Sicherheit im Internet der Dinge leicht gemacht

Gerhard Wunder, FU Berlin und Fraunhofer HHI, Andreas Müller, Robert Bosch GmbH, Christof Paar, Ruhr-Universität Bochum, Hans D. Schotten, TU Kaiserslautern, Thomas Wollinger, Escrypt GmbH, Eduard Jorswieck, TU Dresden und Aydin Sezgin, Ruhr-Universität Bochum

Security Made Easy for IoT

Securing the IoT poses specific challenges which are still only partially solved. These include the often very limited computing, storage, and energy resources of wirelessly connected IoT devices, the high demands on the user-friendliness, as well as the high-cost pressure. Upon this background, the research project PROPHYLAXE ("Providing Physical Layer Security for the Internet of Things"), funded by the BMBF, pursued a novel approach in which the physical properties of the wireless transmission link between two devices are exploited. Based on these properties, cryptographic keys can be generated that are known only to the communicating devices and can be used to secure and authenticate a connection.

Keywords:
IoT, embedded systems, physical layer security, resource-constrained devices, secret key management

Das Internet der Dinge (Internet of Things, IoT) ist – wie alle IT-Systeme – durch Angriffe verwundbar [1]. Dies ist durch zahlreiche aufsehenerregende Vorfälle aus jüngster Zeit belegt, bspw. das „Hacken" in fahrende Autos bei hoher Geschwindigkeit oder sogar Eingriffe in lebenserhaltende medizinische Implantate. Bei der Absicherung des IoT müssen allerdings spezifische Herausforderungen bewältigt werden, die bis heute nur unvollständig gelöst sind. Dazu gehören z. B. die oftmals sehr beschränkten Rechen-, Speicher- und Energieressourcen der häufig drahtlos vernetzten IoT-Geräte, die hohen Anforderungen an die Benutzerfreundlichkeit sowie nicht zuletzt auch der hohe Kostendruck. Vor diesem Hintergrund wurde im vom BMBF geförderten Forschungsprojekt PROPHYLAXE („Providing Physical Layer Security for the Internet of Things") ein neuartiger Ansatz verfolgt, bei dem physikalische Eigenschaften der drahtlosen Übertragungsstrecke zwischen zwei Geräten zur Absicherung der Kommunikation zwischen diesen Geräten ausgenutzt werden. Auf Grundlage dieser Eigenschaften können insbesondere kryptographische Schlüssel erzeugt werden, die nur den kommunizierenden Geräten bekannt sind. In PROPHYLAXE wurde in einer weltweit einmaligen interdisziplinären Kooperation von IT-Sicherheitsexperten, Nachrichtentechnikern und Anwendern erstmalig ein praxistauglicher Ansatz dafür erarbeitet.

Nach dem Siegeszug des Internets gegen Ende des letzten Jahrtausends sowie dem Erfolg von sozialen Netzwerken wie Facebook und Twitter in den letzten 10 Jahren erleben wir mit dem „Internet der Dinge" momentan den nächsten Evolutionsschub der fortschreitenden Digitalisierung unserer Welt. Das IoT wird alle Lebensbereiche durchdringen und dabei nicht nur Menschen, sondern auch Sensoren, Aktoren und andere „Dinge" umfassend vernetzen, um dadurch ein noch nie dagewesenes Maß an Automatisierung, Komfort und Effizienz zu ermöglichen. Ein konkretes Beispiel für entsprechende Anwendungsbereiche ist das intelligente Haus („Smart Home"), das bspw. erkennen kann, wenn ein Fenster geöffnet ist, und dann selbstständig die Heizung herunterregelt, um die Energieeffizienz zu erhöhen. Genauso bildet das IoT aber auch die Grundlage für Industrie 4.0 sowie für zukünftige intelligente Städte („Smart Cities"), die Digitalisierung des Gesundheitswesens oder auch eine effizientere, aber gleichzeitig auch nachhaltigere Landwirtschaft. Das wirtschaftliche Potenzial, das sich daraus ergibt, ist immens. Aktuelle Schätzungen gehen davon aus, dass bereits im Jahr 2020 ca. 30 Mrd. „Dinge" miteinander vernetzt sein werden, wohingegen es im Jahr 2025 schon 75 Mrd. sein sollen [2] – und das ist erst der Anfang. Somit stellt das IoT auch für den Standort Deutschland Chance und Risiko zugleich dar, da sich viele Märkte und Wertschöpfungsketten dadurch grundlegend verändern werden.

Eine unabdingbare Voraussetzung für den Erfolg und die Akzeptanz des IoT ist allerdings ein hohes Maß an Sicherheit, sodass auch in einer hochgradig vernetzten Welt die Daten sicher sind und keine ungewünschten Manipulationen oder Beeinträchtigungen von Systemen möglich werden. In letzter Zeit publik gewordene Beispiele zeigen, dass die potenziellen Auswirkungen von Angriffen im IoT noch viel gravierender und weitreichender sein können als in klassischen IT-Systemen. Dazu ist mithilfe von speziellen Webseiten häufig nicht einmal Expertenwissen notwendig [1]. So gibt es gleich eine ganze Reihe von Angriffen über das Internet auf Autos mit Eingriffen in die Fahrfunktionen [3]. Andere, ebenfalls potenziell lebensgefährliche Angriffe, sind z. B. gegen medizinische Geräte möglich [4]. Dass auch Angriffe gegen vernetzte Produktionsanlagen realistisch sind, wurde dramatisch durch einen erfolgreichen Angriff auf eine deutsche Stahlfabrik demonstriert [5]. Weitere, ebenfalls besorgniserregende Angriffe nutzen IoT-Geräte,

PD Dr.-Ing. Gerhard Wunder, Heisenberg-Fellow ist Leiter der Heisenberg-Arbeitsgruppe Kommunikations- und Informationstheorie, Freie Universität Berlin.

Dr.-Ing. Andreas Müller ist Senior Expert für „IoT Communication Technologies", Robert Bosch GmbH, Zentralbereich Forschung und Vorausentwicklung, Stuttgart.

Prof. Dr.-Ing. Christof Paar leitet den Lehrstuhl „Embedded Security", Fakultät für Elektrotechnik und Informationstechnik, Ruhr-Universität Bochum.

Prof. Dr.-Ing. Hans D. Schotten leitet den Lehrstuhl für Funkkommunikation und Navigation, Technische Universität Kaiserslautern.

Dr. Thomas Wollinger ist Managing Director, ESCRYPT GmbH - Embedded Security.

Prof. Dr.-Ing. Eduard Jorswieck leitet den Lehrstuhl für Theoretische Nachrichtentechnik, Technische Universität Dresden.

Prof. Dr.-Ing. Aydin Sezgin leitet den Lehrstuhl Digitale Kommunikationssysteme, Ruhr-Universität Bochum.

g.wunder@fu-berlin.de
www.mi.fu-berlin.de/en/inf/groups/ag-comm

um klassische Internetangriffe auszuführen, z. B. durch die Realisierung von IoT-Botnetzen [6]. Die potenziellen Angreifer können neben Kriminellen z. B. auch Konkurrenten von Unternehmen sein, die Interesse haben könnten, deutsche Hersteller von IoT-Geräten zu schädigen oder auszuspionieren. Wie durch die „Snowden"-Dokumente belegt, muss aber auch davon ausgegangen werden, dass ausländische Nachrichtendienste das IoT gefährden und mit Angriffen ganze Infrastrukturen, wie z. B. die Energienetze, angreifen könnten. Dieser Zustand ist für vitale Bereiche (z. B. kritische Infrastrukturen, Fabriken, öffentliche Einrichtungen, private Haushalte) daher eine potenzielle Gefährdung. Ziel muss es daher sein, jedes noch so kleine IoT-Gerät mit elementaren und einfach nutzbaren Sicherheitsfunktionen auszustatten.

Bei der Absicherung des IoT sind allerdings spezielle Randbedingungen und Anforderungen zu beachten, die mit etablierten Ansätzen in klassischen IT-Systemen (z. B. Aufruf einer sicheren Internetverbindung beim „Online-Banking") oft nicht in Einklang zu bringen sind. Dabei spielen sogenannte symmetrische Verfahren eine zentrale Rolle, mit denen die meisten Sicherheitsfunktionen hocheffizient auf IoT-Geräten realisiert werden können, z. B. sichere Kommunikation zwischen IoT-Geräten, Zugriffsschutz oder sichere Software-Updates. Symmetrische Verfahren haben allerdings den großen Nachteil, dass die Kommunikationsparteien, z. B. ein IoT-Gerät im Haushalt und das Smartphone des sich auf Reisen befindlichen Besitzers, einen gemeinsamen geheimen kryptographischen Schlüssel vorher vereinbaren müssen. Die Standardlösung im Internet sind komplexe, sogenannte asymmetrische Verfahren, die mit hohem Rechenaufwand von einigen Millionen Multiplikationen (und somit auch hohem Energieverbrauch) einen geheimen kryptographischen Schlüssel zwischen zwei verteilten Kommunikationsparteien erzeugen können. In der Praxis werden asymmetrische Verfahren oftmals auch dafür eingesetzt, um zunächst unbekannte Kommunikationsparteien zu authentisieren. Allerdings verfügen viele IoT-Geräte nur über sehr beschränkte Rechen-, Speicher- und Energieressourcen (z. B. durch Batteriebetrieb), weshalb der Einsatz solcher Verfahren in vielen Fällen nicht möglich ist. Zudem sollte eine Absicherung im IoT möglichst auf Verfahren aufgebaut werden, deren Sicherheit auch dann nicht kompromittiert werden kann, falls einmal leistungsfähige Quantencomputer zur Verfügung stehen, was in nicht allzu ferner Zukunft voraussichtlich der Fall sein wird. In diesem Fall werden alle zurzeit eingesetzten klassischen asymmetrischen Ansätze angreifbar werden. Eine Alternative dazu wäre eine manuelle Schlüsselverteilung, bspw. durch die Eingabe eines Passworts in den beteiligten Geräten. Dies ist aufgrund der sehr großen Anzahl an IoT-Geräten, die sicher miteinander vernetzt werden sollen, allerdings mit einem sehr hohen logistischen bzw. organisatorischen Aufwand verbunden und aufgrund der Tatsache, dass viele IoT-Geräte oftmals nicht über eine komfortable Benutzerschnittstelle verfügen (wie z. B. ein Display oder eine Tastatur), auch nur bedingt möglich.

Weiterhin werden viele Dinge im IoT, nachdem sie einmal installiert und in Betrieb genommen worden sind, für einen langen Zeitraum aktiv bleiben, wobei nachträgliche Wartungen (z. B. zum Austausch von Schlüsseln) möglichst vermieden werden sollen. Ein Beispiel hierfür sind intelligente Sensoren zur Überwachung der Luftqualität in Städten, die z. B. auf Straßenlaternen montiert werden können und somit ggf. auch nur sehr schwer zugänglich sind. Um dennoch langfristig ein ausreichendes Maß an Sicherheit gewährleisten zu können, ist eine regelmäßige, möglichst automatisierte Aktualisierung der verwendeten Schlüssel erforderlich – analog zur regelmäßigen Erneuerung von Passwörtern bei klassischen IT-Systemen. Schließlich ist eine sehr einfache Handhabbarkeit der Verfahren notwendig, sodass auch Personen ohne spezielle IT-Kenntnisse in der Lage sind, auf einfache Art und Weise ein neues IoT-Gerät sicher in ein Netzwerk zu integrieren. Nur so kann sichergestellt werden, dass starke Sicherheitstechnologien auch verbreitet zum Einsatz kommen und somit den oben angedeuteten Bedrohungsszenarien effektiv entgegengewirkt werden kann. Daraus entsteht der Bedarf nach innovativen, neuen Verfahren, die diese besonderen Randbedingungen geeignet berücksichtigen und im PROPHYLAXE-Projekt sowie darauf aufbauenden Anschlussaktivitäten der beteiligten Partner entwickelt wurden.

Die Innovationen im Detail

Der PROPHYLAXE-Ansatz: Vom Funkkanal zum Schlüssel

Das Ersetzen von asymmetrischer Kryptographie gilt als bekannte und grundlegende Herausforderung für IoT-Anwendungen. Um dieses Problem zu lösen, wurde in PROPHYLAXE ein Ansatz gewählt, der sich vollkommen von der sich auf mathematische Berechnungskomplexität stützenden klassischen Kryptographie unterscheidet und stattdessen physikalische Phänomene ausnutzt. Im vorliegenden Fall ist dies die Physik der Funkkommunikation, d. h. des Übertragungskanals zwischen den IoT-Geräten, welcher in die Sicherheitsarchitektur mit einbezogen wird. Dies ist möglich, da eine Vielzahl von IoT-Geräten über

drahtlose Standards, wie z. B. WLAN oder Bluetooth, vernetzt ist. Der Übertragungskanal hat spezifische Eigenschaften, die im Zusammenhang mit IT-Sicherheit äußerst vorteilhaft sind:

a. Zeitliche Veränderung: Durch kleine Veränderungen in der Umgebung in der Größenordnung der Wellenlänge der Funksignale werden Pfade zufällig gedämpft oder verstärkt. Der Übertragungskanal wirkt hierdurch wie ein Zufallsgenerator für kryptographische Schlüssel.
b. Umkehrbarkeit des Übertragungswegs und Nicht-Angreifbarkeit: Aus der Physik der Wellenausbreitung ist bekannt, dass die Kommunikationsparteien den physikalisch gleichen Übertragungskanal messen (Reziprozität) und dieser auch außerhalb einer sehr kleinen Umgebung (typischerweise wenige cm) nicht durch einen Angreifer rekonstruiert werden kann.

Der Übertragungskanal kann als eine physikalische Zufallsquelle aufgefasst werden, auf die beide Kommunikationsparteien (und nur diese) Zugriff haben. Dieser Umstand kann sowohl für die Ableitung eines kryptographischen Schlüssels als auch für die Authentisierung (z. B. durch räumliche Nähe) genutzt werden. Das Grundprinzip der Schlüsselgewinnung ist wie folgt (Bild 1): Die Kommunikationsparteien sind die IoT-Geräte „Alice" und „Bob". Sowohl Alice als auch Bob messen zuerst nacheinander den Übertragungskanal, indem sie ein bekanntes Testsignal senden. Aufgrund der Umkehrbarkeit dieses Kanals erzeugen beide Kommunikationsparteien daraus einen nur ihnen bekannten kryptographischen Schlüssel. Damit kann die Kommunikation zwischen Alice und Bob nachfolgend mittels hocheffizienter, symmetrischer Verfahren abgesichert werden.

Bild 1: Das Grundprinzip des PROPHYLAXE-Ansatzes.

Das Grundprinzip wurde in [7] erstmalig für die Schlüsselgewinnung untersucht und in weiteren Veröffentlichungen verfeinert, siehe [8, 9]. Um aus diesen bekannten Grundlagen ein praktisches Gesamtsystem mit starken Sicherheitseigenschaften zu realisieren, waren allerdings umfassende interdisziplinäre Forschungsanstrengungen erforderlich, die ein modernes „Security-Engineering" mit nachrichtentechnischer und informationstheoretischer Grundlagenforschung verknüpfen. Das PROPHYLAXE-Konsortium hat erstmalig erreicht, die dem Kanal zugeschriebenen Eigenschaften und den gesamten Ansatz umfassend und tiefgreifend zu verifizieren und damit die Grundlage für eine praktische Realisierung zu legen. Im Folgenden sind die wesentlichen Innovationen zusammengefasst. Dabei wird neben der hochinnovativen Lösung für drahtlose IoT-Geräte auch eine neu entwickelte Erweiterung auf drahtgebundene Systeme sowie die Authentisierung von IoT-Geräten vorgestellt.

Benutzerfreundliches Schlüsselmanagement für drahtlose IoT-Geräte

Es gab zwei grundlegende Fragestellungen, die gelöst werden mussten: die Korrektheit (d. h. die Machbarkeit in der Praxis) des Ansatzes und die Sicherheit des Gesamtsystems.

(A) *Korrektheit der Technologie:* Die erste grundlegende Fragestellung bestand in der Klärung, ob unter den in der Realität gegebenen Rahmenbedingungen für IoT-Geräte tatsächlich kryptographische Schlüssel generiert werden können, da fast alle IoT-Geräte in der Praxis nur sehr eingeschränkten Zugriff auf die Parameter des physikalischen Übertragungskanals haben. Um eine weite, flexible Einsetzbarkeit zu erreichen, wurde die PROPHYLAXE-Technologie so entwickelt, dass allein ganz spezifische und einfach zugängliche Parameter des Übertragungskanals ausreichend sind. Diese können in allen drahtlosen Übertragungsstandards, z. B. WLAN, vom Empfangsmodul zur Verfügung gestellt werden. In PROPHYLAXE konnte nachgewiesen werden, dass diese Parameter stark zeitlich schwanken, sodass schon nach einigen Sekunden hinreichend Entropie (d. h. ausreichend Zufall) für einen kryptographischen Schlüssel vorhanden ist. Für die eigentliche Berechnung der Schlüssel sind zahlreiche anspruchsvolle Teilschritte zu lösen, die in Bild 2 dargestellt sind [10]. Eine besondere Herausforderung war neben der ausreichenden Zufälligkeit die Zuverlässigkeit, d. h. es muss sichergestellt werden, dass die beiden Kommunikationsparteien wirklich identische Schlüssel erzeugen [9].

(B) *Sicherheit der kryptographischen Schlüssel:* Die zweite kritische Frage bestand darin, ob ein Angreifer ebenfalls in der Lage ist, den gemeinsamen Schlüssel zu erzeugen. Diese Frage wurde bisher in der Literatur kaum behandelt, ist für den Einsatz der Technologie jedoch von zentraler Bedeutung. Hierfür wurden im Rahmen von PROPHYLAXE komplexe theoretische Überlegungen und umfangreiche Messkampagnen durchgeführt. Ein wesentliches Ergebnis ist, dass ein Angreifer sich in unmittelbarer Nähe des zu schützenden IoT-Geräts befinden muss. Der für einen erfolgreichen Angriff maximale Abstand beträgt

in der Regel wenige cm. Ein weiterer wichtiger Aspekt ist, dass der Nutzer seine Schlüssel fortlaufend aktualisieren kann. Hierzu reichern die beiden Kommunikationsparteien im laufenden Betrieb ihre Schlüssel fortlaufend mit „neuem Zufall" aus den übertragenden Anwenderdaten an. Dadurch ist ein Angreifer gezwungen, nicht nur während der Initialisierungsphase, sondern während der gesamten Lebensdauer des Geräts einen extrem engen Abstand zum Zielgerät einzuhalten.

Mit den beiden beschriebenen Charakteristika, korrekte Erzeugung kryptographischer Schlüssel mit hoher Entropie sowie hoher Angriffsresistenz, können nun Sicherheitssysteme mit den folgenden sehr attraktiven Eigenschaften realisiert werden [10]:

- Erzeugung kryptographischer Schlüssel zwischen IoT-Geräten mit niedrigem Rechen- und Energieaufwand. Im Zusammenspiel mit hocheffizienten, symmetrischen Verfahren wie AES oder 3DES können die Geräte nun sicher und mit Integritätsgarantie kommunizieren.
- Geräte können durch die vereinbarten Schlüssel sicher erkannt werden.
- Die PROPHYLAXE-Technologie kann auch im Zusammenspiel mit klassischem asymmetrischem Schlüsselaustausch verwendet werden, z. B. durch die Etablierung eines initialen Schlüssels mit asymmetrischen Verfahren und die anschließende Aktualisierung mit PROPHYLAXE-Technologie.
- Die vereinbarten Schlüssel sind resistent gegen Angriffe durch Quantenrechner. Alle zurzeit im Einsatz befindlichen asymmetrischen Verfahren, insbesondere RSA und elliptische Kurven, sind potenziell angreifbar durch Quantenrechner. Da diese in wenigen Jahrzehnten zur Verfügung stehen könnten, wird durch die PROPHYLAXE-Technologie Langzeitsicherheit gewährleistet.

Ein äußerst attraktiver Aspekt ist, dass die Laufzeit lediglich linear mit der Schlüssellänge anwächst, d. h. ein 256-Bit-Schlüssel benötigt doppelt so lange wie ein 128-Bit-Schlüssel. Dies ist ungemein vorteilhaft gegenüber den asymmetrischen Verfahren, die alle eine kubische Komplexität besitzen, d. h. eine Verdoppelung der Schlüssellänge führt zu einer Verachtfachung des Rechen- und Energieaufwands.

Benutzerfreundliche Authentisierung von IoT-Geräten

Neben der Verteilung und Aktualisierung von kryptographischen Schüsseln ist ein zweites grundsätzliches Problem der IT-Sicherheit die initiale Authentisierung von IoT-Geräten. Wenn ein neues IoT-Gerät in ein Netzwerk sicher integriert werden soll, muss insb. sichergestellt werden, dass das neue IoT-Gerät auch ein legitimes Gerät ist und nicht ein potenzieller Angreifer, der sich nur als solches ausgibt. Klassischerweise kommen hierfür zertifikatsbasierte Ansätze zum Einsatz, was aus Komplexitätsgründen in IoT-Anwendungen sehr oft aber nicht möglich ist. Vor diesem Hintergrund haben die PROPHYLAXE-Partner auch für dieses weitere grundlegende Problem zwei innovative Ansätze speziell für das IoT entwickelt. Bei beiden Ansätzen wird ausgenutzt, dass der Anwender neben dem IoT-Gerät über ein sogenanntes „Trusted Device" verfügt (bspw. ein Smartphone), mit dem er sich auf konventionelle Art und Weise gegenüber einem Netzwerk authentisieren kann, also bspw. unter Verwendung von komplexen asymmetrischen Verfahren. Dies ist möglich, da diese Geräte über deutlich mehr Rechenleistung und eine komfortablere Benutzerschnittstelle verfügen als viele IoT-Geräte.

Ansatz 1: Abstandsbasierte Authentisierung durch Kanaleigenschaften

In diesem Fall begibt sich ein Benutzer zur Authentisierung eines neuen IoT-Geräts mit seinem „Trusted Device" in unmittelbare Nähe des IoT-Geräts. Der Access Point, zu dem eine sichere Verbindung aufgebaut werden soll, kann dann den Übertragungskanal zu dem „Trusted Device" vermessen. Zeitgleich baut er eine Kommunikation zu dem neuen IoT-Gerät auf und vermisst ebenfalls die Übertragungsstrecke zu diesem. Somit kann er dann die gemessenen Eigenschaften beider Übertragungsstrecken vergleichen. Wenn sich das „Trusted Device" wirklich in unmittelbarer Nähe des korrekten Neugeräts befindet, sind die Kanäle sehr ähnlich und der Access Point hat somit den Nachweis, dass er mit dem korrekten Gerät spricht. Er kann nachfolgend optional einen Schlüsselaustausch, wie im vorherigen Abschnitt beschrieben, mit dem IoT-Gerät durchführen. Entscheidend für die Sicherheit des Ansatzes ist, dass ein Angreifer wieder gezwungen ist, die physikalischen Eigenschaften des Kanals zu schätzen und ggf. nachzubilden. Wie bereits dargelegt, wurde durch die aufwendigen Untersuchungen in PROPHYLAXE festgestellt, dass dies nur möglich ist, wenn er selber in unmittelbarer Nähe des angegriffenen Geräts ist. Gerade bei

Literatur

[1] Süddeutsche Zeitung: Das Internet der Dinge ist kaputt! 2016. URL: http://gfx.sueddeutsche.de/apps/58343704f38f33fb247b637d/www/, Abrufdatum 17.01.2017.

[2] IHS Technology: IoT platforms: enabling the Internet of Things, Whitepaper. 2016. URL: https://cdn.ihs.com/www/pdf/enabling-IOT.pdf, Abrufdatum 17.01.2017.

[3] Heise Security: Hacker steuern Jeep Cherokee fern. URL: http://www.heise.de/newsticker/meldung/Hacker-steuern-Jeep-Cherokee-fern-2756331.html, Abrufdatum 17.01.2017.

[4] Collao, S. E. M.: Medical Devices: Pwnage and Honeypots. URL: http://www.irongeek.com/i.php?page=videos/derbycon5/break-me14-medical-devices-pwnage-and-honeypots-scott-erven-mark-collao, Abrufdatum 17.01.2017.

[5] Bundesamt für Sicherheit in der Informationstechnik (BSI): Bericht zur Lage der IT-Sicherheit in Deutschland 2014. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf, Abrufdatum 17.01.2017.

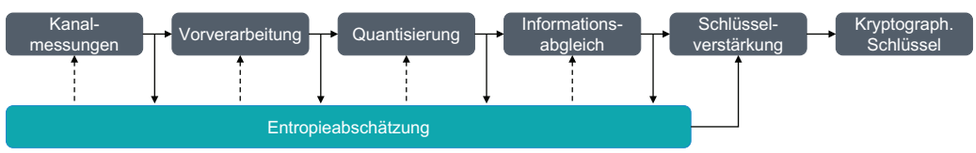

Bild 2: Module der PROPHYLAXE-Technologie zur Schlüsselerzeugung.