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-

Die Top 3 Netzwerk-Themen der nächsten 5 Jahre

instanz zu bringen. Das alles geht mit den vorhandenen Routing-Verfahren entweder gar nicht oder nur sehr eingeschränkt. Bis vor kurzer Zeit hätte ich gesagt, die Lösung für dieses Problem muss ein hybrides SDN-Netzwerk sein. Und SDN ist eben nicht nur eine Provider-Technologie. SDN wurde auch entwickelt, um Probleme in normalen Unternehmen zu lösen, die nicht Google oder Facebook heißen. Hier stellt sich die Frage: wie kommen wir zu einer flexiblen Steuerung von Verkehrs-Strömen. Wir werden dies mit Ihnen auf dem Forum diskutieren und dabei auch die Frage nach der Zukunft von SDN stellen.

Wären das auch Ihre Favoriten für die Netzwerk-Technologien der nächsten 5 Jahre gewesen? WLAN ist ja leicht als solche Technologie auszumachen.

Wie auch immer, Sie können sehen, wir werden auch in diesem Jahr ein ComConsult Netzwerk Forum mit viel Diskussion und auch Kontroversen haben. Es gibt eben einen Grund, warum sich hier jedes Jahr die Netzwerk-Branche trifft.

In diesem Sinne
Ihr Dr. Jürgen Suppan

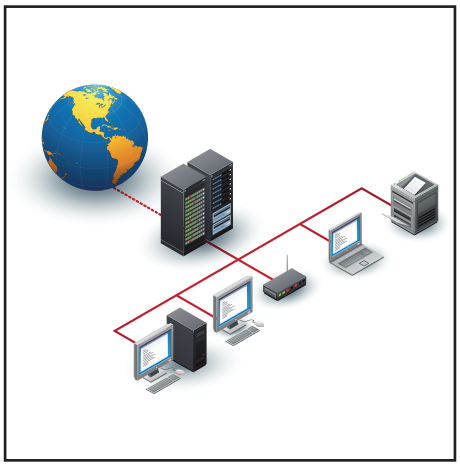
ComConsult Netzwerk Forum 2016
18.04. - 21.04.16 in Königswinter

Die ComConsult Akademie veranstaltet vom 18.04. bis 21.04.16 ihr "ComConsult Netzwerk Forum 2016" in Königswinter.

Das ComConsult Netzwerk Forum 2016 stellt die vier momentan dominantesten Netzwerk-Themen in den Mittelpunkt der Veranstaltung:

- Neue Technologien und IT-Architekturen: wie müssen sich Netzwerke ändern?
- Netzwerk-Design: skalierbare Kapazitäten, Service-orientiert und sicher
- WLAN-Design mit 802.11ac Wave 2 und die saubere Integration ins LAN-Design
- Sicherheit in Netzwerken: Zertifikate und NAC

Am ersten Tag analysieren wir u.a. ob wir zentral gesteuerte Netzwerk-Lösungen brauchen. An einer Reihe ausgewählter Anwendungsbeispiele wird untersucht, ob eine ausgelagerte Data-Plane den Betrieb, die schnelle Bereitstellung und die Gestaltung unterstützt oder ob das Ganze zu komplex wird. Hintergrund dazu ist die Frage, wie man Overlay-Netzwerke am besten konfigurieren und betreiben kann (verbunden natürlich mit der Frage, ob man sie überhaupt braucht).



Diese ergänzen wir um die praktische Frage nach der Zukunft des WAN: können sich WANs gegenüber dem Internet durchsetzen?

Am zweiten Tage steht Netzwerk-Design mit allen neuen Technologien im Vordergrund:

- Network Function Virtualization
- SDN
- 25/50/100: neue Bandbreiten für wen?
- Trill kontra Fabricpath kontra SPB kontra VXlan
- Layer 3 Design mit modernsten Technologien: wo stehen wir?

Der dritte Tag stellt zwei Sonderthemen in den Vordergrund, die in allen aktuellen Projekten eine tragende Rolle spielen und auch speziell das Jahr 2016 bestimmen werden:

- WLAN-Design nach 802.11ac Wave 2 und seine Integration in LAN-Design
- Sicherheit mit Zertifikaten und NAC

Das ComConsult Netzwerk Forum 2016 ist das richtig Forum zur richtigen Zeit.

Wir analysieren exklusiv für Sie:

- welche neuen Technologien und Produkte stehen für bessere und wirtschaftlichere Netzwerke zur Verfügung?
- wie verändern sich Anforderungen an Netzwerke?
- wie verändert sich Netzwerk-Design und wie können Sie die Vorteile zu Ihren Gunsten nutzen ohne das gesamte Netzwerk ablösen zu müssen?

Unser Vertiefungstag in diesem Jahr dreht sich komplett um IPv6 und die aktuellen Projekterfahrungen in diesem Bereich.

Fax-Anmeldung an ComConsult 02408/955-399

Ich buche den Kongress
ComConsult Netzwerk Forum 2016
18.04. - 21.04.16 in Königswinter

☐ 18.04. - 21.04.16 in Königswinter
zum Preis von € 2.590,-- netto - 4 Tage

☐ 18.04. - 20.04.16 in Königswinter
zum Preis von € 2.390,-- netto - 3 Tage

☐ Bitte buchen Sie mir ein Hotelzimmer

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Vorname _____ Nachname _____

Firma _____ Telefon/Fax _____

Straße _____ PLZ,Ort _____

eMail _____ Unterschrift _____

Programmübersicht - ComConsult Netzwerk Forum 2016

Montag, den 18.04.2016 - IT-Architekturen und neue Technologien

9:30 bis 10:30 Uhr
Die Top-Themen 2016
- Warum sich SDN in Unternehmensnetzen nicht durchsetzt (Unterschiede zwischen Unternehmens- und Hyperscaler-Netzen)
- WANs unter zunehmendem Einfluss der Entwicklungen im Internet
- Risiken des Aufschubs der IPv6-Einführung

Dr. Behrooz Moayeri, ComConsult Beratung und Planung GmbH

10:30 bis 11:30 Uhr
Cloud Computing: Einsatz im Unternehmen
- Anspruch vs. Marketing: Was ist Cloud Computing eigentlich?
- Cloud-Produkte im Unternehmenseinsatz:
  - Nutzbarkeit: Cloud-Produkte sind „anders“
  - Anforderungen an die Netzwerke und die Infrastruktur
  - Wo liegen Nutzungsgrenzen und typische Probleme
- Erfahrungen aus konkreten Projekten

Dipl.-Math. Cornelius Höchel-Winter, ComConsult Research GmbH

11:30 Uhr Kaffeepause

12:00 bis 12:45 Uhr
Internet of Things
- Was ist IoT / Industrie 4.0
- Anwendungsbereiche, Einsatz-Szenarien
- Architektur und Protokolle
- Wo steht die Standardisierung?
- IoT Roadmap der nächsten Jahre

Dipl.-Inform. Petra Borowka-Gatzweiler, UBN

12:45 Uhr Mittagspause

14:15 bis 15:00 Uhr
Wandel der Netzwerkarchitekturen in Zeiten von SDN
- Private Cloud und Hybrid Enterprise verändern die Anforderungen
- Von SDN zu SDx, sind Sie bereit dafür?
- Separierung von Underlay und Overlay Netzmanagement
- Warum Layer 3 Underlay Designs
- Für Enterprise braucht man mehr – Layer 2 over Layer 3 mit VXLAN
- VXLAN Control Plane Optionen – mit (SDN) Controller und ohne
- Wie passen VMware und OpenStack ins Bild

Dipl.-Ing. Markus Nispel, Extreme Networks GmbH

15:00 bis 15:45 Uhr
Docker: Fluten Container bald das RZ?
- Was sind Container und wie funktionieren sie?
- Wie unterscheiden sich Container von klassischen Virtualisierungstechniken?
- Was sind die Vor- und Nachteile? Was werden die typischen Anwendungsgebiete von Containern sein?
- Was sind die Konsequenzen für das Netzwerk von Rechenzentren?
- Sind Container in der Cloud?

Markus Schaub, ComConsult-Study.tv

15:45 Uhr Kaffeepause

16:15 bis 17:15 Uhr
Cloud-Computing: der rechtliche Rahmen und die Herausforderungen

Dr. Fabian Niemann, Bird & Bird LLP

ab 18:00 Uhr Happy Hour im Foyer

Dienstag, den 19.04.2016 - LAN-Design: Planung, Betrieb

9:00 bis 10:00 Uhr
SDN/NFV
- Wo steht der SDN-Markt?
- Was ist NFV? (Architektur, Einsatzszenarien, Marktbedeutung)
- Abgrenzung und Überlappung von NFV und SDN
- NFV und Network Services (Service Chaining mit NSH)

Dipl.-Inform. Petra Borowka-Gatzweiler, UBN

10:00 bis 11:00 Uhr
Netzdesign im Vergleich
- Layer 3 Design mit z.B. BGP
- Layer 2 Design mit SPB
- Layer 4 Design mit z.B. QUIC
- Lösungen wie NSX, ACI oder OpenFlow

Markus Geller, ComConsult Research GmbH

11:00 Uhr Kaffeepause

11:30 bis 12:30 Uhr
Erfahrungen mit IPv6 bei BMW
- Motivation
- Vorgehensweise
- Herausforderungen
- Erfahrungen / Probleme
- Status und Ausblick

Dipl. Ing. Bernhard Haring, BMW AG

12:30 Uhr Mittagspause

14:00 bis 14:45 Uhr
Architektur im Rechenzentrum - 25, 50 und 100G
- Einführung in eine neue Generation von offenen und skalierbaren RZ Switchen
- 25G, die neuen 10G? • 50G, die neuen 40G für Storage?
- 100G, der neue 40G Interconnect?
- Anwendungsfälle für Rechenzentren
- Remote Direct Memory Access über Converged Ethernet (RoCE) in der Praxis

Arne Heitmann, Mellanox Technologies Ltd.

14:45 bis 15:30 Uhr
Fabrics kontra Standard-Design an Projektbeispielen

Heinz Behrens, Avaya GmbH & Co KG

15:30 Uhr Kaffeepause

16:00 bis 17:00 Uhr
40 Gigabit-Ethernet und mehr: Auswahl zukunftssicherer Schnittstellen und der optimalen Verkabelung
- Simplizität der alten und Komplexität der neuen physikalischen Schnittstellen
- Schnittstellenvielfalt der Switch-Hersteller
- Unbeachtete Abhängigkeiten zwischen Elektronik und Verkabelung
- MPO war gestern, LC ist heute! Ist das so?
- Unbekannte Modul-Inkompatibilität der verschiedenen Datenraten
- Die universelle Verkabelung für alle Datenraten

Dipl.-Ing. Hartmut Kell, ComConsult Beratung und Planung GmbH

Programmübersicht - ComConsult Netzwerk Forum 2016

Mittwoch, den 20.04.2016 - WLAN-Design: Planung und Betrieb / Sicherheit

9:00 bis 10:00 Uhr

Neue WLAN-Techniken und ihr Einfluss auf Enterprise WLANs

- DCF: „Pest“ oder Segen für die Entwicklung des WLAN?
- Die dritte Welle der WLAN Chips rollt auf uns zu! Wie profitieren Enterprise WLANs davon? • MU-MIMO ist angeblich DER Schlüssel zu höherer Performance. Was ist an dieser Behauptung dran?
- Warum IEEE 802.11ac eigentlich KEIN "Gigabit WLAN" ist und es auch nie werden wird!
- Welche Anwendungen brauchen überhaupt WLAN mit mehr als 1 Gigabit/s?
- Ausblick: Parallelität wird (mal wieder) die Kapazität erhöhen

Dr. Joachim Wetzlar,
ComConsult Beratung und Planung GmbH

10:00 bis 11:00 Uhr

Wireless, aber richtig!
Von echtem Multi-Gigabit zu LTE-Erweiterungen auf dem Weg zu 5G

- Megatrend Mobilität: Status und Wachstum
- IEEE 802ad reloaded: Änderungen gegenüber der Version von 2010
- Echtes Multi-Gigabit mit 802ad/WiGig im 60 GHz-Bereich, Produktlage
- LTE Rel. 13 und LTE Advanced: Carrier Aggregation, HetNets und LTE/WiFi Interworking
- Gefährdungen durch LTE in lizenzfreien Bändern, LAA, LTE-U, MuLTEfire
- Was 3GPP schon heute für 5G vorbereitet

Dr. Franz-Joachim Kauffels,
Technologie- und Industrie-Analyst

11:00 Uhr Kaffeepause

11:30 bis 12:30 Uhr

WLAN in der Praxis: Ein WLAN für alle Umgebungen, Nutzertypen und Anwendungsfälle

- WLAN Infrastruktur: Indoor, Outdoor, Remote Office, Mesh, ZeroTouch-Provisioning, Beacons, Analytics – Was brauche ich wo ?
- Beacon-Beispiel im Enterprise: automatische Konferenzraumerkennung
- Sichere Integration verschiedener Nutzertype: Mitarbeiter, BYOD, Gäste, IoT-Devices
- IT definiert Regeln und Benutzer nutzt Self-Service Abläufe
- Firewall im Perimeter, Datacenter oder direkt im User-Access
- Applikationserkennung und Web Reputation im Access
- Nahtlose Integration von Wired-Access in das System

Reinhard Lichte,
Aruba - a Hewlett Packard Enterprise Company

12:30 Uhr Mittagspause

14:00 bis 14:45 Uhr

Fallstricke und Best Practice bei NAC

- Warum IEEE 802.1X immer noch ein Alptraum sein kann
- Best Practice NAC: Wie NAC erfolgreich umgesetzt und betrieben werden kann
- Welches Sicherheitsniveau mit NAC überhaupt geschaffen werden kann
- Ist MACsec eine Alternative?
- Evolution von NAC: Von Advanced Monitoring über Profiling bis hin zur Abwehr zielgerichteter Angriffe

Dipl.-Inform. Daniel Prinzen,
ComConsult Beratung und Planung GmbH

14:45 bis 15:30 Uhr

Sichere Kommunikation im Netz mit Zertifikaten: Alptraum oder etablierte Technik?

- Von NAC über Web-Anwendungen bis zum SSL-VPN: Anwendungen von Zertifikaten zur sicheren Kommunikation
- Fallstricke Schlüsselmanagement und Vertrauenskette: Welche Sicherheitsvorfälle es gab und was wir dagegen tun können
- Certificate Pinning und Certificate Transparency: Warum das Konzept der Vertrauenskette dringend renoviert werden musste

Dr. Simon Hoff,
ComConsult Beratung und Planung GmbH

15:30 Uhr Ende der 3-tägigen Veranstaltung -
Kaffeepause für Teilnehmer der 4-tägigen Veranstaltung

Donnerstag, den 21.04.2016 - Optionaler Zusatztag "IPv6"

ab 9:00 den ganzen Tag

IPv6 Migration: Projektvorbereitung und Umsetzung

- Organisation eines IPv6 Rollouts (Planung des Vorgehens, was muss wann entschieden werden, welche Abteilungen sind in welcher Projektphase gefordert, wo existiert Schulungsbedarf)
- Adresskonzept (Welche Alternativen stehen zur Verfügung, was sind die Vor- und Nachteile)
- Zuweisung von IPv6 Adressen (Welche Verfahren stehen zur Verfügung, wie integriert man Komponenten, die kein DHCPv6 unterstützen)
- Anforderungen an Netzwerk- und Infrastrukturkomponenten (Erstellung von Anforderungsprofilen für einzelne Komponenten, Testdurchführung, ausgewählte Testergebnisse)
- LAN-Archtitektur (Redundanzverfahren: VRRP, HSRP, Routing von IPv6, Umgang mit QoS bei IPv6)
- Migration der Internetpräsenz
- Migration von Anwendungen und Appliances
- Erstellung eines Anforderungskataloges für die Anschaffung von Hard- und Software
- Externe Anbindungen (WAN, Internet, Internet-VPN, Externe Partnerunternehmen)
- Security (Ergebnisse von Proxy-Tests, Firewalls & IDS, First-Hop-Security)

Markus Schaub,
ComConsult Study.tv

10:30 Uhr Kaffeepause
12:45 Uhr Mittagspause
15:30 Uhr Ende der 4-tägigen Veranstaltung

Folgende Aussteller nehmen bisher an der Ausstellung teil:

AixpertSoft
aruba a Hewlett Packard Enterprise company
AVAYA Engage The Power of We
ComConsult BERATUNG + PLANUNG
ComConsult Research
ComConsult Study.tv
controlware communicationssystems
Extreme Connect Beyond the Network
savvius

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.

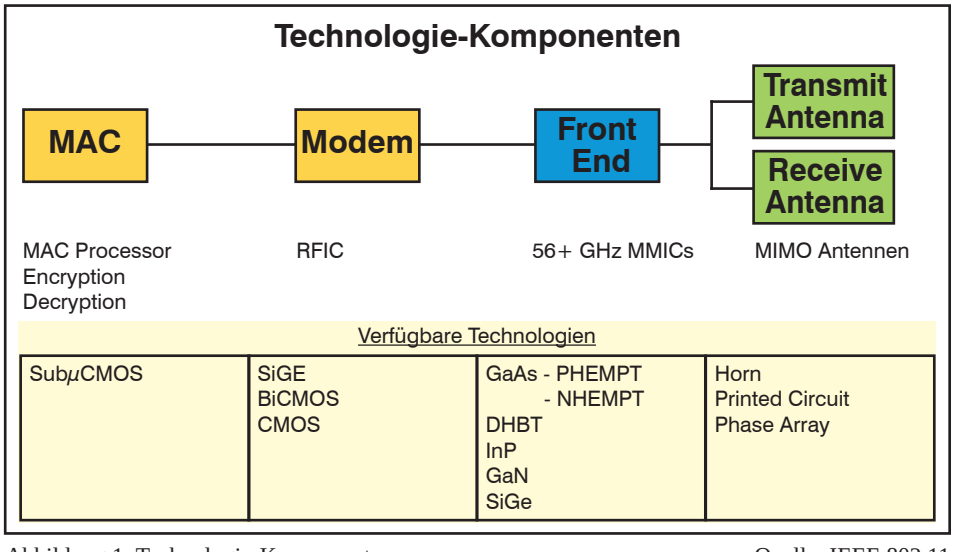


Abbildung 1: Technologie-Komponenten Quelle: IEEE 802.11

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.

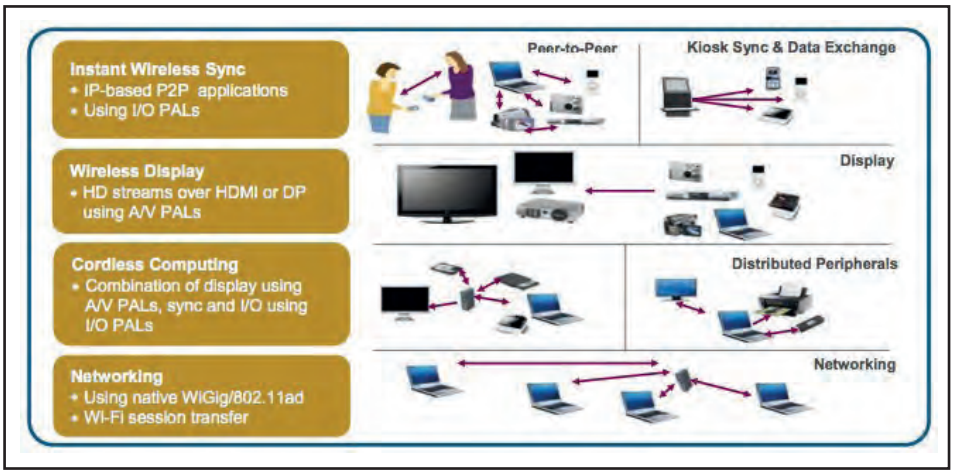


Abbildung 2: Nutzungsmodelle Quelle: WiFi Alliance

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

Noch hat man den Eindruck, dass die Einführung von WiGig „nice to have“ ist, aber es irgendwie auch ohne geht. Es gibt aber einen extrem wichtigen Sektor, wo man heute schon absehen kann, dass er sich ohne eine Technik wie WiGig nicht weiterentwickeln kann. Und dieser Bereich hängt mit folgender drängenden Frage zusammen:

Was (zum Teufel) macht ein Dutzend fremder WLANs in meinem Wohnzimmer?

Grade habe ich nochmal nachgesehen. Wenn ich auf meinem Notebook „Systemeinstellungen“ > „Netzwerk“ > WLAN ansteuere, gibt mein (betagter 11n) WLAN-Adapter die Information, dass es sage und schreibe 13 WLANs gibt, mit denen ich mich verbinden könnte. Nur eins ist meins. Das andere dreckige Dutzend verseucht einfach meinen Luftraum. Es soll ja Leute wie den Autor geben, die in Wohnungen wohnen und dort gibt es einfach dieses Problem. Bei normalem Internet-Surfen führt das zu einer erheblichen Varianz bei den Ladezeiten von Webseiten, bei eMail kann das Versenden eines kompakten Zweizeilers schon mal dauern. Ab einem gewissen Verseuchungsgrad entsteht ein erhebliches Missverhältnis zwischen der möglichen Leistung von Endgeräten und der real verfügbaren Überragungsleistung. Den Providern ist das (noch) relativ gleichgültig, sie verkaufen ihre 3Play-Lösungen an jeden der nicht wegläuft. Das Problem kennt jeder, der nicht in einem freistehenden Mini-Palast wohnt. Spricht man es auf einer Veranstaltung, wie z.B. Winterschule, an, kommt sofort Stimmung auf. Letztlich meinte ein Teilnehmer, man habe sich im Rahmen der Hausgemeinschaft auf einen Frequenzplan geeinigt. Schön für ihn, das war dann wohl eine große Nerd-WG. Ich habe z.B. eine Mischbepflanzung aus Ärzten, Freiberuflern, leitenden Angestellten, Studenten und Senioren. Die Worte „Kanal“ und „WLAN“ brauche ich schon gar nicht in den Mund zu nehmen.

Nun könnte man sagen, dass man ja schon länger mit diesem Problem lebt. Es ist aber dabei so, dass die Fernsehprogramme heute hier noch dominant überwiegend aus Kabeln kommen, entweder direkt (altes Kabelfernsehen) oder digital mit Set Top Box. Die Anbieter wie z.B. Telekom (Entertain) oder Unity Media (Horizon) verbinden die Set Top Boxen wohl wissend per Kabel (Ethernet oder Koax) mit ihrer Infrastruktur und via HDMI-Kabel mit dem TV-Gerät.

Nun gibt es aber einen völlig neuen Trend, der durch die Werbung von Amazon für den Fire TV-Stick, der die Welt des Streamings günstig erschließen soll, folgendermaßen auf den Punkt gebracht wird: „Einfach in den Fernseher stecken, mit dem WLAN verbinden und los geht’s!“ Wenn das alle hier im Haus machen, geht gar nichts mehr!! Man darf auch nicht vergessen, dass die meisten neueren TV-Geräte ohnehin Internet-fähig sind und auch einen WLAN-Adapter besitzen.

Die Realisierung multipler HD (oder gar UHD) Video-Streams in Mehrfamilienhäusern über die bestehende 11n oder 11ac-Technik wird aber enorm schnell an ihre Grenzen stoßen!

Wieso multiple Ströme? Nun, mit einem Programm gibt sich heute kaum eine Familie zufrieden. Nehmen wir ein Beispiel. Am 25.12.2015 gab es die Helene Fischer Show, „Ich einfach unverbesserlich 2“ (mit den Minions) und „Der Hobbit 2: Smaugs Einöde“ jeweils als Free-TV-Premieren GLEICHZEITIG. Wäre da noch ein halbwegs wichtiges Fußballspiel hinzugekommen, würde sich die Frage nach dem Anstieg der weihnachtlichen Mordrate schon ernsthaft stellen. Die Set Top Box Besitzer konnten wenigstens aufnehmen.

Wie schon im ersten Teil meiner Wireless Trilogie im Dezember-Insider dargestellt, gibt es den eindeutigen Trend der „Cord Cutter“ oder „Nevers“, meist jüngeren Leuten, die nie einen Kabelanschluss hatten oder keinen mehr wollen. Es gibt überhaupt keine Diskussion mehr darüber, dass der Trend für die nächste Generation Fernsehen zum Streaming über Internet geht. Die Provider weltweit rüsten schon sein mehreren Jahren ihre Backbones entsprechend auf und auch die Frage des Zubringens von Multi-Gigabit-Leistung in Wohnungen ist mit Standards wie DOCSIS 3.1 und optischen Backbones mit neuen DWDM-Techniken längst gelöst.

Provider, Hersteller von Consumer Electronics und ganz besonders Streaming Programmanbieter wie Netflix und die eher konventionellen Anbieter wie Disney werden es nicht hinnehmen, dass ein Gigabit-WLAN-Rohrkrepierer wie 11ac in überfüllten Bändern die mögliche Leistung ihrer Systeme, Geräte und Angebote beschädigt und damit ihr Geschäft ruiniert!

Der nächste WLAN-Standard 11ax ist zu weit weg, man benötigt sofort Lösungen, spätestens vor dem Weihnachtsgeschäft 2016. WiGig hat nicht nur die nötige hohe Leistung, sondern die geringe Reichweite wird jetzt zur Stärke, weil in einem Wohngebäude natürlich so viele WiGig Systeme problemlos koexistieren können, wie es Zimmer gibt!

Schließlich ist die Diskussion darüber, ob LTE nun auch noch in die lizenzfreien Bereiche vordringt, längst nicht ausgestanden. Die Prognose des Autors ist hier eher düster, weil die 5 GHz-WLANs keine wirkliche Lobby haben.

Für den Consumer Bereich gilt: WiGig wird massiv und schnell zu vernünftigen Preisen kommen. Was das für die flächendeckenden WAN-Infrastrukturen in privaten Netzen von Unternehmen und Organisationen bedeutet, diskutieren wir am Ende des Artikels.

Die WiGig®-Technologie

Die WiGig®-Technologie basiert auf der IEEE 802.11ad-Spezifikation, die ursprünglich von der Wireless Gigabit (WiGig) Alliance entwickelt wurde. Die WiGig

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

MAC- und PHY-Spezifikationen wurden 2010 bei IEEE im Rahmen des IEEE 802.11ad-Standardisierungsprozesses eingereicht und Ende 2012 verabschiedet. Normalerweise können daher WiGig und 802.11ad synonym verwendet werden. Die WiGig-Alliance verschmolz 2013 mit der WiFi-Alliance®. Die WiGig-Technologie benutzt das 60 GHz-Band zur Unterstützung von Datenraten bis zu 7 Gbps. In früheren Betrachtungen auch dieses Autors wurde nachgewiesen, dass die Chancen, dem Ziel von 7Gbps nahe zu kommen, bei 11ad wesentlich besser sind als bei 11ac, wo diese Zahl anfangs ja auch ausgegeben wurde. Das liegt u.A. an einem anderen Steuerungsverfahren, welches statt DCF eingesetzt werden kann und deterministisch arbeitet.

Der Nachteil eines WLANs im 60 GHz-Bereich liegt in den problematischen Ausbreitungseigenschaften der Millimeterwellen. Wir werden darauf später noch eingehen, aber man kann schon festhalten, dass die Reichweite von WiGig-Netzen grob auf einen nicht allzu großen Innen-Raum beschränkt ist.

Schon im Standard von 2010 war daher Beamforming ein wesentliches Thema, weil das generell zu Funküberragungssystemen bei solch hohen Frequenzen gehört. Man hatte sich damals auch schon überlegt, dass ein Endgerät transparent zu anderen Frequenzbereichen umschalten können sollte, wenn es mit der Millimeterwellen-Übertragung einfach nicht klappt.
Es ist schon an dieser Stelle wesentlich festzuhalten, dass WiGig NICHT als Substitutionstechnologie für WiFi geplant wurde, sondern als sinnvolle Ergänzung.

Durch die Verschmelzung von WiGig- und WiFi-Alliance wurde es eigentlich erst möglich, harmonische Konnektivitätslösungen unter Nutzung beider Technologie-Alternativen, die natürlich parallel betrieben werden können, zu entwickeln. Mitglieder der WiFi-Alliance haben das WiGig CERTIFIED ®-Programm entwickelt, um die Prüfung von Produkt-Interoperabilität zu ermöglichen. Interoperabilitäts-Tests haben seit 2014 stattgefunden und zertifizierte Produkte bekommen eine entsprechende Kennzeichnung.

Kurzer Überblick

Die WiGig / IEEE 802.11ad Spezifikation enthält wichtige Schlüssel-Komponenten für die Maximierung der Leistung, die Minimierung von Komplexität und Kosten, die Harmonisierung mit existierenden WiFi-Lösungen und die Unterstützung wirkungsvoller Sicherheitslösungen. In diesem Artikel werden wir die wesentlichen Elemente relativ kompakt behandeln. Für Einzelheiten z.B. zu speziellen Protokollen sei der Interessent auf die älteren Darstellungen dieses Autors verwiesen, die teilweise gratis online genutzt werden können, siehe Literaturverzeichnis. Zusammenfassend bietet WiGiG:

- Unterstützung von Datenraten von bis zu 7 Gbps. Alle Geräte, die auf der Spezifikation basieren, können mit Gigabit-Datenraten umgehen.
- Spezielles Design zur Unterstützung unterschiedlicher Endgeräte-Typen von kompakten mobilen Geräten wie Smartphones über Tablets und Notebooks bis hin zu höchst leistungsfähigen stationären oder mobilen Computern. Dies umfasst auch ein angepasstes Leistungs-Management.
- Unterstützung von WiFi-artigen Netzwerk-Implementierungen mit der Möglichkeit des transparenten Umschaltens zwischen 802.11-Netzen auf jedem Frequenzband einschließlich 2,4 GHz, 5 GHz und 60 GHz.
- Unterstützung von Beamforming zur Maximierung der Signalstärke und einer robusten Kommunikation auch jenseits der 10m-Distanz
- Sicherheit unter Nutzung des Galois/Counter Modes der AES-Verschlüsselung
- Unterstützung von drahtlosen Hochleistungs-Implementierungen von HDMI, DisplayPort, USB und PCIe

WiGig / IEEE 802.11ad definiert als Anhang zu 802.11 PHY und MAC des 60 GHz-Systems. Mit nativer Unterstützung für IP-Support über 60 GHz wird es einfacher, Transceiver zu konstruieren, die sowohl als reine 60 GHz-Systeme (mit dem verbesserten Steuerungsverfahren) als auch in Kommunikation mit existierenden 2,4- und 5 GHz-WiFi-Systemen (mit DCF) arbeiten können. Der Multi-Band-Betrieb wird über die „Upper“ MAC gesteuert. (siehe Abbildung 3)

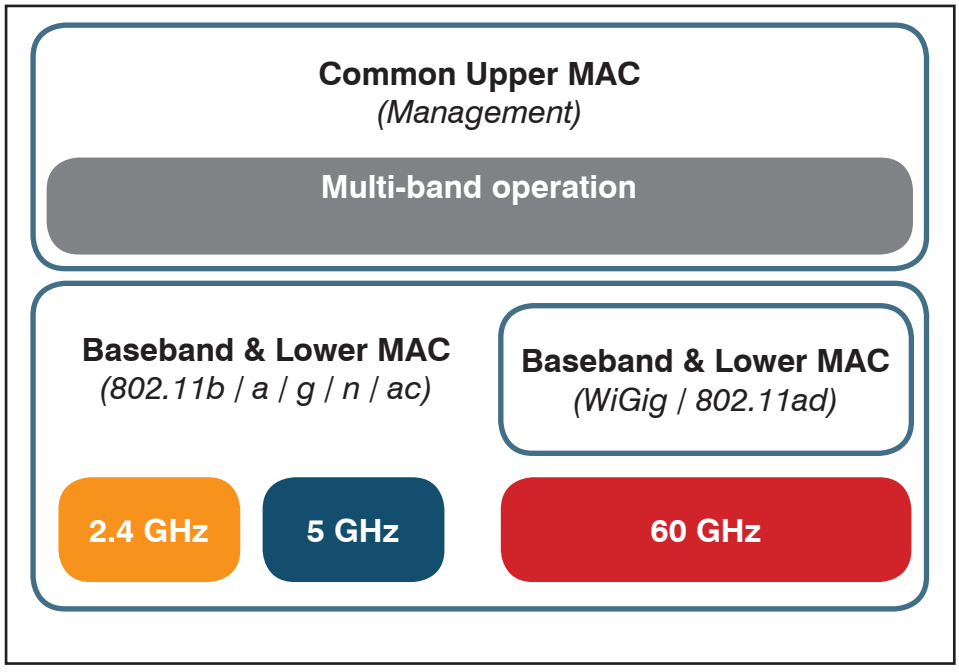


Abbildung 3: WiGig-Architektur Quelle: WiFi Alliance

Nach oben hin wird die Architektur durch verschiedene so genannte Protocol Adaption Layer (PAL) abgerundet, die die Implementierung verschiedener Datenübertragungs- und Display-Standards über die 60 GHz-Übertragungsressource unterstützen. Die PALs erlauben die Implementierung dieser Systeme direkt oberhalb der WiGig MAC & PHY neben der schon angesprochenen direkten IP-Unterstützeng. Die WiGig Display Extension WDE realisiert kabelloses HDMI, während die I/O-PALs für drahtlose SD-, USB- und PCIe-Kommunikation sorgen. Die Standards für diese Elemente sind veröffentlicht. Die hier beschriebene Menge ist ein Start-Set, was jederzeit erweitert werden kann. (siehe auch Abbildung 4)

WiGig PHY

Kommen wir zur PHY. Das lizenzfreie 60 GHz-Band ist eigentlich ein Paradies für WLANs. Es ist fast überall in weitem Bereich verfügbar, wobei es nur recht geringe Unterschiede zwischen den einzelnen Teilen der Welt gibt. Außer in China ste-

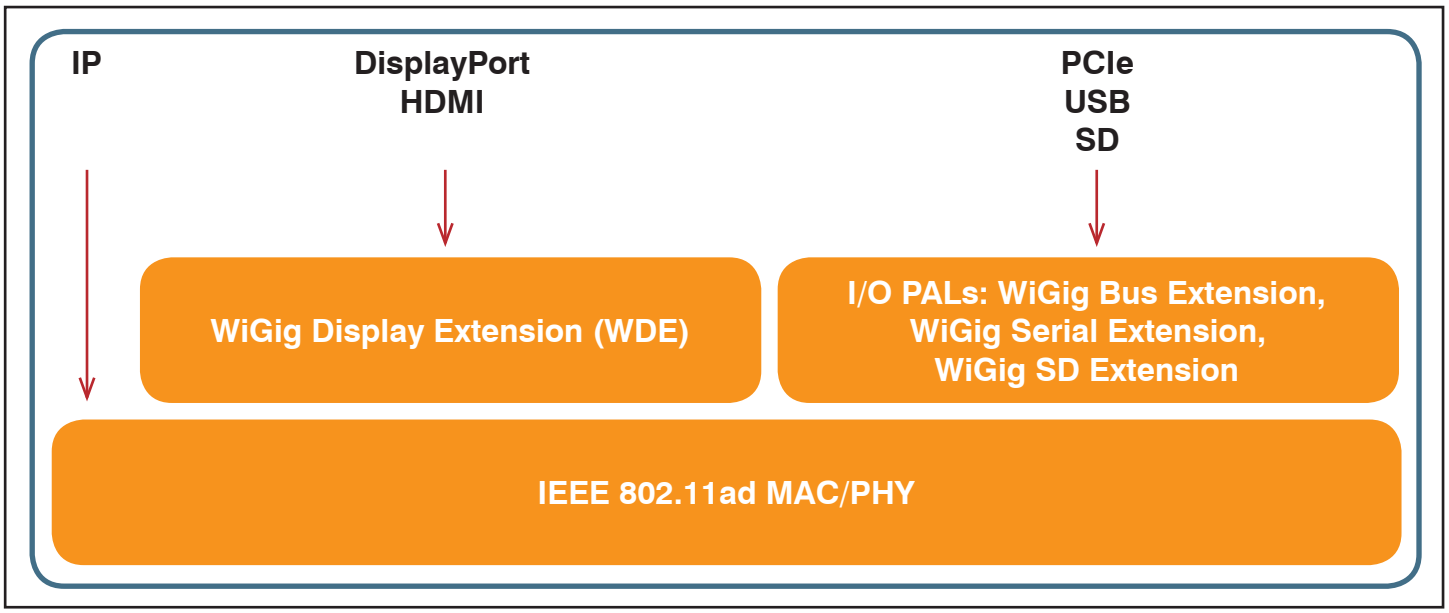


Abbildung 4: Protocol Adaption Layers

Quelle: WiFi Alliance

hen 7 oder 9 GHZ an Spektrum zur Verfügung (siehe auch Abbildung 5). Die bislang bekannten Implementierungen machen daraus vier Kanäle von der titanischen Breite 1,7 oder 2,16 GHz. Erinnern Sie sich? Im 2,4 GHz-Band haben wir für alle Kanäle zusammen eine Bandbreite von 83,5 MHz. Bei 802.11ac sprechen wir über 20, 40, 80 oder 160 MHz breite Kanäle. Aber selbst 10 160 MHz-Kanäle können es nicht mit einem einzigen WiGig-Kanal aufnehmen.

Wieso hat man nicht 10, 20 oder mehr Kanäle im 802.11ad definiert? Nun, mit den WLANs im 2,4- und 5 GHz-Bereich möchte man flächendeckende Infrastrukturen aufbauen. Dafür benötigt man mindestens drei Kanäle. Es kann aber durchaus sein, dass sich an einer Stelle mehrere WLANs überlappen oder dass man anderen Diensten, wie in Europa dem Radar, ausweichen muss. Wenn wir ehrlich sind, zu Beginn der Entwicklung war die WLAN-Kanaltrennung so schlecht, dass man in der Praxis nur einen Bruchteil der eigentlich theoretisch verfügbaren Kanäle nutzen konnte. Das hat sich mittlerweile zwar verbessert, ist aber weiterhin optimierungsbedürftig.

Im 60 GHz-Bereich kennen wir diese Probleme nicht. Mit extrem wenigen Ausnahmen gibt es hier keine anderen Funkdienste und spätestens Wände setzen der Signalausbreitung unüberwindbare Grenzen. Es geht hier einfach um Speed, nicht um Reichweite. Und wenn man nur einen Raum abdeckt, sind vier Kanäle eigentlich schon ein Übermaß. Man hat sich aber überlegt, dass man vielleicht in einer späteren Ausbaustufe auch parallele Übertragung mit mehreren Kanälen nutzen können möchte.

Die Spezifikation unterstützt zwei Arten von Modulations- und Codierungsverfahren, die jeweils unterschiedliche Vorzüge haben:

- Orthogonal Frequency-Division Multiplex OFDM unterstützt wegen ihrer Stabilität Kommunikation über größere Distanzen. OFDM hat als im 60 GHz-Bereich besonders zu nennende Besonderheit einen vergleichsweise größeren sog. Delay-Spread, der mehr Flexibilität im Umgang mit Hindernissen und Reflexionen bietet. Außerdem erlaubt OFDM die höchsten Übertragungsgeschwindigkeiten von bis zu 7 Gbps.

- Single Carrier (SC) verbraucht normalerweise weniger Leistung, was für kleine mobile Geräte wesentlich ist. Hier werden Geschwindigkeiten von bis zu 4,6 GHz realisiert.

Beide Modulations- und Codierungsverfahren nutzen gemeinsame Elemente wie die Präambel oder die Kanalcodierung. Das erleichtert die Implementierung. Um eine Zertifizierung zu erreichen, müssen alle Geräte SC unterstützen, OFDM ist optional. Bei der Initialisierung einer Session gibt es einen Austausch hinsichtlich der Modulations- und Codierungsfähigkeiten und eine kurze Verhandlung, was man denn nutzt. Das stellt sicher, dass alle zertifizierten Geräte immer miteinander kommunizieren können. Natürlich gibt es auch innerhalb eines Modulationsverfahren unterschiedliche Vorcodierungen, die letztlich unterschiedliche Signalstabilitäten repräsentieren. Je einfacher die Vorcodie-

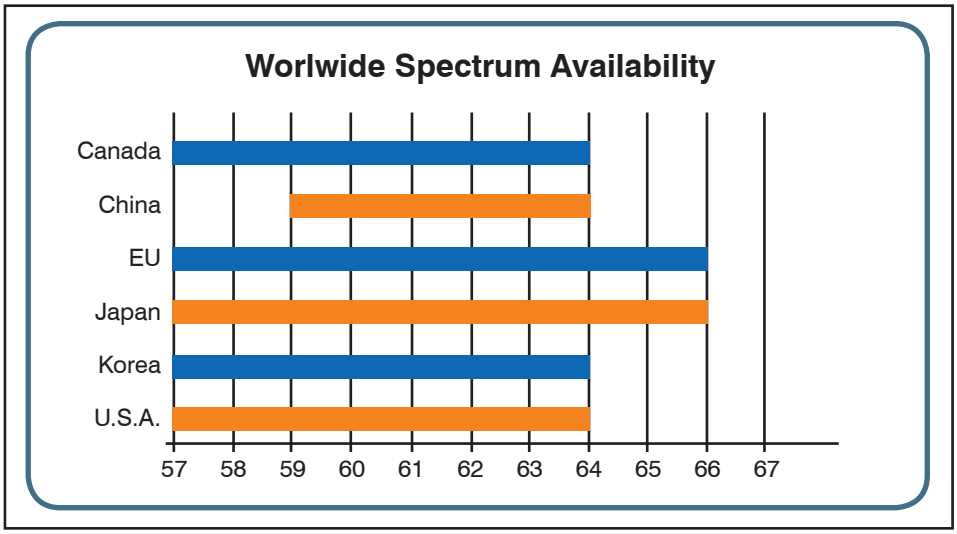


Abbildung 5: Verfügbarkeit des 60 GHz-Spektrums weltweit

Quelle: WiFi Alliance

rung, desto unempfindlicher ist das Signal. Zwei Stationen verhandeln zunächst eine Codierrate, die zu einer Geschwindigkeit führt, die das schwächere Gerät maximal unterstützen kann, denn nicht alle Geräte werden z.B. fast 7 Gbps verarbeiten können. Sollte diese Vorcodierung zu einem Signal führen, welches im laufenden Betrieb zu schwach ist, wird auf die nächste Stufen herunter geschaltet. Das kennen wir ja schon von anderen WLANs. Die Abbildung 6 zeigt die mögliche Leistung einer WiGig-Zelle mit OFDM in Abhängigkeit von der gewählten Vorcodierung.

Eine weitere spannende Eigenschaft ist jedoch, dass ein WiGig-System bei Verschlechterung der Rahmenbedingungen für die Kommunikation im 60 GHz-Band unterhalb der Möglichkeiten des Ausgleichs durch die Wahl der Vorcodierung auch in das 5 GHz- oder 2,4 GHz-Band und einen „ac-Modus“ herunterschalten kann. Das ist ein wesentliches, Praxis-orientiertes, Ergebnis der Weiterentwicklung des Standards.

Am Ende des Artikels werden wir eine sehr fortschrittliche Lösung für einen ad-Adapter vorstellen. Der kann nicht nur auf ac, sondern auch auf LTE umschalten.

Die Nutzung des 60 GHz-Bandes erlaubt extrem schnelle Kommunikation, hat aber auch das Problem, dass der Verlust bei der Signalausbreitung erheblich höher ist als in den 2,4 oder 5 GHz-Bändern. Signale im 60 GHz-Band können viel leichter durch physikalische Barrieren gestört werden als die in niedrigeren Frequenzen. Normales Mauer- oder Ständerwerk, das von den anderen WLANs zwar mit Verlust,

Modulation	Code-Rate	Datenrate (Mbit/s)
SQPK	1 / 2	693
QSPK	1 / 2	1386
16-QAM	1 / 2	2772
64-QAM	5 / 8	5197,5
64-QAM	13 / 16	6756,75

Abbildung 6: OFDM Modulations- und Codierungsschemat Quelle: IEEE 802.11ad

aber immerhin noch durchlaufen wird, ist für 60 GHz-Signale im Rahmen der durch die internationale Gesetzgebung festgelegten Grenzen für die Signalstärke völlig undurchdringlich. Ein Mensch, der sich in den Signalweg stellt, ebenfalls. Sogar Nebeltröpfchen können eine vernichtende Wirkung haben. Da das Signal physikalisch aber irgendwo hin muss, reflektiert es einfach an praktisch jedem Widerstand. Jede herkömmliche Antenne, die wir in diesem Zusammenhang einsetzen können, streut das Signal an seiner Quelle in verschiedene Richtungen. Dadurch entstehen im Zusammenhang mit den Reflexionen verschieden lange Laufwege der einzelnen Signalanteile. Das schwächt nicht nur das Signal, sondern führt auch zu unerwünschten Störungen in Form von Echos.

Die IEEE 802.11ad Spezifikation begegnet diesen Herausforderungen durch adaptives Beamforming. Diese Technik erlaubt dann auch stabile Kommunikation über Distanzen von mehr als 10m hinweg. Beamforming benutzt Richtantennen, um die Interferenzen zu reduzieren und das Signal zwischen zwei Stationen in einen konzentrierten Strahl zu focussieren und ermöglicht auf diese Weise schnellere Datenübertragung über größere Distanzen. Während des Beamformings etablieren zwei Geräte eine Kommunikation und unterziehen ihre Antennen-Einstellungen einem permanenten Fine-Tuning um die Qualität der Verbindung so weit zu steigern, bis genügend Leistung für die Realisierung der gewünschten Datenübertragungsrate vorhanden ist.

Die technische Ausführung der Richtantennen ist wegen der kürzeren Wellenlängen vergleichsweise einfacher als z.B. bei 2,4 oder 5 GHz. Es sind Felder aus mehreren Antennen, die auf einen flachen Träger oder direkt auf eine Gehäusewand des (mobilen) Endgerätes aufgebracht werden. Bis jetzt sind nur für Access Points auch größere Antennen bekannt, die aber direkt auch für geringere Frequenzen genutzt werden. Durch die Multiplikation der Anzahl der Antennen zweier kommunizierender Geräte ergeben sich entsprechend viele Kombinationsmöglichkeiten. Das Beamforming besteht einfach darin, diese schnell systematisch auszutesten und dann die aktuell stärkste Kombination zu verwenden. Da sich die Verhältnisse bei mobilen Endgeräten natürlich laufend ändern und sich die Verhältnisse im Raum ebenfalls schnell ändern können, wird das Beamforming in kurzen Abständen immer wieder neu kalibriert. Das Verfahren hat den Vorteil, auch bei allen denkbaren MIMO-Konfigurationen zu funktionieren. Hier muss man dann eben das Verhalten von Antennengruppen bewerten.

Medium Access Control MAC-Layer

In der Literatur werden ältere Quellen genannt, die die Funktionen von 802.11ad

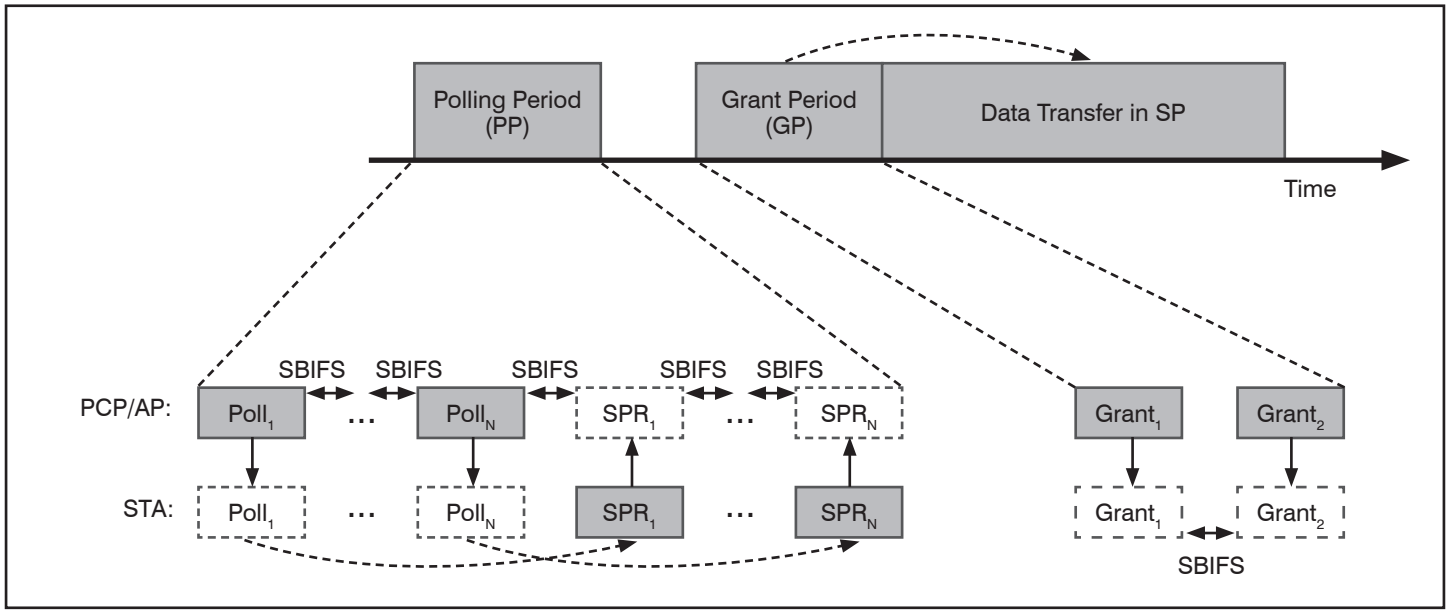


Abbildung 7: Dynamische periodische Zuordnung von Services Quelle: IEEE 802.11ad

in der Version von 2010/2011 umfangreich darstellen. Zusammenfassend gibt es neben dem aus Kompatibilitätsgründen beibehaltenen DCF-Verfahren ein sehr elegantes Request-Grant-Verfahren, das deterministisch arbeitet und daher nicht mehr bis zur Hälfte der Bandbreite verschwendet wie DCF. In diesem Verfahren gibt es Zyklen, in denen Stationen zunächst ihre Kommunikationswünsche anmelden können (Polling Phase), die anschließend systematisch und der Reihe nach abgearbeitet werden (Grant Phase und Datenübertragung). (siehe auch Abbildung 7)

Die aktuelle Version der MAC hat folgende Erweiterungen erfahren:

- **Netzwerk-Architektur:** die Spezifikation definiert eine neue Netzwerk-Architektur, die es unter Umgehung des grade beschriebenen deterministischen Steuerungsverfahrens erlaubt, dass zwei Stationen direkt miteinander kommunizieren. Das eröffnet neue Möglichkeiten im Rahmen der Anwendungen wie z.B. die schnelle Synchronisation zweier Geräte oder die Übertragung audiovisueller Daten zu einem Projektor. Zu Beginn wurde 802.11ad einfach als schnelleres WLAN entwickelt, also auch unter der Prämisse, dass es eine Reihe von Stationen in einer Zelle gibt, die um die Kapazität wetteifern. Betrachtet man die Realität aber genauer, ist es sehr häufig der Fall, dass ohnehin nur zwei Stationen in einer Zelle sind, z.B. ein Notebook und eine Docking-Station. Dann benötigt man nicht noch eine zentrale Instanz, die jetzt die Kommunikation reguliert. Zusätzlich unterstützt die Spezifikation auch existierende 802.11 Netzwerk-Architekturen einschließlich der Nutzung eines gemeinsamen Access Points für verschiedene WiFi-Netze. Das ist sehr praktisch, wie wir noch sehen werden.

- **Nahtlose Multi-Band Operation:** eine Kommunikations-Sitzung kann schnell und nahtlos von einem Kanal im 60 GHz-Band an einen Kanal in einem Band mit geringerer Frequenz, wie 2,4 oder 5 GHz umgelegt werden. Das ist für den Fall, in dem die Kommunikation im 60 GHz-Band nicht mehr möglich ist. Diese Multi-Band Betriebsweise führt zu einer erheblich verbesserten Benutzererfahrung. Nutzer, die ein integriertes WiFi/WiGig-Gerät haben, können mit der Nutzung einer Verbindung ohne spürbare Unterbrechung fortfahren, wenn ihr Gerät von einem 60 GHz-Kanal in einen WiFi-Kanal auf einer geringeren Frequenz wechselt. Die maximal nutzbare Leistung wird in diesem Fall natürlich auf das, was der WiFi-Kanal zu bieten hat, eingeschränkt. Es kann aber sein, dass das gar nicht oder kaum auffällt, weil natürlich sofort in einen 60 GHz-Kanal zurückgeschaltet wird, wenn dieser verfügbar ist.

  Das hört sich jetzt erst einmal sehr kompliziert an, hat aber einen ganz einfachen Hintergrund. Nehmen wir einmal an, ein Nutzer sitzt im Wohnzimmer und streamt grade einen Film vom Access Point auf sein iPad. Wie wir wissen, wird beim Video-Streaming ja immer von einigen Sekunden bis zu einigen Minuten vorgepuffert. Nun stellt sich eine andere Person einfach mitten in die Luftlinie zwischen WiGig AP und iPad und der Raum ist zu groß, als dass der AP eine „Umleitung“ via der Nutzung von Reflexionen finden kann. Ein normal gebauter Mensch ist ein nahezu undurchdringliches Hindernis für das Millimeterwellen-Signal. Also würde die Verbindung eigentlich abbrechen. Im Rahmen der Multi-Band Operation wird jetzt schnell z.B. in das 5 GHz-Band umgeschaltet und es ist zu mindestens für eine gewisse Zeit kein Problem, dass die Daten langsamer weiterlaufen, weil ja noch welche gepuffert sind. In jedem Fall ist es um ein Vielfaches besser als der Abbruch der Verbindung zur Video-Quelle. Ist die Person endlich aus dem Funkweg verschwunden, geht es sofort im 60 GHz-Band weiter. Bei der Entwicklung von 802.11ad gab es Hunderte Seiten Berechnungen für die mögliche Ausbreitung im 60 GHz-Bereich für bestimmte Szenarien wie Wohnzimmer, Büro, Besprechungsraum und freier Arbeitsraum. Letztlich wurden sie alle unnütz, wenn man das plötzliche Auftauchen eines Hindernisses in Äquivalenz zu der Freundin, die sich vor den Fernseher stellt, wenn grade das spannende Fußballspiel läuft, berücksichtigen möchte. Der Alltag und viele Nutzungsszenarien wimmeln von solchen Störungen, je mehr, desto länger man nachdenkt. Also war das Hinzufügen der Ausweichfunktion die einzige sinnvolle Lösung.

- **Power Management.** Es gibt einen neuen, reihenfolgeorientierten Zugriffsmodus mit dem Ziel der Senkung des Stromverbrauchs. Zwei Geräte, die miteinander über eine gerichtete Verbindung kommunizieren, können die Perioden, in denen sie aktiv kommunizieren, zeitlich genau festlegen. Zwischen diesen Perioden können sie schlafen, um Energie zu sparen. Diese fortschrittliche Möglichkeit ermöglicht es Geräten, ihr Power Management auf die aktuelle Verkehrslast zuzuschneiden und ist besonders für batteriebetriebene mobile Geräte von Nutzen. Der Sinn mag sich nicht sofort erschließen, aber eigentlich basiert die gesamte verteilte Datenverarbeitung auf Funktionen, die nach einem Zeitplan ab und an etwas machen und zwischendurch eben nicht. Einfaches Beispiel ist eMail. Ein Endgerät wie ein Notebook belagert das Postfach des Nutzers nicht in einer Endlosschleife, sondern sieht von Zeit zu Zeit nach, ob neue eMails da sind, die man herunterladen muss. Daten für die Qualität einer Verbindung werden auch nur periodisch erfasst. Dringend benötigt man eine solche Funktion im Zusammenhang mit dem IoT. Es macht z.B. keinen Sinn, einen Stromzähler alle 3 Millisekunden abzulesen und dabei unnütz Energie zu verschwenden.

- **Erweiterte Sicherheit.** Die vergleichsweise strengen Sicherheitsmechanismen in IEEE 802.11 WiGig Certified-Geräten basieren auf der Nutzung des Galois/Counter Modus der AES-Verschlüsselung. Dieser Modus hoher Effizienz ist für die Unterstützung von Hochgeschwindigkeits-Verbindungen geeignet und kann in Hardware implementiert werden.

Protocol Adaption Layer PALs

Die PALs erlauben die drahtlose Implementierung bekannter und beliebter Schnittstellen von Computern und Consumer Elektronik über 60 GHz-Netze. So können für bestimmte Anwendungen direkt Geräte mit entsprechend eingebauten Möglichkeiten produziert werden, wie z.B. drahtlose Displays. Die Definition der PALs direkt in den IEEE 802.11ad MAC & PHY ermöglicht die effiziente Implementierung in Hardware statt in einer Kombination weiterer Protokoll-Elemente mit Software-Steuerung, was die Leistung erhöht und den Verbrauch senkt. Bisher wurde folgendes definiert:

- **Audio-Video:** WiGig Display Extension WDE. WDE ermöglicht die drahtlose Übertragung audiovisueller Daten wie z.B. die Übertragung von Videos aus einem Computer oder einer Kamera auf einen Projektor oder ein Display. Dieser PAL unterstützt drahtlose Implementierungen des High Definition Multimedia Interface (HDMI ®) und des High-bandwidth Digital Content Protection (HDCP) Schemas zum Schutz digitaler Inhalte bei der Übertragung über solche Schnittstellen. Die Lösung skaliert, damit komprimierte und unkomprimierte Videos übertragen werden können.

- **I/O-PALs: WiGig Bus Extension, Wi-**

Gig SD Extension und WiGig Serial Extension. Die I/O-PALs unterstützen die drahtlose Implementierung bekannter Computer-Schnittstellen über 60 GHz. Zu den drei aktuell definierten können jederzeit weitere hinzutreten. Die WiGig Bus Extension dient der PCIe-Implementierung. Diese Schnittstelle wird in verschiedenen Ausbaustufen für die Kommunikation zwischen CPUs und Speichern zu I/O-Controllern, die Speicher, Netzwerk-Adapter und andere Schnittstellen antreiben, aber auch für Verbindungen zu Offload-Prozessoren z.B. für eine optimierte Bildverarbeitung benutzt. Die WiGig Implementierung erlaubt die drahtlose Synchronisation sowie die Kommunikation zu Speicher und anderen peripheren Einheiten mit Multi-Gigabit-Geschwindigkeit. **WiGig SD Extension.** SD Speichermedien sind ein beliebtes Instrument zur Speicherung von Daten wie Dokumenten, Fotos und AV-Inhalten auf mobilen Geräten. Die WiGig SD Extension ist so gestaltet, dass sie von einem Host-Gerät, z.B. einem Notebook, unmittelbar auf einen SD-Speicher in einem entfernten Gerät, z.B. einem Smartphone, drahtlos zugreifen kann. Natürlich könnte man die Daten zwischen den Geräten auch auf anderen Wegen austauschen. Die SD-Implementierung ist aber besonders Batterie-schonend und erlaubt einen Multi-Gigabit Datentransfer mit erheblicher Stromersparnis gegenüber anderen Alternativen. **WiGig Serial Extension:** USB wird normalerweise dazu benutzt, ein Gerät mit externer Peripherie und anderen Geräten zu verbinden. Die WiGig Serial Extension ist nichts anderes als eine Multi-Gigabit wireless USB-Schnittstelle und erleichtert die Konstruktion von Geräten wie USB Docking Stationen. Die Entwicklung wurde von der WiFi Alliance an das USB Implementers Forum (USB-IF) weitergegeben, damit dort eine medien-unabhängige Spezifikation entwickelt werden kann.

WiGig-Komponenten und Produkte

Alles deutet darauf hin, dass wir es mit einem schnell aufschäumenden Markt zu tun haben, vieles war offensichtlich schon vorbereitet und wartet nur auf seinen Startschuss. Wir können hier nur einige Beispiele nennen.

Interessant sind sicherlich die ersten Notebooks und Docking Stationen, die zeigen, dass es sich hier nicht um eine isolierte Entwicklung handelt:

- Lenovo Think Pad X1 mit Skylake Core i7 Prozessor und WiGig für ca. 1300 US$
- Lenovo Wireless Charging und WiGig Monitor Dock für 250 US$

Abbildung 8: ACER Travel Mate P 648 Quelle: ACER

- ACER Travel Mate P 648 ab ca. 800 US$
- DELL 5000 WiGig Docking Station ab 36,- € bei amazon
- HP Advanced Wireless Docking Station für 350 US$

Natürlich kann man Notebooks auch nachrüsten, z.B. mit dem WiGig® USB-Adapter von Sibeam. Es gibt auch weitere Referenzarchitekturen, wie z.B. die HYDRA System IP Architektur von Blu Wireless.

Sehr auffällig ist natürlich der nach Angaben des Herstellers „Erste 11ad/WiGig®“ Router, der Talon AD 7200 von TP-Link. Er hat nicht nur die Möglichkeit, Verbindungen nahtlos von WiGig® auf 802.11ac umzuschalten, wenn das nötig ist, sondern kann auch WiGig® und 11ac parallel benutzen. Damit kommt er mit 7,2 Gbps auf eine Maximal-Leistung jenseits der 11ad-Spezifikation. Lediglich die Ausstattung mit nur vier Gigabit Ethernet-Schnittstellen für den Uplink erscheint mickrig. Das wird in der Serie ab Sommer sicher besser. (siehe Abbildung 9)

Technisch basieren die Lösungen natürlich auf entsprechenden Chipsets. Bekannt ist der WiGig-Chipset von Peraso

Abbildung 9: TP-Link AD 7200 WiGig Router Quelle: TP-Link

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

Abbildung 10: Qualcomm Tri-Band Adapter Quelle: Qualcomm

mit verschiedenen interessanten Kommunikationsmöglichkeiten und der WiGig Chipset von Wilocity. Dieser Hersteller ist wirklich von Beginn an bei der 802.11ad Entwicklung. Nun haben wir ja gesehen, dass WiGig alleine noch keinen wirklichen Sommer macht, es sollte mindestens mit 11ac kombiniert werden. Für 11ac gibt es einen bekannten Chipset von Atheros. Wie praktisch, dass dieses Unternehmen zu Qualcomm gehört und es auch eine gute Zusammenarbeit mit Wilocity gibt. So entsteht der erste Tri-Band Adapter für ad/ac mit 60/5/2,4 GHz. (siehe Abbildung 10)

Technisch noch spannender ist allerdings der nächste Schritt, den Qualcomm mit den Konnektivitäts-Möglichkeiten des neuen Snapdragon 820-Prozessors gemacht hat. Kern ist ein neuerlich erweitertes X12 LTE-Modem, welches zusammen mit anderen Funktionen des Prozessors die heute aktuellsten Ausbaustufen von 4G LTE und WiFi für Mobilgeräte der Oberklasse anbietet. Die Funktionen / Leistungen sind:

- LTE Advanced
  - Cat. 12 (bis zu 600 Mbps) im Downlink (33 % mehr als Cat. 10)
  - Cat. 13 (bis zu 150 Mbps) im Uplink (200% mehr als Cat. 10)
  - Bis zu 4X4 MIMO in einem Downlink-LTE-Träger

- Konnektivität in lizenzfreien Bereichen
  - 2X2 MU-MIMO (802.11ac)
  - Multi-Gigabit 802.11ad
  - LTE-U
  - LTE + WiFi Link Aggregation (LWA)

- Unterbrechungsfreie Dienste über verschiedene Verbindungsarten
  - Next Gen HD Voice & Video Calling über LTE und WiFi (HD Voice over LTE (VoLTE) und Video over LTE (ViLTE). Ein spezieller Monitor überwacht die Real-Zeit-Qualität des WiFi und entscheidet, ob man zu LTE und ggf. zurück schalten muss.
  - Verbindungskontinuität über WiFi, LTE, 3G und 2G

- RF Front End Innovationen
  - Advanced Closed Loop Antennen Tuner
  - Qualcomm 360 Grad Front End Solution
  - WiFi / LTE Antennen-Sharing

Das X12-LTE-Modem ist nicht nur im Zusammenhang mit dem Prozessor, sondern auch einzeln erhältlich und konnte mit dreifacher Carrier Aggregation und 256 QAM eine Spitzenleistung von 600 Mbps mit LTE erreichen. Der Snapdragon 820 ist der erste öffentlich verfügbare Prozessor mit 4X4 LTE MIMO Support und kann auf diese Weise den Durchsatz eines einzelnen LTE Carriers verdoppeln. Die maximale11ac-Leistung mit 2X2 MIMO 80 MHz-Kanälen beträgt 867 Mbps, während 11ad auf bis zu 4,6 Gbps kommt. WiGig wird also hier mit SC-Modulation implementiert, dem besonders stromsparenden Modus. Das reicht natürlich locker für 4K Streaming.

Man kann durchaus sagen, dass zu Beginn 2016 der Snapdragon 820 mit seinen Kommunikationsmöglichkeiten eine wirklich fortgeschrittene Komponente darstellt. Er wird ab Mitte Januar von Samsung im 14 nm FinFET-Prozess hergestellt. Es gibt auch schon ein erstes Smartphone mit diesem Prozessor vom chinesischen Anbieter LeTV, aber auch Samsung wird den Prozessor in seiner Premium Reihe S7 verwenden.

Fazit und Konsequenzen

WiGig ® ist eine wichtige Komponente im zukünftigen Wireless-Spektrum. Im Consumer-Bereich ist es nicht mehr weg zu denken, wie bereits ausführlich dargestellt wurde. Es ist in keinem Fall eine Substitution für 11ac WLANs, sondern eine sinnvolle Ergänzung.

Unternehmen und Organisationen, die ihre eigenen flächendeckenden drahtlosen Infrastrukturen betreiben möchten, müssen natürlich wie bisher auch eine professionelle Systemplanung für 11ac vornehmen lassen. WiGig ist dabei zunächst eine Art Joker, den man immer einsetzen kann, wenn aus welchen Gründen auch immer die 11ac-Leistung nicht ausreicht. Das kann sofort passieren, oder aber erst in einigen Jahren mit der Einführung qualitativ sehr hochwertiger UC-Lösungen.

Sollte tatsächlich der Ernstfall eintreten und die lizenzfreien Bereiche auch für LTE freigegeben werden, wird es an einigen Stellen wie bereits im letzten Artikel beschrieben zu bösen Überraschungen kommen. Auch hier ist WiGig hilfreich, weil eine Zelle sozusagen in einem Raum eingeschlossen ist und auch von außen nicht gestört werden kann, etwa wie Rapunzel. Was sicher nicht so gut funktioniert ist die Einführung einer flächendeckenden 11ad-Lösung in großen Räumen, wie z.B. Großraumbüros. Bis wir dazu gute Aussagen machen können, müssen wir messen, probieren und die Produktentwicklung abwarten.

Allerdings ist die Infrastruktur-Anbindung der (vielen kleinen) WiGig-Zellen nicht ganz umsonst. Man wird Zellen zunächst mit Lösungen nach den neuen Ethernet-Standards für 5 Gbps anbinden können, mittelfristig wird man aber um 10 GbE kaum herumkommen. Hier wäre eine Weiterentwicklung wünschenswert, die 10 GBASE-T auch über „schlechtere“ Leitungen ermöglicht, so wie DOCSIS das mit alten Telefonkabeln macht. Technisch nach Ansicht des Autors kein Problem, nur die Gremien müssen es machen.

Der Snapdragon von Qualcomm zeigt allerdings, wohin die Entwicklung ab jetzt gehen wird. Wir werden eine neue Generation mobiler Endgeräte bekommen, die nicht nur mit allen verfügbaren Funkdiensten klar kommen, sondern sie auch noch sinnvoll ZUSAMMEN nutzen können. Das ist eine ganz neue Qualität, die das Leben sicherlich an einigen Stellen erheblich erleichtert und eine gewisse innere Abstraktion von den einzelnen Funkdiensten erlaubt.

Literatur

Kauffels, F.-J.: „Multi-Gigabit Wireless nach IEEE 802.11ad und WiGig“, Teil 18 der Reihe „Professionelle Datenkommunikation“ auf www.comconsult-research.de

Kauffels, F.-J.: „Multi-Gigabit Wireless Netzwerke“, Video von 2010, www.comconsult-study.tv , Themenbereich WLAN

Standpunkt

Bitfehler, eine seltene Spezies

Der Standpunkt von Dr. Joachim Wetzlar greift als regelmäßiger Bestandteil des ComConsult Netzwerk Insiders technologische Argumente auf, die Sie so schnell nicht in den öffentlichen Medien finden und korreliert sie mit allgemeinen Trends.

Erinnern Sie sich noch an die Zeiten, in denen man Ethernet mit Koaxialkabeln („Yellow Cable“ bzw. „Cheapernet“) aufbaute? Oder haben Sie vielleicht einst ein Token-Ring-Netz betrieben? Dann wissen Sie, dass es in diesen Netzen häufig Fehler gab, die auf der Schicht 1 des OSI-Referenzmodells zu suchen waren. Kollisionen im Ethernet führen zu Bitfehlern und auch der Token Ring war nicht frei von Effekten der Schicht 1, wie z.B. das gefürchtete „Beaconing“. Heute findet man derlei Effekte noch im Wireless LAN; eine gute Kenntnis der Physik drahtloser Übertragung ist für den WLAN-Betrieb unabdingbar.

Bei drahtgebundenen Netzen hat sich das Thema scheinbar erledigt. Die große Mehrzahl der Fehlersituationen, die ich untersuche, treten auf den OSI-Schichten 4 bis 7 auf. Es sind also häufig Komponenten der Anwendungen oder die TCP Stacks, die zu Problemen führen.

Mit einem solchen Problem hatte ich es neulich offenbar zu tun: Der Kunde betreibt weltweit eine ERP Software, die an seinem zentralen Rechenzentrum „gehostet“ ist. An einer Außenstelle traten regelmäßig Verbindungs-Abbrüche während des Login-Vorgangs an der ERP Software auf. Der Client meldete „Connection Reset by Peer“. Aha, „Reset“ ist ein Mechanismus des Transmission Control Protocol (TCP), ausgelöst durch den TCP Stack oder durch einen Fehler der ihn nutzenden Anwendung.

Eine erste Protokollanalyse im Rechenzentrum des Kunden zeigte, dass ab einem bestimmten Punkt keine Pakete mehr vom Client empfangen wurden. Schließlich gab der Server auf und sendete „Reset“. Jetzt war die Gegenprobe auf der Seite des Clients zu machen. Eine lokal installierte Protokollanalyse-Software auf dem Client (z.B. „Wireshark“ oder „Tcpdump“) zeigte, dass der Client ein bestimmtes Paket wiederholt in Richtung des Servers aussandte, von diesem aber nie eine Bestätigung dafür erhielt. Schließlich war das „Reset“ des Servers zu erkennen.

Ein bestimmtes Paket wurde nicht übertragen, trotz mehrfacher Wiederholung. Was konnte die Ursache dafür sein? Wir vermuteten zunächst, ein bestimmtes Muster im Paket würde vom Intrusion Prevention System (IPS) am Standort fälschlicherweise verworfen („False Positive“). Entsprechende Einträge im Log des IPS konnten wir jedoch nicht ausmachen.

Eine Messung hinter den IPS sollte den Beweis erbringen. Dank eines fernbedienbaren Protokollanalysators und eines freundlichen Mitarbeiters in der Außenstelle war das schnell eingerichtet: Nun konnten wir den Datenverkehr unmittelbar am Ethernet-Anschluss des Provider-Routers beobachten, der den Standort mit dem Weitverkehrsnetz verbindet. Und auch hier waren alle Pakete des Clients zu sehen. Also auch dasjenige, welches den Server nie erreichte. Wir konnten letztlich nachweisen, dass das Paket irgendwo im Providernetz verlorenging.

Aber es kam noch besser: Zur späteren Dokumentation wollte ich die Paketaufzeichnung vom Protokollanalysator der Außenstelle herunterladen. Doch das schlug fehl – Timeout! Auch hier ergab die Protokollanalyse, dass ein bestimmtes Paket nicht übertragen werden konnte. Klar: Wenn ein bestimmtes Bitmuster die Ursache war, steckte dieses ja in genau der Paketaufzeichnung, die ich nun übertragen wollte.

Durch Vergleich der verworfenen Pakete konnte ich dieses Bitmuster isolieren – eine auffällige Folge von Nullen und Einsen. In eine kleine Datei gepackt, ließ sich auch diese nicht von der Außenstelle über das Provider-Netz übertragen. Von unseren Beobachtungen überzeugt, hat der Provider später eine Komponente getauscht und damit das Problem beseitigt.

Die eigentliche Ursache für das Problem habe ich letztlich nicht herausfinden können. Es ist aber die Vermutung erlaubt, dass die fragliche Bitfolge bei irgendeiner Komponente zu einer Fehlinterpretation von Bits geführt hat. Die OSI-Schicht 2 würde in diesen Fällen das Paket wegen falscher Prüfsumme verworfen haben. Und das kann der Netzbetreiber (hier der Provider) an den entsprechenden Fehlerzählern im Netzmanagement erkennen.

Was lernen wir daraus? Erstens ist es gut, über Messmöglichkeiten an verschiedenen Orten zu verfügen, um derlei Nachweise führen zu können. Fernbedienbarkeit der Messmittel ist dafür eine wichtige Voraussetzung. Und Mitarbeiter vor Ort, die soweit geschult sind, dass sie bei Aufbau und Einrichtung im Zweifel unterstützen können.

Zweitens habe ich gelernt, dass es tatsächlich „verrückte“ Effekte auf der Ebene der Bitübertragungsschicht geben kann, die in seltenen Fällen zu Fehlern führen. So selten, dass sie durch die Maschen des Netzmanagements hindurchfallen. Vergleichbare Effekte haben meine Kollegen übrigens auch schon in Fiber Channel SANs gefunden, mit ebenso „verrückten“ Auswirkungen.

Fazit: Fehler auf der Bitübertragungsschicht sind selten geworden. Umso unerwarteter sind ihre Auswirkungen.

Aktuelle Sonderveranstaltung

IT-Kommunikation im Umfeld von Fertigung und Automation 13.06. - 14.06.16 in Bonn

Die ComConsult Akademie veranstaltet vom 13.06. bis 14.06.16 ihre Sonderveranstaltung "IT-Kommunikation im Umfeld von Fertigung und Automation" in Bonn.

Fertigungsnetze unterscheiden sich von Büronetzen. In Fertigungsnetzen werden eine hohe Verfügbarkeit, die Vermeidung unnötiger Bedrohungen und trotzdem hohe Flexibilität erwartet. Mit der aktuellen Technologie-Entwicklung stellt sich aber immer mehr die Frage, ob eine klare Trennung zwischen Büro und Fertigung in Zukunft erreichbar sein wird. Es stellt sich auch die Frage, ob wir nicht über genügend leistungsfähige Architekturen und Werkzeuge verfügen, um einen Grad an Schutz und Kontrolle zu etablieren, der die Kombination aus Sicherheit, Leistung und Flexibilität möglich macht.

Während über Konzepte wie Internet of Things (IoT) und Smart Home überwiegend visionär gesprochen wird, haben produzierende Unternehmen schon seit Jahren eine stark steigende Anzahl von Geräten in ihren Industrienetzen. Insofern ist für diese Firmen die vierte industrielle Revolution kein Bruch mit dem Bisherigen, sondern die konsequente Fortsetzung der dritten, nämlich der Automatisierung.

Mit der aktuellen Technologie-Entwicklung stellt sich immer mehr die Frage, ob eine klare Trennung zwischen Büro und Fertigung in Zukunft noch erreichbar sein wird. Diese Sonderveranstaltung analysiert wie Fertigungsnetzwerke auf diese Herausforderungen reagieren können und wie mit geeigneten Technologien Sicherheit, Leistung und Flexibilität gewährleistet werden kann.

In diesem Seminar lernen Sie
- Wo stehen wir technologisch im Bereich Fertigungsnetze?
- Was wollen wir oder wozu werden wir gezwungen?
- Wie kann ein guter Weg in die Zukunft aussehen?

Durch die Veranstaltung führen Sie:
Dr. Simon Hoff ist technischer Direktor der ComConsult Beratung und Planung GmbH und blickt auf jahrelange Projekterfahrung in Forschung, Standardisierung, Entwicklung, Planung und Betrieb in den Bereichen IT-Sicherheit, lokale Netze und mobile Kommunikationssysteme zurück.

Dipl.-Ing. Hartmut Kell ist Leiter des Competence Center IT-Infrastrukturen der ComConsult Beratung und Planung GmbH vermittelt sein Fachwissen aus umfangreichen Praxiserfahrungen bei der Planung, Projektüberwachung, Qualitätssicherung und Einmessung von Netzwerken in Form von Publikationen und Seminaren.

Dr.-Ing. Joachim Wetzlar ist seit mehr denn 20 Jahren Senior Consultant der ComConsult Beratung und Planung GmbH und leitet dort das Competence Center „Data Center“. Er verfügt über einen erheblichen Erfahrungsschatz im praktischen Umgang mit Netzkomponenten und Serversystemen. Neben seiner Tätigkeit als Trouble-Shooter führt Herr Dr. Wetzlar als Projektleiter regelmäßig Netzwerk- WLAN- und RZ-Redesigns durch.

Fax-Antwort an ComConsult 02408/955-399

Anmeldung

IT-Kommunikation im Umfeld von Fertigung und Automation

Ich buche das Seminar
IT-Kommunikation im Umfeld von Fertigung und Automation

☐ 13.06.-14.06.16 in Bonn
zum Preis von € 1.590,-- netto

☐ Bitte buchen Sie mir ein Hotelzimmer

Buchen Sie über unsere Web-Seite
www.comconsult-akademie.de

Vorname	Nachname
Firma	Telefon/Fax
Straße	PLZ,Ort
eMail	Unterschrift

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

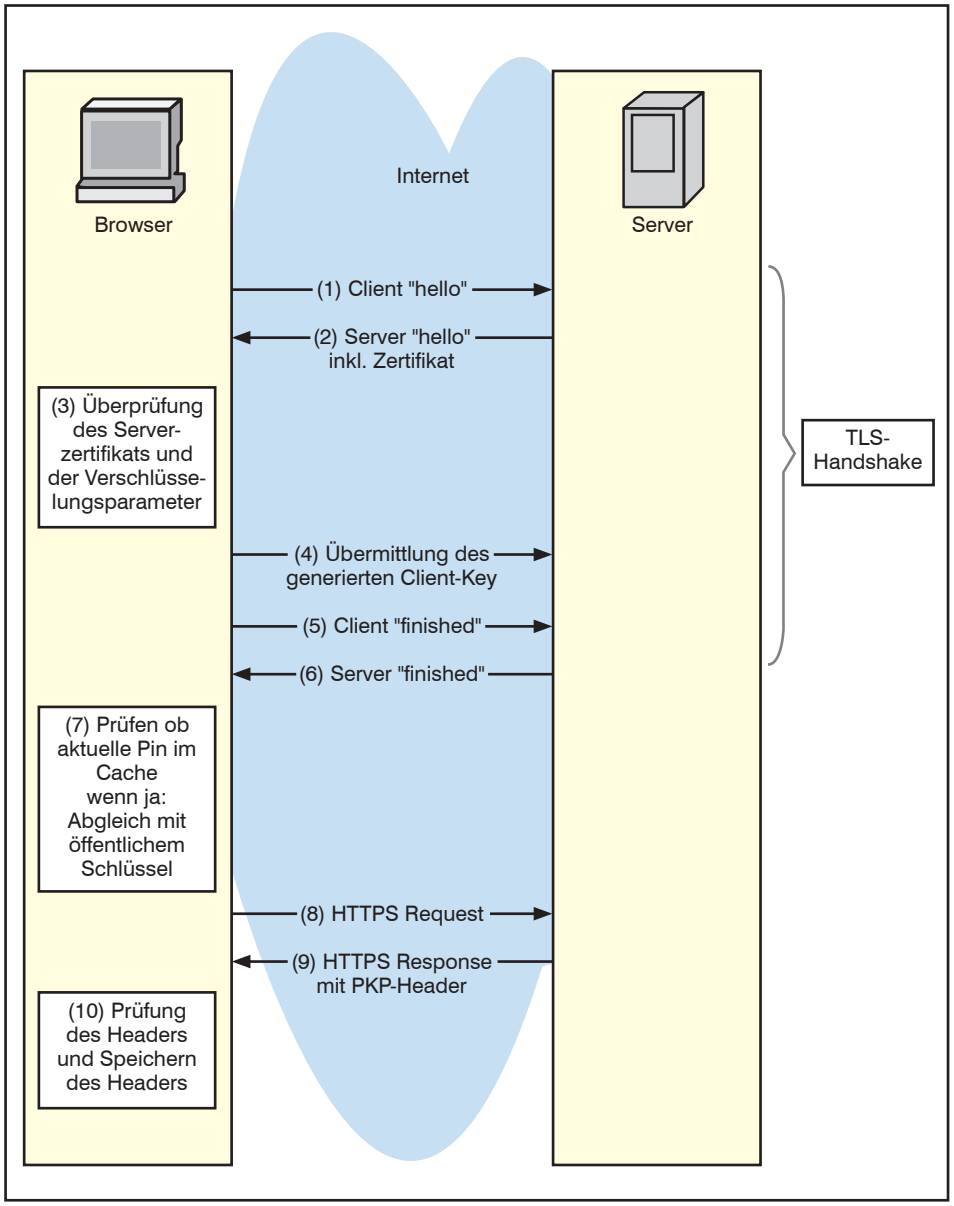


Abbildung 1: Erfolgreiche Authentisierung mittels PKP

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-

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

nes öffentlichen Schlüssels. Dabei stellt die SPKI nur einen Teil des öffentlichen Schlüssels dar. Innerhalb eines PKP-Headers können mehrere Pins definiert werden. Der RFC 7469 verpflichtet dazu mindestens zwei Pins zu definieren:

- Der erste Pin ist dabei die Information über einen, sich derzeitig in der verwendeten Zertifikatskette befindenden, öffentlichen Schlüssel.

- Zusätzlich wird als weiterer Pin ein sogenannter Backup Pin definiert, der die Informationen eines öffentlichen Schlüssels beinhaltet und nicht in der derzeit verwendeten Zertifikatskette vorkommt. Dieser gepinnte öffentliche Schlüssel kommt zum Einsatz, wenn der eigentliche öffentliche Schlüssel nicht mehr genutzt werden kann, zum Beispiel weil dieser kompromittiert oder gesperrt wurde, abgelaufen oder verloren gegangen ist.

- Wird als Backup-Pin der Schlüssel eines Serverzertifikats verwendet, so sollte dieses Zertifikat sicher gespeichert werden und unbenutzt sein. Wird der öffentliche Schlüssel einer Zertifizierungsstelle als Backup-Pin verwendet, so muss sichergestellt werden, dass diese in der aktuellen Zertifikatskette nicht verwendet wird. In diesem Fall können von der gepinnten Zwischenzertifizierungsstelle neue Zertifikate für die Domäne erstellt werden.

Gepinnt werden können öffentliche Schlüssel von Serverzertifikaten, von Zertifikaten von Zwischenzertifizierungsstellen oder Zertifizierungsstellen. Die Entscheidung welche öffentlichen Schlüssel und damit welche Art von Zertifikaten gepinnt werden, kann weitgehende Konsequenzen mit sich bringen und sollte deswegen wohl überlegt getroffen werden.

Es können mehrere Pins definiert werden, dabei sollte aber das Ziel, die Anzahl der Zertifizierungsstellen, welche ein Zertifikat für eine Domäne ausstellen können, zu minimieren, nicht aus dem Fokus geraten.

Max-age: Dieser Parameter definiert die Laufzeit eines Pins und gibt an, wie lange der Webbrowser eine Domäne als Known Pinned Host definiert. Dabei zählt die Zeit ab dem Moment, an dem der Browser diese als Known Pinned Host identifiziert hat. Nach Ablauf der Zeit erhält der Browser neue Pins von der entsprechenden Domäne mittels TOFU-Verfahren. Für die Wirksamkeit von PKP ist die Wahl des Wertes max-age entscheidend.

Wird der Wert zu klein definiert, bietet PKP keinen Schutz für User, welche die entsprechende Domäne nur unregelmäßig besuchen, da diese dann meist eine Verbindung auf TOFU basierend aufbauen. Dies vergrößert die Angriffsfläche.

Wird der Wert zu groß gewählt, kann es zu fehlgeschlagenen Validierungen kommen, obwohl der von der Domäne übertragene Pin valide ist. Dies kann passieren, wenn die Pin-Konfiguration einer Domäne geändert wurde, alte Pins im Cache von Browsern jedoch noch gültig sind. Es sollte daher bei Definition der max-age immer die Nutzungszeit der Schlüssel berücksichtigt werden. Dies muss auch bei der Auswahl der Pins berücksichtigt werden.

includeSubdomains: Optional definiert der Parameter includeSubdomains, ob PKP nur für einen Domänennamen gilt, oder auch für Sub-Domänen. Wenn eine Sub-Domäne jedoch ein anderes Zertifikat nutzt als die Second-Level-Domäne (test.example.com & example.com) sollte der Einsatz dieses Feldes gut durchdacht werden. Im schlimmsten Fall wird zuerst example.com (mit includeSubdomains) aufgerufen und die zugehörigen Pins werden im Cache des Browsers gespeichert. Wird nun test.example.com aufgerufen, schlägt die Validierung des Pins fehl, da der Browser den gepinnten öffentlichen Schlüssel des verwendeten Serverzertifikates für example.com für die Dauer von max-age als einzigen erlaubten Pin akzeptiert, jedoch der öffentliche Schlüssel für test.example.com validiert wird.

report-uri: Ein weiteres optionales Feld des PKP-Headers ist report-uri. In diesem Feld kann eine URL angegeben werden, an die Log-Daten gesendet werden, falls eine Pin-Validierung fehlschlägt. Durch diese Funktion ist der Betreiber einer Domäne in der Lage, falsche Zertifikate oder Probleme, welche beim Pinning auftreten, zu identifizieren und zu beheben. Der Parameter report-uri kann entweder im Standard-PKP-Header verwendet werden, oder in einem Public-Key-Pins-Report-Only (PKP-RO)-Header, um beispielsweise zum Testen von Serverkonfigurationen ausschließlich das Reporting zu nutzen. RO-Pins werden nicht im Cache des Browsers gespeichert und führen bei fehlgeschlagener Validierung nicht zur Sperrung der Domäne, sondern informieren ausschließlich anhand der report-uri. PKP-RO und report-uri werden derzeit nur vom Chrome Browser ab Version 46 unterstützt.

Statisches Pinning

Eine Schwachstelle des PKP ist das TOFU-Prinzip. Hierbei wird davon ausgegangen, dass beim ersten Aufruf einer Domäne die korrekte Domäne und damit das zugehörige valide Zertifikat präsentiert

wird. Trifft dies nicht zu, wird ein falscher Pin gespeichert und dem Browser der Zugriff auf die korrekte Domäne gesperrt. Um dies zumindest bei den großen Internetunternehmen zu verhindern, sind deren Pins statisch auf einer sogenannten Preloaded Pin List im Browser verankert. Für diese Domänen gilt nicht mehr das TOFU Prinzip, da die Pins schon vor dem ersten Aufruf im Browser hinterlegt sind. Statische Pins verwenden zum Beispiel Google, Twitter, Mozilla, Firefox, Tor und Dropbox. Aktuell wird statisches Pinning allerdings nur von Firefox und Chrome umgesetzt.

Statisches Pinning eignet sich aber nicht für einen flächendeckenden Einsatz, da die Liste statischer Pins beliebig lang würde und eine Pflege durch den Browseranbieter nicht zu leisten wäre. Weiterhin würde dies auch bedeuten, dass neben den Zertifizierungsstellen eine zweite Instanz geschaffen wird, welche die Zuordnung von öffentlichen Schlüsseln zu Domänen prüft und deren Überprüfung weiteres Potential für Missbrauch bietet. Große Internetunternehmen können untereinander die Richtigkeit von öffentlichen Schlüsseln bzw. Zertifikaten und Pins sicherstellen. Das flächendeckende Authentisieren von Domänen ist durch die Browseranbieter aber nicht umzusetzen.

Was wird gepinnt

Wie schon erwähnt, können öffentliche Schlüssel einer Domäne, Zwischenzertifizierungsstellen oder Zertifizierungsstellen gepinnt werden.

Wenn der öffentliche Schlüssel eines Servers gepinnt wird, ist die Angriffsfläche am kleinsten, da für diesen Server nur zuvor festgelegte, öffentliche Schlüssel bzw. die zugehörigen Zertifikate genutzt werden können. Jedoch ist die Gefahr, dass die Domäne für Browser welche PKP nutzen, dann zeitweise nicht erreichbar ist, größer. Dieser Fall tritt ein, wenn das Schlüsselpaar auf Grund von Verlust, gestohlenem privaten Schlüssel oder Schlüsseltausch bei Ablauf der Zertifikate ersetzt werden muss. Nutzer von PKP werden dann für den Zeitraum von max-age ausgesperrt. Hier hilft eine entsprechende Wahl des Backup Pins.

Wird der öffentliche Schlüssel einer Zwischenzertifizierungsstelle gepinnt, sind der Schlüsseltausch und die damit verbundene Erstellung neuer Zertifikate einfacher. Denn auch ohne Verwendung des Backup Pin, kann zeitnah ein neuer öffentlicher Schlüssel durch die gepinnte Zwischenzertifizierungsstelle signiert werden. Dadurch, dass der öffentliche Schlüssel der signierenden Zertifizierungsstelle gepinnt wurde, wird auch das so erstellte Zertifikat von Browsern akzeptiert. Zeitgleich vergrößert sich hier die Angriffsfläche, da schließlich alle von dieser Zwischenzertifizierungsstelle signierten Zertifikate akzeptiert werden Wird die Zwischenzertifizierungsstelle kompromittiert, kann der Angreifer den Webserver imitieren und Validierungen der Pins verlaufen erfolgreich.

Feature	Chrome	Firefox	Internet Explorer	Edge	Opera (Chromium)	Safari
Basis PKP	Ab Version 46	Ab Version 35	Nein	Nein	Ja	Nein
Report Only	Ab Version 46	Nein	-	-	Ja	-
Report URI	Ab Version 46	Nein	-	-	Ja	-
Certificate Transparency	Ab Version 33	Nein	Nein	Nein	Ja	Nein
statische Pins	Ab Version 13	Ab Version 32	Nein	Ja	Ja	Nein
PKP Level	Level 1	Konfigurierbar	-	-	Level 1	-

Tabelle 1: Browserunterstützung von PKP

Wenn der öffentliche Schlüssel einer Wurzelzertifizierungsstelle gepinnt wird, vergrößert sich die Angriffsfläche erneut, da die Pins der Serverzertifikate von allen Zwischenzertifizierungsstellen erfolgreich validiert werden könnten. So benötigt der Angreifer, wie bei dem Beispiel CNNIC / MSC Holding, nur eine Zwischenzertifizierungsstelle mit der er sich selbst Zertifikate für gewünschte Domänennamen ausstellen kann. Alternativ kann auch eine Zwischenzertifizierungsstelle, welche ohne Prüfung die gewünschten Zertifikate ausstellt, genutzt werden.

Um die Angriffsfläche möglichst klein zu halten, empfiehlt sich generell die Verwendung von vertrauenswürdigen Zertifizierungsstellen. Wird der öffentliche Schlüssel eines Servers gepinnt, so sollte der Schlüssel einer Zwischenzertifizierungsstelle als Backup Pin genutzt werden. Wird als Backup Pin ebenfalls der öffentliche Schlüssel eines Servers genutzt, entspricht dieser zum Zeitpunkt des Einsatzes eventuell nicht mehr den selbstauferlegten Bestimmungen (Zertifikat abgelaufen oder Schlüssellänge nicht standardkonform). Beim Pinning muss daher die Balance zwischen Angriffsfläche und Verfügbarkeit des Dienstes gefunden werden.

Umsetzung im Browser

Aktuell unterstützen Browser unterschiedliche Funktionalitäten von PKP. (siehe Tabelle 1 und 2)

Teilweise können in Browsern durch den Browser-Hersteller statische Pins hinterlegt werden.

Manche Browser unterstützen ergänzend dazu auch statische Pins, die vom Nutzer manuell im Browser hinterlegt werden können. Für diese Pins ist der Nutzer selbst verantwortlich. Änderungen der Pins von Domänen müssen vom Nutzer manuell übernommen werden. Werden Pin-Änderungen nicht übernommen, so führt dies dazu, dass die betroffene Domäne für den betroffenen Browser nicht mehr erreichbar ist. Hat ein Angreifer Zugriff auf ein Endgerät, kann dieser die Browserkonfiguration ändern und so auch PKP aushebeln.

In manchen Fällen ist es gewollt, verschlüsselte Verbindungen aufzubrechen, und einen Friendly-MitM einzusetzen. Beispiele hierfür sind der Betrieb von Proxy-Servern, Intrusion Prevention Systemen und Firewalls, die auch verschlüsselte Kommunikation analysieren sollen. In diesen Fällen wird dem Browser nicht das Zertifikat der aufgerufenen Domäne angezeigt, aus welchem Grund PKP nicht mehr uneingeschränkt genutzt werden kann. Wird Friendly-MitM eingesetzt, muss PKP daher mindestens für Zertifikate des Friendly-MitM deaktiviert werden (Level 1).

In manchen Browsern können unterschiedliche PKP-Level eingestellt werden. Es wird dabei mindestens unterschieden zwischen

- vollständiger Deaktivierung von PKPs: PKP wird nicht genutzt (Level 0),
- teilweiser Deaktivierung von PKP: PKP wird für manuell im Browser hinterlegte Vertrauensanker deaktiviert (Level 1) oder
- strikter Aktivierung von PKPs: PKP wird für jede Domäne, welche dieses unterstützt, genutzt (Level 2).

Alternativen zu PKP

Alternativen zum Pinning bieten beispielsweise DNS-based Authentication of Named Entities (DANE, RFC 6698) und Certificate Transparency (CT, RFC 6962).

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

Feature	Android			iOS				Windows Phones	
	Chrome	Firefox	Opera	Safari	Opera	Firefox	Chrome	Internet Explorer	Opera
Basis PKP	Ja	Ab Version 35	Nein	Nein	Nein	Nein	Ja	Nein	Nein

Tabelle 2: Unterstützung von PKP auf mobilen Endgeräten

Stärken	Schwächen
Minimierung der Angriffsfläche	Aktuell geringe Verbreitung
Erkennung von Angriffen	Nutzung nur für HTTPS
Vergleichsweise kostengünstige Umsetzung	Fehlkonfigurationen können gravierende Folgen haben
	Sicherheitsgewinn abhängig von gewählten Pins
	TOFU

Tabelle 3: Stärken und Schwächen von PKP

Die Idee von DANE ist mit der des PKP zu vergleichen. DANE verknüpft eine Domäne mittels DNS-Eintrag mit einem bestimmten Zertifikat. Dadurch wird festgelegt, welches Zertifikat für diese Domäne genutzt werden darf. Die Verknüpfung zwischen Zertifikat und Domäne wird in der DNS-Security Extension gespeichert. DANE setzt daher eine DNSSEC-Infrastruktur voraus. Da DNSSEC-Infrastrukturen aktuell nicht flächendeckend gegeben sind und auch noch nicht klar ist, wie diese umgesetzt werden soll, kann DANE nur selektiv in Netzen, in welchen DNSSEC genutzt wird, eingesetzt werden.

Bei CT handelt es sich um ein experimentelles Projekt, welches von Google initiiert worden ist. Ziel von CT ist es, dass alle durch Zertifizierungsstellen ausgestellten Zertifikate sichtbar gemacht werden und nachvollziehbar wird, welche Zertifikate durch welche Zertifizierungsstellen ausgestellt worden sind. Die Grundlage dafür bilden CT-Logs. CT-Logs sind Listen, in welchen alle ausgestellten Zertifikate aufgeführt werden und in welche Zertifizierungsstellen die von ihnen ausgestellten Zertifikate eintragen. Die CT-Logs sind so aufgebaut, dass einmal hinzugefügte Einträge nicht verändert oder gelöscht werden können. Jeder kann Zertifikate in CT-Logs eintragen. Die CT-Logs werden außerdem regelmäßig in einem Hash Baum konsolidiert. CT-Logs können von jedem darauf hin überprüft werden, ob diese ein bestimmtes Zertifikat enthalten. Einem jeden Zertifikat ist die Information mitzugeben, in welchem CT-Log dies aufgeführt worden ist. CT kann die Ausstellung falscher Zertifikate nicht verhindern, es wird jedoch wahrscheinlicher, dass falsch ausgestellte Zertifikate entdeckt und gesperrt werden.

Fazit und Empfehlung

Insgesamt bietet PKP bei richtiger Konfiguration eine gute Möglichkeit, den Angriffsvektor für HTTPS-Verbindungen zu verkleinern und je nach Browser Domänenbetreiber bei MitM-Angriffen zu alarmieren (report-uri). Allerdings ist die richtige Konzeption und Konfiguration von PKP dafür zwingende Voraussetzung. Konzeptions- und Konfigurationsfehler führen schnell dazu, dass Domänen trotz vorhandener gültiger Zertifikate nicht erreichbar sind. Zusätzlich bietet PKP auch keinen absoluten Schutz vor Zertifikatsmissbrauch. Dies ist einerseits darin begründet, dass der Einsatz von PKP auf HTTPS beschränkt ist, andererseits aber auch darin, dass der Browser den Pin, welcher ihm beim ersten Besuch einer Domäne präsentiert wird, als korrekt annimmt (TOFU). Dies verbreitert zwar den Anwendungsbereich von PKP, bietet jedoch die Möglichkeit, diese erste Verbindung für einen Angriff zu nutzen. Aktuell ist PKP weiterhin nur gering verbreitet, sowohl was den Einsatz von PKP auf Webservern angeht, als auch die vollumfassende Unterstützung von PKP inklusive aller Features in Browsern. Es bleibt allerdings zu hoffen, dass sich dies in nächster Zeit ändert, da PKP bei gut geplantem Einsatz die Sicherheit von HTTPS für Nutzer deutlich erhöht (siehe Tabelle 3). Es wird daher empfohlen PKP für alle eigenen Web-Angebote in Betracht zu ziehen, die einen erhöhten Schutzbedarf hinsichtlich Vertraulichkeit und Integrität haben.

Verweise

[1] https://googleonlinesecurity.blogspot.de/2015/03/maintaining-digital-certificate-security.html

[2] http://www.heise.de/security/meldung/Microsoft-entzieht-Indischer-CA-das-Vertrauen-2255992.html

[3] http://www.macwelt.de/news/Browser-Updates-Gefaelschte-SSL-Zertifikate-fuer-Google-Yahoo-und-Microsoft-3252191.html

ComConsult Veranstaltungskalender

Lokale Netze für Einsteiger, 15.02.-19.02.16 in Aachen

Garantietermin

Dieses Seminar vermittelt kompakt und intensiv innerhalb von 5 Tagen die Grundprinzipien des Aufbaus und der Arbeitsweise Lokaler Netzwerke. Dabei werden sowohl die notwendigen theoretischen Hintergrundkenntnisse vermittelt als auch der praktische Aufbau und der Betrieb eines LANs erläutert. Ausgehend von einer Darstellung von Themen der Verkabelung und der grundlegenden Übertragungsprotokolle werden die wichtigen Zusammenhänge zwischen der Arbeitsweise von Switch-Systemen, den darauf aufsetzenden Verfahren und der Anbindung von PCs und Servern systematisch erklärt.

Preis: € 2.490,-- netto

IP-Wissen für TK-Mitarbeiter, 22.02.-23.02.16 in Bonn

Garantietermin

Dieses Seminar vermittelt TK-Mitarbeitern ohne Vorkenntnisse im Bereich LAN und IP das erforderliche Wissen zur Planung und zum Betrieb von VoIP-Lösungen. Die Inhalte sind so gegliedert, dass Sie die Grundlagen schnell verstehen. Es werden die wichtigsten VoIP spezifischen Aspekte vorgestellt und unter Praxis-relevanten Gesichtspunkten beleuchtet. Die Themen erstrecken sich von IP und LAN Grundlagen hin zu Praxis relevanten Themen wie QoS, Jitter und Bandbreiten Fragen. Ziel ist es dem IP-Unkundigen die wichtigen Grundlagen der Netzwerk Technik kompakt und praxisnah zu vermitteln.

Preis: € 1.590,-- netto

Das PSTN stirbt: Die neue Kommunikation mit SIP/IP, 08.03.16 in Bonn

Garantietermin

Die Sonderveranstaltung zum Thema PSTN-Migration hin zu All-IP bietet top-aktuelle Informationen und Analysen mit ausgewählten Experten. Eine ausgewogene Mischung aus Analysen, Hintergrundwissen und Projekterfahrungen in Kombination mit Produktbewertungen und Diskussionen liefert das ideale Umfeld für alle Planer, Betreiber und Verantwortliche solcher Lösungen.

Preis: € 1.090,-- netto

Netzzugangskontrolle: Technik, Planung und Betrieb, 14.03.-16.03.16 in Berlin

Garantietermin

Dieses 3-tägige Seminar vermittelt den aktuellen Stand der Technik der Netzzugangskontrolle (Network Access Control, NAC) und zeigt die Möglichkeiten aber auch die Grenzen für den Aufbau einer professionellen NAC-Lösung auf. Schwerpunkt bildet die detaillierte Betrachtung der Standards IEEE 802.1X, EAP und RADIUS. Dabei wird mit IEEE 802.1X in der Fassung von 2010 und mit IEEE 802.1AE (MACsec) auch auf neueste Entwicklungen eingegangen.

Preis: € 1.890,-- netto

TCP/IP-Netze erfolgreich betreiben, 14.03.-16.03.16 in Berlin

IP ist die Grundlage jeden Netzes. Die Protokolle TCP und UDP bilden die Basis jeder Anwendungskommunikation. Es werden zudem Kenntnisse über Routingprotokolle, DHCP, DNS benötigt. Dieses Seminar vermittelt praxisnah das notwendige Wissen.

Preis: € 1.890,-- netto

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen, 14.03.-16.03.16 in Köln

Garantietermin

Dieses Seminar vermittelt alle notwendigen Projektschritte zu einer erfolgreichen Umsetzung von VoIP Projekten. Diese erstrecken sich über die Einsatz- und Migrations-Szenarien, die einsetzbaren Basis-Technologien und Komponenten und die erweiterten TK-Anwendungen wie IVR, UM oder UC. Es werden Bewertungskriterien für eine TK-Lösung und eine Übersicht über den bestehenden TK-Markt mit allen etablierten Hersteller vorgestellt.

Preis: € 1.890,-- netto

Interne Absicherung der IT-Infrastruktur, 14.03.-15.03.16 in Köln

In diesem Seminar lernen Sie wie man die Sicherheit von LAN, WAN, Endgeräten, RZ-Bereichen, Servern und SAN erreicht. Konkrete Beispiele aus der Praxis zeigen den Weg zu einer erfolgreichen IT-Sicherheits-Lösung.

Preis: € 1.590,-- netto

Internetworking: optimales Netzwerk-Design mit Switching und Routing, 04.04.-08.04.16 in Aachen

Dieses Seminar vermittelt alles Wichtige, was Sie zum Thema LAN wissen müssen. Es werden unterschiedlichen Einsatzszenarien für Routing und Switching beleuchtet und das notwendige Wissen zur erfolgreichen Planung und dem Betrieb von Netzwerk Infrastrukturen vermittelt. Die Abdeckung der Themen erstreckt sich über Layer 2 Redundanzverfahren, Routing und Tunneltechnologien, sowie Netzwerkmanagement Fragen. Einen weiteren Schwerpunkt bildet das Kapitel Office Network. Hier werden der Aufbau und die Integration von WLAN Strukturen detailliert beleuchtet. Abgerundet werden diese Informationen durch verschiedene praktische Übungen und einen Blick auf die aktuelle Markt- und Produktsituation der führenden Hersteller von Netzwerk-Komponenten.

Preis: € 2.490,-- netto

RZ-RZ-Kopplung - alles nur eine Frage der Bandbreite?, 11.04.16 in Stuttgart

Rechenzentren in entfernten Standorten zu betreiben erfordert sich mit IT-Sicherheit, Desaster Recovery, Service Level Agreements und Hochverfügbarkeit auseinander zu setzen. Dabei sind zum Teil Vorgaben bspw. vom BSI zu beachten. In dieser Schulung werden die aktuellen Techniken erläutert und für die richtige strategische Entscheidung zu einem Gesamtkonzept zusammengeführt.

Preis: € 1.090,-- netto

Crashkurs IT-Recht für Nichtjuristen, 11.04.-12.04.16 in Stuttgart

Diese Veranstaltung wendet sich an IT-Leiter, Compliance-Beauftragte und Geschäftsführer, die sich kompakte und praktische Grundkenntnisse zu den rechtlichen Eckpunkten des IT-Projektes verschaffen wollen. Die Inhalte sind insbesondere an Nichtjuristen gerichtet, die sich nicht alltäglich mit rechtlichen Fragestellungen befassen und eine Grundorientierung suchen. In dem Seminar werden auch Praxisfälle erörtert.

Preis: € 1.590,-- netto

Zertifizierungen

ComConsult Certified Network Engineer

Lokale Netze
15.02. - 19.02.16 in Aachen
09.05. - 13.05.16 in Aachen
19.09. - 23.09.16 in Aachen

TCP/IP-Netze erfolgreich betreiben
14.03. - 16.03.16 in Berlin
20.06. - 22.06.16 in Bonn
24.10. - 26.10.16 in Bonn

Internetworking
04.04. - 08.04.16 in Aachen
04.07. - 08.07.16 in Aachen
14.11. - 18.11.16 in Aachen

Paketpreis für zwei 5-tägige und ein 3-tägiges Intensiv-Seminar € 6.180,-- netto (Einzelpreise: € 2.490,-- netto bzw. 1.890,-- netto)

ComConsult Certified Trouble Shooter

Trouble Shooting in vernetzten Infrastrukturen
10.05. - 13.05.16 in Aachen
27.09. - 30.09.16 in Aachen

Trouble Shooting für Netzwerk-Anwendungen
14.06. - 17.06.16 in Aachen
15.11. - 18.11.16 in Aachen

Paketpreis für beide Seminare inklusive Prüfung € 4.280,-- netto
(Seminar-Einzelpreis € 2.290,-- netto , mit Prüfung € 2.470,-- netto)

ComConsult Certified Voice Engineer

IP-Telefonie und Unified Communications erfolgreich planen und umsetzen
14.03. - 16.03.16 in Köln
11.05. - 13.05.16 in Bonn
24.10. - 26.10.16 in Frankfurt

Session Initiation Protocol Basis-Technologie der IP-Telefonie
11.04. - 13.04.16 in Stuttgart
20.06. - 22.06.16 in Bonn
09.11. - 11.11.16 in Berlin

Umfassende Absicherung von Voice over IP und Unified Communications
25.04. - 27.04.16 in Bonn
04.07. - 06.07.16 in Stuttgart
28.11. - 30.11.16 in Bonn

Optionales Einsteiger-Seminar: IP-Wissen für TK-Mitarbeiter
22.02. - 23.02.16 in Bonn
25.04. - 26.04.16 in Düsseldorf
19.09. - 20.09.16 in Frankfurt

Wir empfehlen die Teilnahme an diesem Seminar **"IP-Wissen für TK-Mitarbeiter"** all jenen, die die Prüfung zum ComConsult Certified Voice Engineer anstreben, ganz besonders aber den Teilnehmern, die bisher wenig bis kein Netzwerk Know How, insbesondere TCP/IP, DNS, SIP usw., vorweisen können.

Basis-Paket: Beinhaltet die drei Basis-Seminare
Grundpreis: € 5.100,-- netto statt € 5.670,-- netto
Optionales Einsteigerseminar: Aufpreis € 1.190,-- netto statt € 1.590,-- netto

Impressum

Verlag:
ComConsult Research Ltd.
64 Johns Rd
Christchurch 8051
GST Number 84-302-181
Registration number 1260709
German Hotline of ComConsult-Research:
02408-955300

E-Mail: insider@comconsult-akademie.de
http://www.comconsult-research.de

Herausgeber und verantwortlich
im Sinne des Presserechts:
Dr. Jürgen Suppan
Chefredakteur: Dr. Jürgen Suppan
Erscheinungweise: Monatlich,
12 Ausgaben im Jahr

Bezug: Kostenlos als PDF-Datei
über den eMail-VIP-Service
der ComConsult Akademie