ComConsult Research

Der Netzwerk Insider

Februar 2016

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

Wireless Trends: IEEE 802.11ad WiGig® 60 GHz Multi-Gigabit WLANs reloaded

von Dr. Franz-Joachim Kauffels

Schon vor über fünf Jahren wurde der Standard IEEE 802.11ad für die Multi-Gigabit-Kommunikation im 60 GHz Millimeterwellen-Bereich definiert. 2012 wurde diese Entwicklung auf Eis gelegt, um den Markteintritt von 11ac nicht zu behindern. Zur CES 2016 taucht das System in einer deutlich überarbeiteten Version wieder auf und jetzt gibt es auch sofort Produkte von Endgeräten über Docking-Stationen bis hin zu einem Access Point / Router. Die Analyse zeigt, dass die Einführung von WiGig® im Consumer Bereich fast unabdingbar ist, wenn man eine Behinderung der Entwicklung des HD/UHD-Streamings vermeiden möchte.

Spannend ist die Entwicklung von Qualcomm, die dem Snapdragon 820 direkt ein kombiniertes 4G LTE / 11ac/ WiGig-Modem gibt und dies schon in Stückzahl herstellen lässt, so dass es ab jetzt auch Smartphones mit diesen Fähigkeiten gibt. Für private Netze in Unternehmen und Organisationen ergeben sich ebenfalls interessante Aspekte, die eine Antwort auf dringende Fragen darstellen könnten. WiGig ist eine sehr interessante Ergänzung der Wireless Palette.

weiter auf Seite 6

Zweitthema

Public Key Pinning - Lösung für den sicheren Einsatz von Zertifikaten?

von Sebastian Wefers und Dr. Melanie Winkler

In der heutigen Zeit findet Informationsaustausch immer häufiger online statt und es werden so auch streng vertrauliche Informationen ausgetauscht, wie beispielsweise beim Online Banking. Zur Absicherung von IP-basierten Zugriffen und insbesondere von Webzugriffen und Verschlüsselung der damit verbundenen Kommunikation hat sich in den letzten Jahren der Einsatz von Zertifikaten durchgesetzt.

Ein Zertifikat enthält, neben weiteren Angaben gemäß des Standards X.509, einen öffentlichen Schlüssel und wird durch eine Zertifizierungsstelle signiert. Der öffentliche Schlüssel ist einem privaten Schlüssel des Zertifikatsinhabers zugeordnet. Informationen, die mit dem öffentlichen Schlüssel verschlüsselt wurden, können nur mit dem zugehörigen privaten Schlüssel entschlüsselt werden. Sobald die Identität eines Zertifikatsinhabers gesichert ist, bilden Zertifikate damit die Möglichkeit zu vertraulicher Kommunikation (asymmetrischer Verschlüsselung).

weiter auf Seite 17

Geleit

Die Top 3 Netzwerk-Themen der nächsten 5 Jahre

auf Seite 2

Aktueller Kongress

ComConsult Netzwerk Forum 2016

ab Seite 3

Standpunkt

Bitfehler, eine seltene Spezies

auf Seite 15

Aktuelle Sonderveranstaltung

IT-Kommunikation im Umfeld von Fertigung und Automation

auf Seite 16

Zum Geleit

Die Top 3 Netzwerk-Themen der nächsten 5 Jahre

Die Vorbereitung des ComConsult Netzwerk Forums 2016 läuft auf vollen Touren. Und wie in jedem Jahr so arbeiten wir auch diesmal an exklusiven Inhalten und Empfehlungen für unsere Teilnehmer, die sie nur auf dem Forum bekommen können.

Naturgemäß setzt solch ein Kongress voraus, dass man Schwerpunkte setzt und wir kommen dem mit der Dreiteilung der Themen nach. Dies ist verbunden mit umfangreichen Diskussionen im Team von ComConsult Research und auch mit den Referenten.

In diesem Jahr hat dies dazu geführt, dass die Kernthemen, mit denen wir uns schon länger befassen, immer klarer werden. Wir werden sie natürlich auch auf dem Forum diskutieren, von daher will ich an dieser Stelle keine abschließenden Antworten geben. Aber ich denke, es ist wichtig, dass diese Kernthemen einmal genannt werden, da sie in Teilen deutlich vom Mainstream dessen abweichen, was im Moment in den Medien diskutiert wird:

1. Wireless-Netzwerke und die Widersprüche der Physik

Es steht außer Frage, dass den Wireless-Netzwerken die Zukunft gehört. Die weitere Zunahme mobiler Endgeräte verbunden mit der gesamten Entwicklung rund um das Internet of Things führt unweigerlich dazu, dass der Trend weg vom Kabel und hin zum Funk ungebrochen und sogar noch intensiviert voran schreiten wird. Seit Beginn dieser Technologie kämpfen wir dabei mit der Physik in einer Funkzelle. Und mehr und mehr sind wir mit den bestehenden Lösungen nicht mehr in der Lage, alle gegebenen Anforderungen zufriedenstellend zu erfüllen. Wir haben einfach physikalisch bedingt einen unlösbaren Widerspruch zwischen den Design-Zielen

- Hohe Anzahl von Teilnehmern in einer Zelle
- Hoher Durchsatz für ein einzelnes Gerät, Schlagwort Gigabit
- Umsetzung eines überschneidungsfreien Frequenzplans

Der neueste WLAN-Standards 802.11ac hat dabei mit MU-MIMO eine neue Technologie eingeführt, die tatsächlich helfen kann, die Teilnehmerzahl pro Zelle zu erhöhen (wenn dann die Teilnehmer diesen Standard auch unterstützen). Aber wir laufen in immer mehr Fällen in Probleme mit den verfügbaren Frequenzen. Und auf

Dauer wird sich dieses Problem deutlich erhöhen, wenn LTE anfängt die 5 GHz-Frequenzbänder ebenfalls zu nutzen.

Von daher kommt man einer einfachen Erkenntnis nicht vorbei: IEEE 802.11ac mag ja eine deutliche Verbesserung gegenüber den bisherigen Standards sein, aber er reicht nicht aus um ein solides Fundament für eine Wireless-Zukunft zu legen. Und tatsächlich muss man erkennen, dass eben wegen der physikalischen Grenzen kein einzelner Standard dieses Fundament liefern können wird. Die Zeiten eines einzelnen dominanten WLAN-Standards sind einfach vorbei. Die Zukunft gehört klar der Kombination von mehreren Standards und die flexible Nutzung je nach Bedarf. Die gerade in Las Vegas abgelaufene CES hat dann auch diesen Weg deutlich untermauert. Und tatsächlich sehen wir die ersten Smartphones und auch Laptops mit diesem Ansatz.

Damit bleibt aber nichts wie es war. Die etablierte gute alte WLAN-Planung ist Schnee von gestern. Wir müssen in der Planung mehrere Standards berücksichtigen und gegeneinander abgrenzen. Wie man das macht, werden wir auf dem ComConsult Netzwerk Forum diskutieren.

2. Das fehlende Session-Layer oder die Quadratur der Fabric

In den 90er Jahren ist die Standardisierung von Kommunikation unter dem Namen “Open System Interconnection OSI” gescheitert. Der Grund war die extrem hohe Komplexität dieses Standards. Statt dessen begann der Siegeszug von TCP/IP. Und dieser Siegeszug hatte genau einen Grund: TCP/IP ist simpel. Leider zahlen wir jetzt den Preis für die Simplizität. Eine IP-Adresse als Hauptadressierung für Applikationen und Geräte ist für eine ganze Reihe von Anwendungen schlicht ungeeignet. So entwickeln wir immer mehr Klimmzüge, um die damit verbundenen Probleme zu lösen. Es startete mit dem Versuch DNS als Vehikel für das Lernen von veränderten IP-Adressen zu nutzen. Das stellte sich als sehr problematisch heraus und selbst wenn alle beteiligten Geräte mitspielen ist es zu langsam. Dann hat Cisco LISP erfunden. Durch die Brust ins Auge. Aber eben der unangemessenen Einfachheit von TCP/IP geschuldet. Dann kam VMware mit NSX und Tunneln. Und damit sind wir voll im Desaster. Noch nie in der Geschichte der Datenkommunikation haben Tunnel zu irgend etwas gutem geführt. Sie sind der Alptraum der Netzwerke. Es gibt Alternativen in Form von komplexen Fabrik-Lösungen wie sie diverse Hersteller anbieten. Und natürlich geht es noch komplexer. Wir können SDN einsetzen und jede einzelne Verkehrsverbindung flexibel programmieren. Es sind ja auch nur ein paar Zehntausend.

Und warum das alles? Ganz einfach: TCP/IP hat kein Session-Protokoll. Und dieses können wir auch leider nicht für unser Forum einführen. So werden wir die verschiedenen Aushilfs-Lösungen natürlich diskutieren. Und wir werden Beispiele aus aktuellen Projekten aufzeigen, damit sie sehen, was heute geht und wie man es machen kann. Aber Sie werden sehen, dass ist äußerst unerfreulich. Hier beißt sich die Katze in den Schwanz. Das kann so nicht bleiben. Wir werden diese Situation nur lösen können, wenn TCP/IP ein Session Layer bekommt.

3. Alles oder Nichts und trotzdem gut

Aus meiner Sicht haben wir ein Problem mit existierenden Sicherheits-Lösungen und Zonen-Konzepten. Die heutige Lösung, Firewalls, IDS-Systeme usw. mitten in den Datenstrom zu stellen ist mit hohen Gigabit-Lasten schlicht unwirtschaftlich. Die Branche hat das erkannt und versucht mit NFV Software-basierte und flexiblere Lösungen zu schaffen. Aber diese Lösungen lösen ein Kernproblem nicht. Wir brauchen eine flexiblere und intelligentere Lösung. Auf der einen Seite gibt es extrem große Datenströme, die ich nicht untersuchen muss, weil ich weiß, dass sie sicher sind. Auf der anderen Seite brauche ich Flexibilität, um Datenströme Ereignisabhängig zu der im Moment besten Prüf-

Schwerpunktthema

Wireless Trends: IEEE 802.11ad WiGig® 60 GHz Multi-Gigabit WLANs reloaded

Fortsetzung von Seite 1

Dr. Franz-Joachim Kauffels ist Technologie- und Industrie-Analyst und Autor. Seit über 30 Jahren unabhängiger, kritischer und oft unbequemer Bestandteil der Netzwerkszene. Verfasser von über 20 Büchern in über 70 Ausgaben sowie über 2000 Artikeln, Videos und Reports.

Schon in 2010/2011 haben wir über WLANs im Millimeterwellen-Bereich diskutiert. Es gab verschiedene Gremien, die sich letztlich auf einen Standard geeinigt hatten. Chip-Hersteller haben damals begonnen, Muster zu bauen, die eine Serienproduktion vorbereiten sollten. Mit geringem Zeitversatz kamen aber auch Chips für die nächste WLAN-Generation im 5 GHz-Bereich nach dem Standard IEEE 802.11ac und fanden sofort reißenden Zuspruch, obwohl die erste Generation von 11ac alles andere als ausgereift war. Damals fiel die Entscheidung, die Weiterentwicklung von WLANs im Millimeterwellenbereich nach 11ad zunächst zurückzustellen, um den Markterfolg von 11ac gewährleisten zu können.

Forscht man in den älteren Dokumenten, kommt man aber auch zu dem Schluss, dass es damals noch einige Probleme mit der Balance zwischen Chip-Herstellungsprozess und Geschwindigkeit der Signalverarbeitung gegeben hat. Wie wir wissen, basiert 11ac auf der Wiederverwendung von 11n-Transceiverkomponenten, die ihrerseits eine Wiederverwendung von 11a-Komponenten sind. Moore´s Law macht es möglich, mit der Zeit immer mehr dieser vergleichsweise langsam getakteten und damit in einem preiswerten Standard-CMOS-Prozess zu bauenden Komponenten auf einen Chip zu bringen und sie eigentlich schlicht parallel zu schalten. Sieht man sich die Konstruktion von 11ac auch nur oberflächlich an, bemerkt man sofort den hohen Grad der inhärenten konstruktiven Parallelität, von der Vorcodierung bis hin zu den MIMO-Übertragungswegen.

Möchte man statt im Zentimeterwellenbereich wie 11a,n oder ac im Millimeterwellenbereich arbeiten, benötigt man mindestens für den Transceiver einen völlig anderen Herstellungsprozess für die Realisierung der integrierten Schaltkreise. Die Abbildung 1 zeigt die grundsätzlichen Zusammenhänge und nennt einige Alternativen.

Alles, was mit der MAC-Ebene und der Vorverarbeitung der Informationen zu tun hat, kann in CMOS oder μCMOS ausgeführt werden, selbst die Einführung zusätzlicher Steuerungs- und Sicherungsmechanismen erlaubt dennoch die Verwendung grundsätzlich bekannter Chip-Elemente. Das gilt auch für den eigentlichen Modem-Teil, der das Signal für die Übertragung vorbereitet. Die Qualität und Komplexität dieser Modem-Teile hat sich von 11n über 11a zu 11ac sehr deutlich verbessert, so dass hier auch mit CMOS oder BiCMOS gearbeitet werden kann. Das Front-End hingegen ist anspruchsvoll, muss das Signal doch auf einen Kanal moduliert werden, der zwischen 1,7 und 2,2 GHz breit ist und sich im 60 GHz-Band befindet. Hier helfen keine Tricks mit Parallelität, sondern es muss eine Schaltkreistechnik zum Einsatz kommen, die die notwendigen Geschwindigkeiten beherrscht, weil Schaltungen in einer solchen Technik eben schnell genug getaktet werden können. Die in Abbildung 1 zu sehenden Herstellungsprozesse haben alle die notwendige Basisqualität, brauchen aber mehr Platz als CMOS und sind deshalb auch teurer. Wunder sind hier allerdings nicht zu vollbringen, möchte man Signale über Glasfaser mit 100 Gbit/s oder mehr übertragen, benötigt man ebenfalls ähnliche Herstellungsprozesse für die Transceiver.

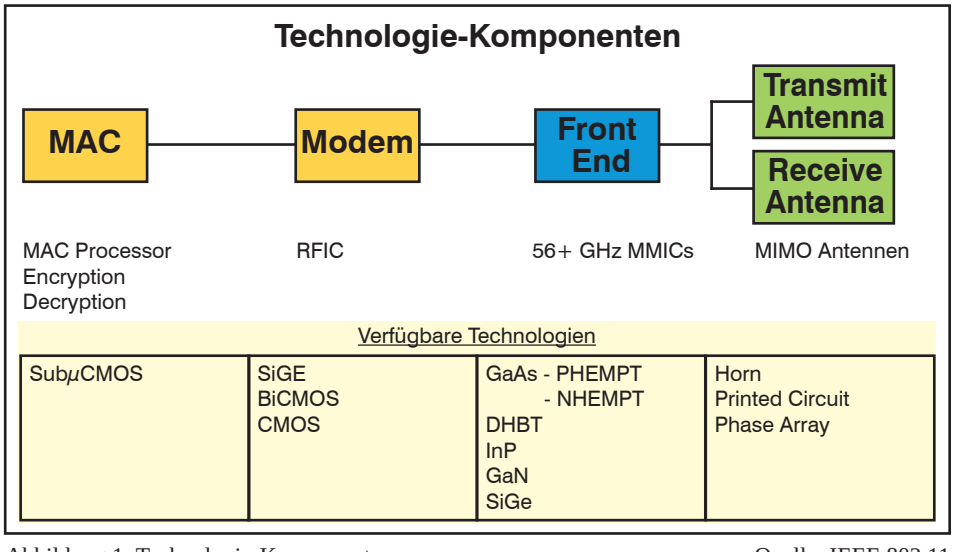

Abbildung 1: Technologie-Komponenten Quelle: IEEE 802.11

2010 war man einfach noch nicht so weit, die für 11ad notwendigen Komponenten zu einem Preis herzustellen, der den Markterfolg vor allem im Consumer-Bereich gestützt hätte. Jetzt sind wir über fünf Jahre weiter und 11ad-Transceiver können zu vernünftigen Preisen hergestellt werden.

So ist es zu erklären, dass auf der Consumer Electronics Show Anfang 2015 11ad- oder WiGig®-Komponenten, wie man es jetzt offensichtlich lieber nennt, in einer auffälligen Breite vom USB-Stick über WiGig-Notebooks bis hin zum nach Angaben des Herstellers ersten WiGig® Access Point vorgestellt wurden.

Zu diesen Komponenten kommen wir gegen Ende des Artikels. Zunächst sehen wir uns Anwendungsbereiche und die Entwicklung des Standards an.

Anwendungsbereiche für WiGig®

Stellen wir uns einfach vor, dass wie eine WLAN-Technik mit folgenden Eigenschaften haben:

- Übertragungsgeschwindigkeit bis nahezu 7 Gbps brutto
- Nur unwesentlicher Verwaltungs-Overhead, Brutto-Leistung bis zu 90% nutzbar
- Arbeitsbereich 50 – 100 qm, Leistung zum Rand hin stark abfallend
- Peer-to-Peer Modus und Access Point / Stationen-Modus
- Keine Interferenzen mit anderen Funkdiensten, lizenzfrei
- Kostenmodell für Consumer-Bereich, nicht teurer als 11ac

Was kann man damit machen? Welche Anwendungen würden optimal unterstützt?

- **Sofortige drahtlose Peer-to-Peer Synchronisation.** Geräte, die sich im Arbeitsbereich befinden, können IP-basiert mit hoher Leistung synchronisiert werden. Das können zwei Smartphones von Personen sein oder alle netzwerkfähigen Geräte, die ein Benutzer z.B. auf seinem Schreibtisch hat. Natürlich gibt es dafür auch schon andere Möglichkeiten wie Bluetooth, aber nicht mit der hohen Leistung von WiGig. Ein anderer Bereich für diese Art der Synchronisation sind Kiosk- bzw. Point of Sales-Systeme. Die Kommunikation zwischen Geräten von Kunden wie Smartphones oder Tablets und Geräten von Verkäufern wie Kassen und andere Systeme zum elektronischen Bezahlen wird in den nächsten Jahren deutlich zunehmen. Auch hier gibt es natürlich Alternativen wie z.B. NFC, die aber teilweise Durchsetzungsprobleme haben und andererseits auch nicht annähernd die Leistung von WiGig haben. Voraussetzung hierfür ist aber auch, dass der neue Übertragungsstandard wirkungsvolle Sicherheitsfunktionen besitzt.

- **Wireless Display.** Im Consumer-Bereich wurden schon zum Weihnachtsgeschäft 2015 in großen Mengen Fernseher mit 4K Ultra-HD-Auflösung verkauft, ohne dass es hinreichende Angebote für Quellen geben würde. Es wird aber so sein, dass die Streaming Anbieter wie Netflix hier die ersten sein werden, bei Netflix gibt es ja sogar schon einen Preis für ein Angebot, welches auch UHD umfasst. Die neuen Fernseher sind alle Internet-fähig, also werden sie die Streams gerne Wireless annehmen. Das wird zunächst ganz gut funktionieren, es sind aber in näherer Zukunft erhebliche Probleme abzusehen, von deren Lösung abhängt, ob diese Industrie so weiter wachsen kann wie bisher oder nicht. Das diskutieren wir gleich. Aber auch alle anderen Verbindungen zu Displays oder Projektoren werden für den Benutzer viel bequemer, wenn sie drahtlos durchgeführt werden können. Ein neues System sollte letztlich eine drahtlose HDMI-Schnittstelle implementieren um höchst mögliche Kompatibilität zu gewährleisten.

- **„Cordless" Computing.** Seit Jahrzehnten sind Arbeitsplätze auch kleine Kabelwüsten, weil man an einen Computer periphere Geräte anschließen möchte. Darüber war niemand unglücklich, bis mit neuen Geräten wie Notebooks oder Tablets und WLANs eine neue Freiheit in der Arbeitswelt und der privaten PC-Nutzung entstanden ist. Die meisten Nutzer haben heute aber die Situation, dass sie zwar draußen oder an einer gemütlichen Stelle mit dem Gerät auf dem Schoß arbeiten können, ab und an aber immer wieder an den Schreibtisch zurück müssen, um periphere Geräte anzuschließen. Zwar gibt es schon lange Einzel-Lösungen wie WLAN-Drucker, aber spätestens bei unterschiedlichen mobilen und stationären Endgeräten und Peripherie wird es schnell uneinheitlich. Außerdem sind konventionelle WLANs zu langsam, um z.B. eine anspruchsvolle Kommunikation zwischen Endgeräten und externen Speichermedien zu unterstützen. Eine gute Lösung für solche Probleme könnte ein „Wireless PCIe" sein, wenn die drahtlose Leistung stimmt.

- **Klassisches Networking.** Natürlich kann man mit einem 7 Gbps WLAN auch klassisches Networking betreiben. Clients und Server werden sich über den Leistungssprung gleichermaßen freuen. Hier ist es aber besonders wichtig, dass die Kommunikation jenseits der physikalischen Grenzen des schnellen Systems oder bei temporären Störungen nicht einfach abreißt, sondern nahtlos auf ein anderes System, wie z.B. ein 11ac-WLAN, umgesetzt wird, bis die betroffene Station wieder im Arbeitsbereich des WiGig-Systems ist und/oder das temporäre Problem nicht mehr existiert. Eine extrem elegante Variante wäre, neben einem WLAN auf anderen Frequenzen auch LTE als zusätzlichen Träger benutzen zu können.

Die Abbildung 2 gibt noch einmal einen kurzen Überblick über mögliche Nutzungsmodelle.

Das ist allerdings erst der Beginn. Es gibt zwei große Bereiche, die in den nächsten Jahren noch erhebliche Anforderungen an die drahtlose Übertragungstechnik stellen werden, nämlich IoT und UC. Darauf können wir hier aber nicht weiter eingehen.

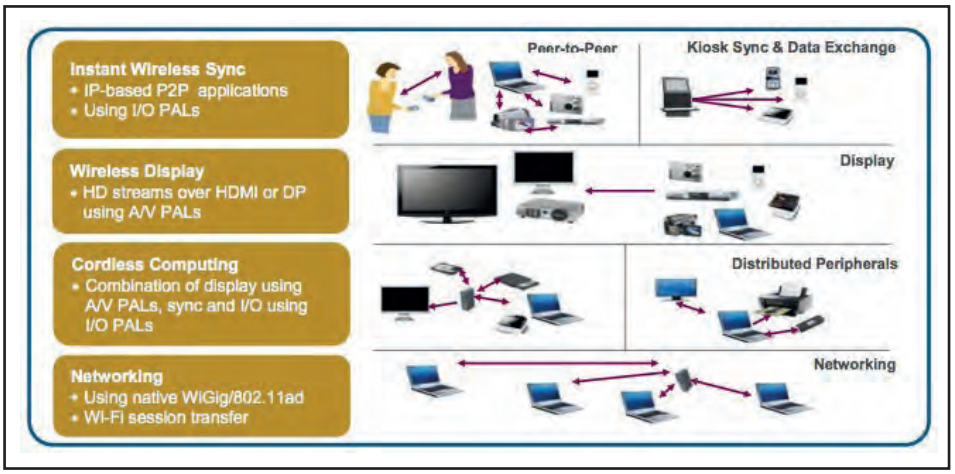

Abbildung 2: Nutzungsmodelle Quelle: WiFi Alliance

Zweitthema

Public Key Pinning - Lösung für den sicheren Einsatz von Zertifikaten?

Fortsetzung von Seite 1

Sebastian Wefers ist als Berater bei der ComConsult Beratung und Planung GmbH in den Bereichen IT-Sicherheit und lokale Netze tätig. Im Themengebiet Netzzugangskontrolle befasst er sich mit der Erstellung von Konzepten und deren praxistauglichen Umsetzung.

Dr. Melanie Winkler ist als Beraterin bei der ComConsult Beratung und Planung GmbH in dem Bereich IT-Sicherheit tätig. Dort beschäftigt sie sich besonders mit Sicherheitskonzeptionen nach ISO 27001 und BSI Grundschutz und deren Umsetzung.

Die Identität eines Zertifikatseigentümers wird über eine Zertifizierungsstelle bestätigt, indem diese das Zertifikat (und damit den öffentlichen Schlüssel) nach Prüfung der Identität des Eigentümers signiert. Auf diese Weise ist über die Signatur auch sichergestellt, dass Zertifikate nicht ohne weiteres manipuliert werden können, ohne dass dies bei einer Prüfung mittels der Signatur auffallen würde. Vertraut man darauf, dass eine Zertifizierungsstelle eine angemessene Identitätsprüfung durchführt, so kann man grundsätzlich allen von dieser Zertifizierungsstelle ausgestellten Zertifikaten vertrauen. Zertifikate bieten damit eine Möglichkeit zu verschlüsselter Kommunikation ohne manuelle Prüfung der Identität eines jeden Kommunikationspartners.

Die Verbreitung von Zertifikaten wird in den nächsten Jahren voraussichtlich noch weiter wachsen. Dies ist bedingt durch die immer größere Sensibilisierung der Öffentlichkeit hinsichtlich der Notwendigkeit vertrauliche Informationen angemessen zu schützen, welche insbesondere nach den Bekanntmachungen von Edward Snowden noch einmal zugenommen hat. Die erhöhte Verbreitung von Zertifikaten wird darüber hinaus aber auch eine erhöhte Anzahl ans Internet angebundener Geräte durch Internet of Things und durch Projekte wie Let's Encrypt gefördert, welche es auch für Privatpersonen, Vereine oder kleinere Organisationen ermöglichen, Zertifikate einfach und kostengünstig einzusetzen.

Jedoch gibt es bei dem Einsatz von Zertifikaten ein grundsätzliches Problem. Die Wirksamkeit des Schutzes durch Zertifikate steht und fällt mit der Vertrauenswürdigkeit der Zertifizierungsstellen. Es wird bei Nutzung von Zertifikaten darauf vertraut, dass die ausstellende Zertifizierungsstelle die Identität des Zertifikatsinhabers angemessen überprüft hat und diese mit den Angaben im Zertifikat übereinstimmen. Nur so ist sichergestellt, dass es sich bei dem Kommunikationspartner auch tatsächlich um die angenommene Identität handelt. In der Praxis ist dies jedoch nicht immer gegeben. Es gibt eine Vielzahl von Zertifizierungsstellen, welche Zertifikate für jeden möglichen Zertifikatsinhaber, signieren können. Die Zertifizierungsstelle legt dabei selbst fest ob und auf welche Art die Überprüfung der Identität eines Antragsstellers vor der Zertifikatsausstellung erfolgt. Sie können daher auch bewusst oder unbewusst Zertifikate auf falsche Identitäten ausstellen.

Die Struktur der Zertifizierungsstellen ist hierarchisch aufgebaut, historisch gewachsen und auf Grund dessen unübersichtlich. Jeder Browser besitzt eine Liste von Zertifizierungsstellen, welche von ihm als vertrauenswürdig eingestuft werden. Aufgrund der unübersichtlichen Struktur ist es allerdings sehr schwierig festzulegen, welche Zertifizierungsstellen vertrauenswürdig sind und es werden immer wieder Zertifizierungsstellen als solche eingestuft, die nicht vertrauenswürdige Zertifikate ausstellen. Dies liegt teilweise daran, dass Zertifizierungsstellen Zertifikate ausstellen, welche zur Ausstellung weiterer Zertifikate berechtigt sind (Zwischenzertifizierungsstellen). Die Korrektheit der von der Zwischenzertifizierungsstelle ausgestellten Zertifikate kann von der Zertifizierungsstelle nicht überprüft werden.

In der Vergangenheit hat dies schon häufiger dazu geführt, dass Zertifizierungsstellen gültige Zertifikate ausgestellt haben, bei welchen der Eigentümer des Zertifikats nicht mit den Angaben im Zertifikat übereinstimmte. So wurden beispielsweise durch die chinesische Zertifizierungsstelle CNNIC [1] und die indische Zertifizierungsstelle NIC [2] Zertifikate für unterschiedliche Google-Domänen ausgestellt. Nach einem Hackereinbruch bei der Zertifizierungsstelle Comodo [3] wurden im Namen dieser falsche aber gültige Zertifikate beispielsweise für Domänen von Microsoft, Yahoo, Google und Skype ausgestellt.

Das Problem bei fälschlich ausgestellten (gültigen) Zertifikaten ist, dass diesen vertraut wird, wenn die ausstellende Zertifizierungsstelle als vertrauenswürdig im Browser oder Endgerät einer Person gelistet ist. Der Eigentümer eines gefälschten Zertifikats ist dann in der Lage beispielsweise Spoofing oder Man-in-the-Middle (MitM)-Angriffe durchzuführen und so vertrauliche Informationen abzugreifen. Ein Angreifer könnte sich dann als Webseite für Mail-Zugriff ausgeben und sämtliche Kommunikation mitlesen.

Public Key Pinning - Lösung für den sicheren Einsatz von Zertifikaten?

Um dieses Problem zu minimieren, ist es seit einiger Zeit möglich öffentliche Schlüssel einer Webseite zu pinnen. Durch die Nutzung von Public Key Pinning (PKP) wird für HTTPS-Verbindungen festgelegt, welche öffentlichen Schlüssel genutzt werden dürfen, um HTTPS-Verbindungen zu einer Domäne aufzubauen, bzw. um Zertifikate für eine Domäne zu signieren. Dadurch, dass der öffentliche Schlüssel des Zertifikatsinhabers im Zertifikat hinterlegt ist, wird so ein Missbrauch von Zertifikaten deutlich erschwert.

Idee des Public Key Pinning

Die PKP Extension für HTTP (RFC 7469) soll die Gefahr der Nutzung fälschlich ausgestellter Zertifikate für HTTPS-Verbindungen verkleinern. Dazu wird ein zusätzlicher HTTP-Header definiert, in dem Informationen über die für die HTTPS-Verbindung zu einer Domäne zulässigen, öffentlichen Schlüssel als Hash-Wert (Pin) hinterlegt werden. Die Verknüpfung erfolgt dabei zwischen dem Domänennamen und dem öffentlichen Schlüssel, die IP-Adresse der Domäne wird nicht betrachtet.

Beim ersten Verbindungsaufbau zu einer Domäne speichert der Browser oder ein alternativer Webclient die im Header hinterlegten Informationen zu den zulässigen Schlüsseln (Trust-On-First-Use, TOFU). Die Zeit, für welche die Informationen gespeichert werden, ist im Header definiert. Bei jeder Verbindung zu einer Domäne, welche PKP nutzt, überprüft der Browser, ob für diese Domäne ein Pin hinterlegt ist und, ob dieser noch gültig ist. Falls nicht, erfolgt die Verbindung wie beim ersten Verbindungsaufbau zu einer Domäne. Sind gültige Pins vorhanden, so überprüft der Browser, ob der öffentliche Schlüssel des von der Domäne genutzten Zertifikats zu einem der gespeicherten Pins passt. Ist dies der Fall, wird der Domäne vertraut und die Verbindung wird aufgebaut, anderenfalls wird die Verbindung abgelehnt. (siehe Abbildung 1)

Bei PKP wird darauf vertraut, dass die erste Verbindung zu einer Domäne korrekt ist, das heißt, dass sich bei der ersten Verbindung kein Angreifer in die Verbindung eingeschaltet hat. PKP kann falsche Zertifikate daher nicht vollständig vermeiden, aber die Gefahr für Angriffe über Zertifikate wird verringert. PKP kann beispielsweise für Banking-Seiten genutzt werden, um die Gefahr eines MitM-Angriffs beim Online-Banking zu minimieren. Bei der ersten Verbindung mit der Domäne der Bank werden dann PKP-Informationen übertragen. Bei allen weiteren Aufrufen des Online-Banking kann nun überprüft werden, ob es sich auch wirklich um die Webseite

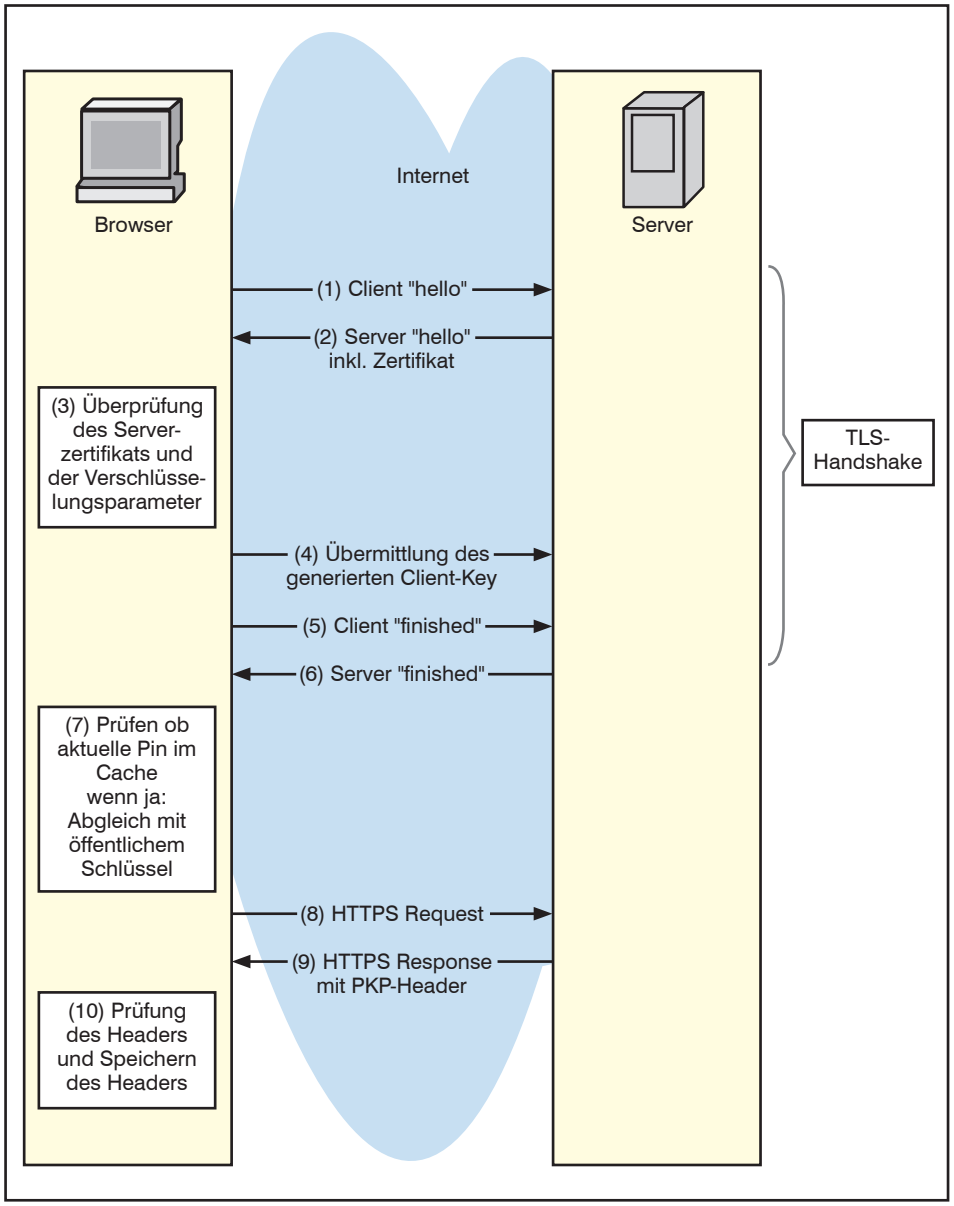

Abbildung 1: Erfolgreiche Authentisierung mittels PKP

der Bank handelt oder ob sich ein Angreifer in die Verbindung eingeklinkt hat.

Es wird empfohlen, PKP zusammen mit HTTP Strict Transport Security (HSTS) zu verwenden. Beim HSTS wird dem Browser von einer Domäne mitgeteilt, dass die Verbindung zu dieser Domäne in Zukunft ausschließlich über HTTPS erfolgen soll. So kann verhindert werden, dass PKP über die Nutzung von HTTP-Verbindungen ausgehebelt wird.

Dynamisches Pinning

PKP funktioniert, indem für eine Domäne ein weiterer HTTP-Header definiert wird, welcher unter anderem die zu prüfenden Pins enthält. Die im Header erhaltenen Informationen werden beim erstmaligen Aufruf einer Domäne direkt im Anschluss an den TLS-Handshake übertragen, im Browser gespeichert und solange diese gültig sind bei nachfolgenden Aufrufen verwendet, um die präsentierten Zertifikate und deren Pins zu validieren. Schlägt die Validierung fehl, sperrt der Browser den Zugriff auf die Domäne.

Ein PKP-Header bestehen aus den folgenden Feldern:

- pin-sha256
- max-age
- includeSubdomains
- report-uri

pin-sha256: Ein Pin ist ein base64-kodierter sha256-Hash eines Subject Public Key Information (SPKI) Fingerprints ei-