanforderung bei hoher Sicherheit
- Minimierung der Interaktionen auf Protokollebene
- Minimierung nicht-automatisierter Interaktionen
- Sicherer und vollständiger Transfer der Besitz- und Eigentumsrechte innerhalb des Rechtesystems

4.5 Flexibilität gegenüber Veränderung

Warum sollte ich jemandem länger vertrauen als zur Erfüllung einer Aufgabe notwendig ist? Für klassische Zertifikatsinfrastrukturen gelten wegen des hohen Aufwands für Schlüssel- und Zertifikatsverteilung Gültigkeitsdauern im Bereich von 4 Tagen bereits als extrem kurz.

Ein zukunftstaugliches System muss daher im Stande sein Zertifikate und Delegationen auszustellen, deren Gültigkeit in Sekunden, Minuten und Stunden gemessen wird.

Im gleichen Zuge ist es auch wichtig, seine Meinung ändern zu können. Konkret bedeutet dies, den Grad einer Delegation anpassen zu können, ohne in der Delegationskette nachfolgende Delegationen anfassen zu müssen. Stattdessen sollten lokale Änderungen eines Knotens dynamisch in die Auswertung längerer Ketten integriert werden.

Ein oft unterschätzter Anwendungsfall ist auch die Einführung neuer Gerätegenerationen und Softwareversionen. Dies gilt gerade im Hinblick auf Interoperabilität mit bestehenden Geräten im Feld. Modelle zur Fähigkeitsaushandlung zwischen Geräten sind alt, jedes Faxgerät ist dazu fähig. Dies jedoch direkt im Rahmen der Rechtedelegation durch Zertifikatsinfrastrukturen zu abstrahieren, ist bisher nur teilweise und sehr eingeschränkt angegangen worden. So lässt sich üblicherweise aushandeln, welche kryptografischen Algorithmen zwischen zwei Parteien verwendet werden können. Eine darüber hinaus führende, weitergehende Aushandlung von Fähigkeiten zwischen Geräten – sogenannte “Capabilities” – oder von im Rahmen der Rechtedelegation definierten szenariospezifischen Beschreibungssprachen ist dabei bisher garnicht oder nur in

Insellösungen umgesetzt.

4.6 Einfacher Betrieb

Die Benutzung einer Zertifikatsinfrastruktur sollte möglichst einfach vonstattengehen. Je näher das Verhalten der Lösung am natürlichen Verständnis der Benutzer liegt umso größer wird der Grad ihrer Akzeptanz sein. Die Stellen an denen ungewollte Nebeneffekte verursacht werden können, müssen minimiert werden.

5 Rettung in der Blockchain?

Betrachtet man die aktuellen Entwicklungen, so zeigt sich, dass in den letzten Jahren vor allem Blockchain, Ledger-Technologien oder allgemeine Trustless-Systems als Allheilmittel durch das digitale Dorf getrieben werden. Will man eine Kryptowährung entwerfen und dabei niemand Einzelnem vertrauen müssen, ist diese Technologie sicherlich das Mittel der Wahl. Für alle darüber hinaus gehenden Probleme hat sich jedoch gezeigt, dass in der Regel bewährte Technologien existieren, welche diese Anforderungen günstiger und besser lösen als Blockchain.

Das liegt vor allem daran, dass die Technologie Blockchain mit unfälschbarer Nachvollziehbarkeit aller Transaktionen punkten will, ohne dass es dabei notwendig ist einer zentralen Instanz zu vertrauen. Doch mit den üblichen Kontrollanforderungen der Industrie deckt sich dies nicht.

Eine angebliche Lösung hierfür sind "Private Blockchains", welche effektiv unter der Kontrolle einer Firma oder eines Konsortiums stehen. Jedoch lässt sich fälschungssichere Nachvollziehbarkeit durch eine "Append-Only" Datenbank[9][10] wesentlich wirtschaftlicher umsetzen als mit Blockchain, und etablierte Konsenssysteme[11] ermöglichen Entscheidungsfindung zwischen Parteien ohne Notwendigkeit von Vertrauen in Einzelne.

Zusammengefasst lässt sich sagen: Blockchain ist der größt-mögliche Hammer um eine Schraube ins Holz zu treiben.

6 Resilienz durch Graceful Degradation

Wer Infrastruktur anbietet, setzt diese Angriffen aus und selbst Infrastruktur, welche nicht durch Angriff zu Schaden kommt, kann ausfallen oder benötigt Wartungsfenster. Das Sicherstellen des Betriebs, auch im Falle des Wegfalls wesentlicher Systemelemente, ist Kernaspekt dezentraler Systeme.

Dabei spricht nichts gegen den Einsatz von performanten, zentralen oder klassisch verteilten Datenbanken zur Vorhaltung und Kommunikation von Delegationsdaten. Jedoch nur, solange dies nicht zwingende Voraussetzung für den Betrieb ist.

Die Konsequenzen einer solchen Abhängigkeit waren bereits mehrfach bei größeren Ausfällen von Cloudinfrastruktur zu beobachten. So konnten zum Beispiel, verursacht durch den Ausfall des Cloud-Angebotes von Amazon, große Teile des Internets[12] nicht mehr benutzt oder es konnte mitten im Winter nicht mehr

[9] http://couchdb.apache.org/
[10] https://kafka.apache.org/
[11] https://raft.github.io/
[12] https://www.wired.com/2017/02/happens-one-site-hosts-entire-internet/

geheizt[13] werden. Ursache war in beiden Fällen, eine unnötige aber trotzdem vorhandene vollständige Abhängigkeit vom cloud-basierten Backend, welches temporär nicht zur Verfügung stand.

Auf Basis der oben dargelegten Anforderungen sollte sich eine Zertifikatsinfrastruktur modellieren lassen, welche Graceful Degradation spielend umsetzen kann.

Die Infrastrukturen der Zukunft müssen unabhängig von Kommunikationswegen interagieren können. Es muss also möglich sein die zum Betrieb einer Zertifikatsinfrastruktur notwendigen Daten, im Notfall auch über andere, gar beliebige, Kanäle austauschen zu können. So wären unter anderem Peer-to-Peer Netzwerke oder im Extremfall sogar Offlinemedien wie USB-Laufwerke, Smartcards und Store-and-Forward Netzwerke als Datenkanal vorzusehen. Dadurch werden Probleme wie Denial-of-Service Angriffe[14], der Wegfall von Netzverbindungen bzw. Szenarien mit sporadischer oder gar keiner Netzverbindung (z.B. Air-Gapping) lösbar.

Kommt es dennoch zu einem erfolgreichen Angriff auf einen Teilnehmer des Netzes, muss der Einfluss des Angreifers um den kompromittierten Teilnehmer herum isoliert werden können, so dass der Einfluss des Angreifers minimiert wird und zu jeder Zeit von außen quantifizierbar bleibt. Hierbei spielen sowohl Aspekte des Web-of-Trust sowie die Möglichkeit Rechtedelegationen beliebig genau ausdrücken zu können wesentliche Rollen. Denn hier sind Strukturen gefordert, die neben der Isolation betroffener Teilnehmer auch deren Ersetzung im laufenden Betrieb ermöglichen, selbst wenn eine Großzahl der anderen Teilnehmer gerade nicht direkt erreichbar ist.

7 Quo Vadis?

Sind die obigen Grundsteine gelegt, steht im nächsten Schritt nach der Dezentralisierung der Weg zu echten autonomen System als große Herausforderung bevor. Denn bislang beschränkt sich die Debatte über diese auf philosophische Gedankenspiele zu Entscheidbarkeit und Verantwortung[15], doch die technischen Aspekte der Umsetzbarkeit und Absicherung der Kommunikation und Rechtedelegation zwischen autonomen Systemen bleibt bislang weitestgehend unbetrachtet. Doch was ist ein autonomes Systeme ohne seine Interaktion mit seiner Umwelt und anderen Systemen?

Zertifikatsinfrastrukturen und PKI müssen hier Schritt halten, um nicht in naher Zukunft auf der Strecke zu bleiben. Die Alternativen sind ernüchternd: Entweder wird die aktuelle Technologie den Fortschritt behindern oder – die wahrscheinlichere Option – man wird auf solide Sicherheitstechnik in Abwägung gegenüber Benutzbarkeit und Machbarkeit verzichten. Es wird also dringend nötig flexiblere Systeme, welche den dargelegten Aspekten genügen, an die Stelle existierender Technologien treten zu lassen.

Bevor wir über echte Autonomie sprechen können, stellen sich folgende Kernfragen:

- Wie können Systeme selbsttätig von Null an entscheiden, wem um sie herum sie zu welchem Grade initial vertrauen können und wollen?
- Wie lässt sich entscheiden, wie sich dieser Grad an Vertrauen unter welchen Bedingungen über die Zeit verändert?

Die Beantwortung dieser Fragen und die Schaffung moderner, unabhängiger Sicherheitsinfrastrukturen eröffnet uns die Möglichkeit, wieder eine führende Rolle im globalen Wettbewerb einzunehmen.

[13] https://www.nytimes.com/2016/01/14/fashion/nest-thermostat-glitch-battery-dies-software-freeze.html
[14] https://en.wikipedia.org/w/index.php?title=2016_Dyn_cyberattack&oldid=880946301
[15] https://www.washingtonpost.com/news/innovations/wp/2015/12/29/will-self-driving-cars-ever-solve-the-famous-and-creepy-trolley-problem/

Version 1.5, 2019-05-23, Gregor Jehle (gregor@p3ki.com)
P3KI GmbH c/o Recurity Labs GmbH, Wrangelstr. 4, 10997 Berlin, Germany

8 Über den Autor

Gregor Jehle ist Geschäftsführer der P3KI GmbH, einem berliner Startup und Ausgründung der Forschungsabteilung der Recurity Labs GmbH, einem renommierten berliner IT-Security Beratungsunternehmens und beschäftigt sich mit der Entwicklung von vollständig verteilten, dezentralen und föderierten PKIs für Autorisation und Authentifikation, welche auch komplett Offline betrieben werden kann.

www.p3ki.com, contact@p3ki.com, +49 (0)711 22051252 (Stuttgart), +49 (0)30 695399933 (Berlin).