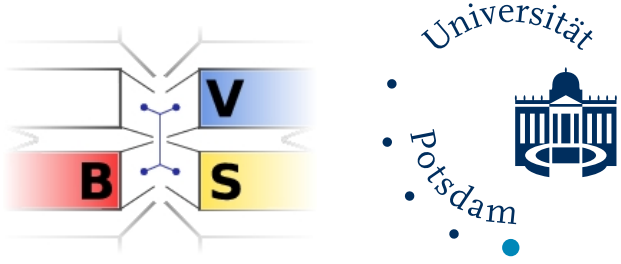
Seminar

(Secure) Communication Networks

Prof. Bettina Schnor

Betriebssysteme und Verteilte Systeme
Institut für Informatik und Computational Science
Universität Potsdam



Sommersemester 2020

Motivation

To deepen our knowledge of computer networks, especially about wireless networks, and to learn more about protocols which get the Internet running,

Motivation

To deepen our knowledge of computer networks, especially about wireless networks, and to learn more about protocols which get the Internet running,

and also to get presentation experiences.

Dates:

- Presentation of topics: 20.4.2020 (online)
- Presentation training: 27.04.2020 (online, Petra Vogel)
- Presentations: Thurday 11.6.2020, 18.6.2020, und 25.6.2020, and as a block course in September (Friday 11.9.2020 and Tuesday 15.9.2020)

Supervisor: Prof. Dr. Bettina Schnor, schnor@cs.uni-potsdam.de

More Infos, News and FAQ: Website

In case you have problems to access some of the literature, contact me!

Requirements

- Deliver the presentation draft at least 2 weeks before the presentation per email
- Make an appointment for discussion at least 2 weeks before presentation
- Successful presentation: max. 45 min. incl. Code-Review + 15 min. Discussion,
  The code review is optional and depends on the topic.
  Handout/Glossary is necessary: 1 DIN A4 page
- Deliver the documentation prepared in LaTeX within 1 week after the presentation. (PDF and double-sided printed)
- **Participation at the presentations is mandatory!**

Grade

The grade is composed as follows:

- 10% presentation draft
- 30% presentation content (including Handout)
- 30% successful presentation (style)
- 30% documentation/seminar paper

The student seminar papers will be collected by Alexandra Roy (roy@cs.uni-potsdam.de) and the collection (Seminarband) will be electronically distributed to the participants only.

Handout: The handout shall be interesting for the other participants. It should include the most important and useful sources (books, papers, websites). If you put figures on the handout, don't forget to cite the source. (The same applies for your slides.)

Therefore, the handout includes:

- the name of the presenter,
- the source of re-used tables or figures,
- recommended sources for further reading,
- a summary/conclusion of your talk: This is the take-away of your talk!
- ...

How to apply for a topic?

1. Send an email with your favorite topic and one alternative until 7th of May! State your preference for the presentation date: June or September!
2. I will do my best (aka FIFO) and will send an email with the final mapping until 11th of May.

This course is open for bachelor and master students.

- The seminar discusses communication protocols and networks and related security aspects. No previous knowledge is required for the course.
- The course is suited for bachelor and master students.
- Topic 1, 2, 6 and 7 are *recommended* for bachelor students.
- The course language is English. Bachelor students may give their talk in German.

Before you start with the preparation of your talk, have a look on:
S. Keshav, How to Read a Paper. - The Three-Pass Approach.

Topics

The wireless session

1. Topic: Wireless Communication: WLAN and WPA2 (IEEE 802.11 and IEEE 802.11i)

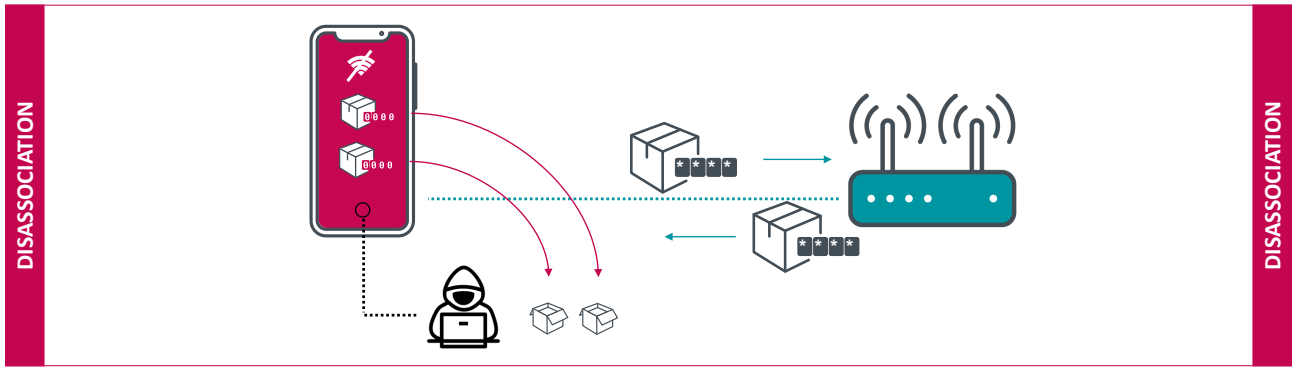


Figure 2 // An active attacker can trigger disassociations to capture and decrypt data

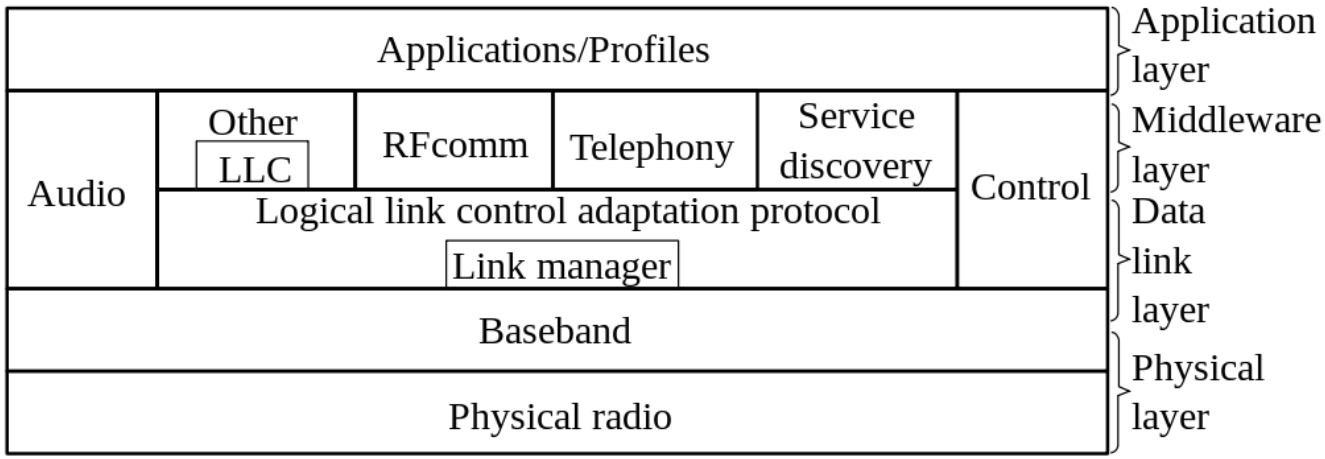
Quelle: Kr00k White Paper

- Medium Access Control Protocol (MAC)
- Frame format
- **Fokus on: 802.11i standard WPA2 (Wi-Fi Protected Access)**
- Security concerns: Hole196, KRACK, Kr00k (CVE-2019-15126) and Co.

Source:

- James Kurose, Keith Ross: *Computer Networking*, Peason, 7th Edition, 2017, Chapter 7.3
- Claudia Eckert: *IT-Sicherheit: Konzepte - Verfahren - Protokolle*, Chapter 15 **(in German)** (the edition from 2013 is online available at UP library)
- Sheila Frankel, Bernard Eydt, Les Owens and Karen Scarfone: *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*, NIST Standard SP 800-97, 2007.
- ESET White paper: Kr00k - CVE-2019-15126 - Serious Vulnerability deep inside your Wi-Fi Encryption

2. Topic: Wireless Communication: Bluetooth - The architecture and protocol stack



Quelle: Wikipedia

- Link Manager protocol (LMP)
- Logical Link Control and Adaptation Protocol (L2CAP)
- MAC and Logical Link Control
- Packet format
- Service Discovery Protocol (SDP)
- Bluetooth application architecture: Bluetooth profiles, Generic Attribute Profile (GATT)
- improvements in Bluetooth 5.1 and 5.2 (2019)

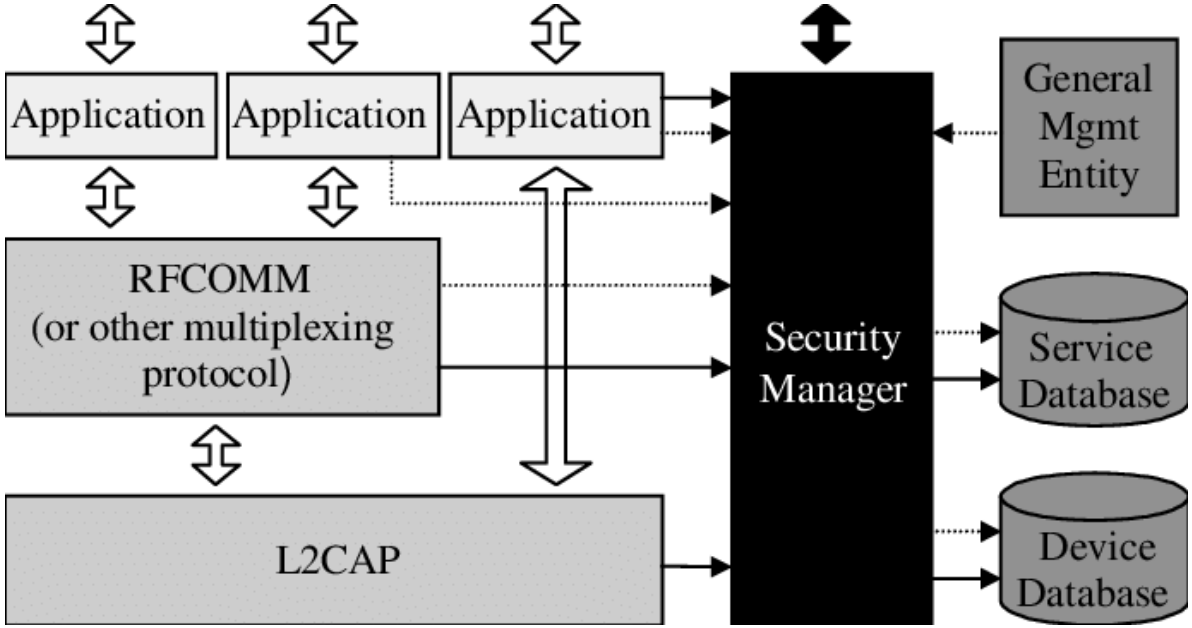
Source:

- *Bluetooth Core Specification Version 5.2, 31.12.2019*, (3256 pages)
- Claudia Eckert: *IT-Sicherheit: Konzepte - Verfahren - Protokolle*, Chapter 15 **(in German)** (the edition from 2013 is online available at UP library)

Instead of a source code review give a feedback for the specification:

- readability
- clarity
- ready to implement after reading?
- Show us an example from the specification!

3. Topic: Wireless Communication: Bluetooth - Security



Quelle: www.researchgate.net

- Security Manager
- encryption (SAFER+ algorithm), authentication, key management
- protocol Data Units (PDUs) for security
- security concerns: Bluejacking and more

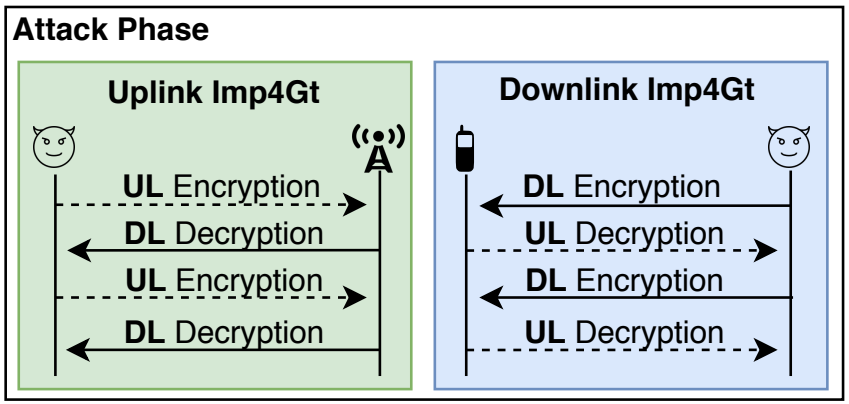
Source:

- *Bluetooth Core Specification Version 5.2, 31.12.2019*, (3256 pages)
- Claudia Eckert: *IT-Sicherheit: Konzepte - Verfahren - Protokolle*, Chapter 15 **(in German)** (the edition from 2013 is online available at UP library)
- Wikipedia: History of security concerns

Instead of a source code review give a feedback for the specification regarding the security aspects!

4. Topic: Mobile Communication: 4G Broadband Cellular Networks: Long Term Evolution (LTE) and the IMP4GT attacks

1. System Architecture Evolution SAE/LTE (aka Evolved Packet System): Key management, encryption, authentication, key hierarchy
2. The IMP4GT attacks



Quelle: Rupprecht et al.

Source:

- James Kurose, Keith Ross: *Computer Networking*, Peason, 7th Edition, 2017, Chapter 7.4
- Claudia Eckert: *IT-Sicherheit: Konzepte - Verfahren - Protokolle*, Chapter 15.3 **(in German)** (the edition from 2013 is online available at UP library)
- *3GPP System Architecture Evolution (SAE): Security Architecture (Release 16, 33401-g20.zip)*,
- David Rupprecht et al.: *IMP4GT: IMPersonation Attacks in 4G NeTworks*, Network and Distributed Systems Security (NDSS) Symposium 2020

5. Topic: Security Aspects of 5G

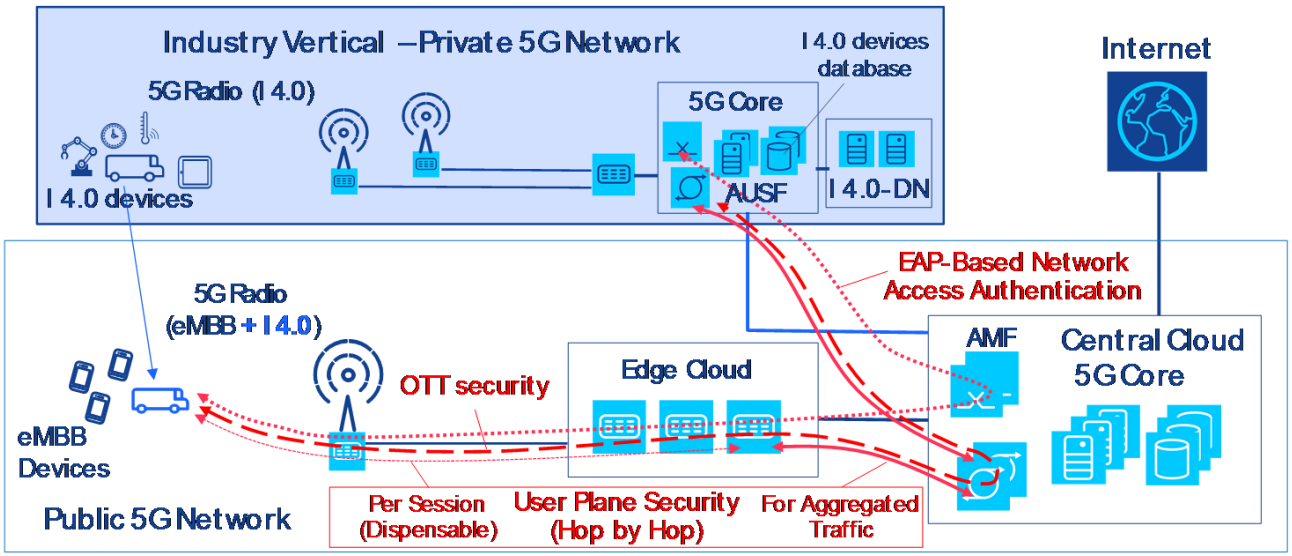


Fig. 1.Roaming Approach for Networks Built on Both Private and Public Network Infrastructure

Quelle: Schneider et al.

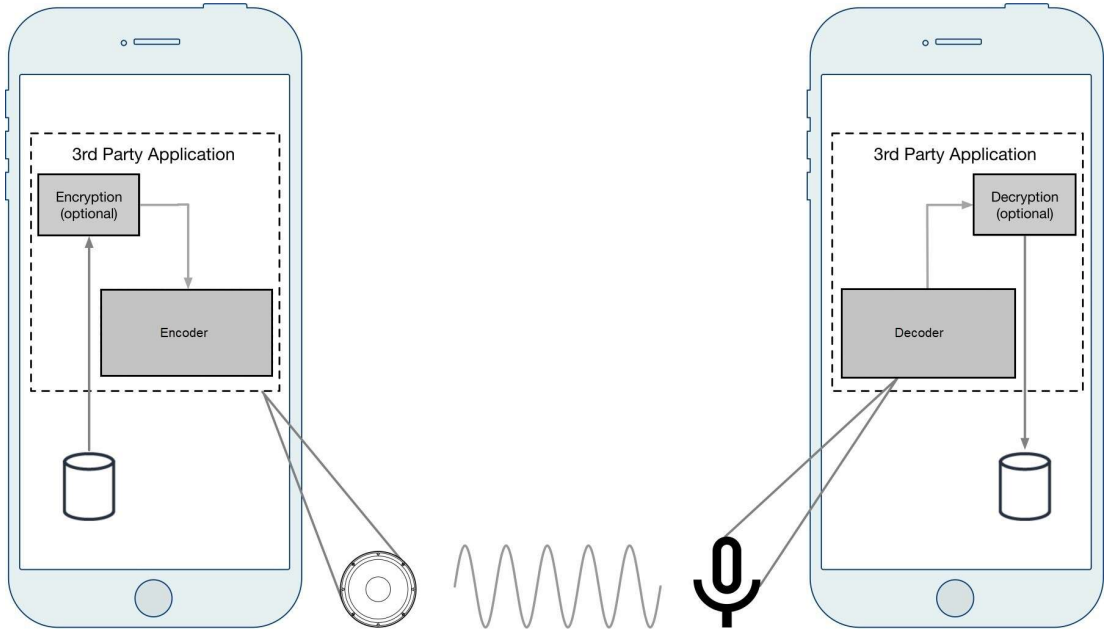
- Overview, Comparison with LTE
- Slice Isolation for Highly Sensitive Third-Party Services (see Schneider et al.)

Source:

- 5G PPP Phase 1 Security Landscape, June 2017
- Xiaowei Zhang, Andreas Kunz: *Overview of 5G security in 3GPP*, IEEE Conference on Standards for Communications & Networking, 2017.

- Peter Schneider et al.: *Providing Strong 5G Mobile Network Slice Isolation for Highly Sensitive Third-Party Services*, IEEE Wireless Communications and Networking Conference (WCNC), 2018.
- Fabrizio Granelli: *Tutorial: Softwarization Concepts and Practice in 5G Communication Systems and Beyond*, slides, 5G Summit, Dresden 2019.
- Jin Cao et al.: *A Survey on Security Aspects for 3GPP 5G Networks*, IEEE Communications Surveys & Tutorials. vol.22, no.1, pp. 170-195, 2020
- Ijaz Ahmad et al.: *Overview of 5G Security Challenges and Solutions*, IEEE Communications Standards Magazine, vol. 2, no. 1, pp. 36-43, MARCH 2018.
- Recent evaluation: Generationenkonflikt: Was 5G in Smartphones bringt, c't 9/2020 **(in German)**

6. Topic: Data over Sound - Übertragung per Ultraschall



Quelle: https://www.eetimes.com/data-over-sound-encryption-is-key/

- Fundamental concepts
- application areas within the Internet of Things
- Privacy Threats
- The SoniControl-Firewall

Source:

- Matthias Zeppelzauer: *Data over Sound*, <KES> - Die Zeitschrift für Informations-Sicherheit, 35. Jahrgang, Nr. 4, 2019. **(in German)**
- Daniel Arp et al.: *Privacy Threats through Ultrasonic Side Channels on Mobile Devices*, Proceedings of the 2nd IEEE European Symposium on Security and Privacy (EuroS&P), 2017.
- Kobus Marneweck et al.: *Why data-over-sound is an integral part of any IoT engineer's toolbox*, White Paper, March 2019.

The IPv6 Sesion

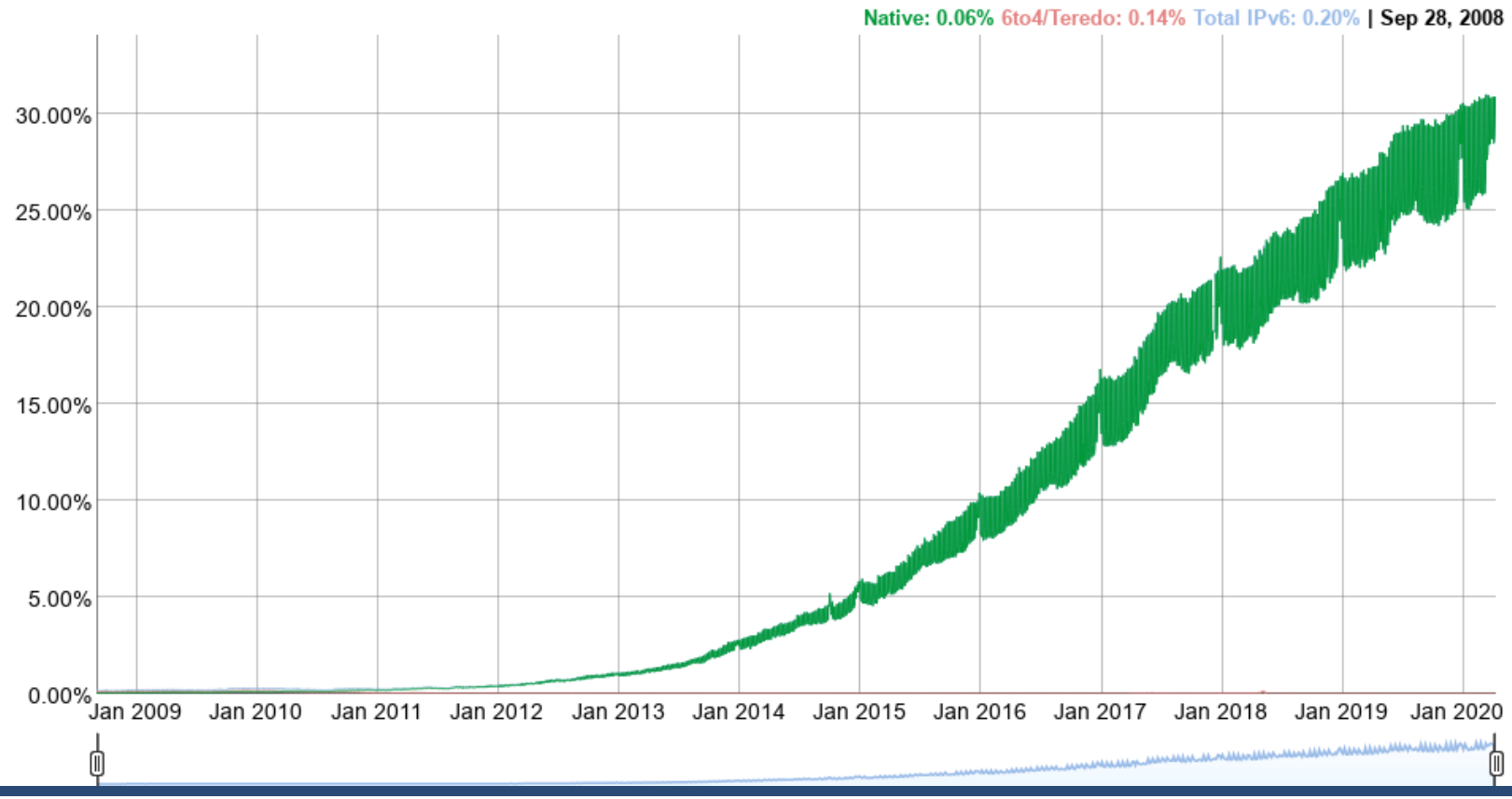
Statistics

Google collects statistics about IPv6 adoption in the Internet on an ongoing basis. We hope that publishing this information will help Internet providers, website owners, and policy makers as the industry rolls out IPv6.

IPv6 Adoption | Per-Country IPv6 adoption

IPv6 Adoption

We are continuously measuring the availability of IPv6 connectivity among Google users. The graph shows the percentage of users that access Google over IPv6.



7. Topic: (Secure) IPv6

- IPv6: differences compared to IPv4
- ICMPv6,
- AH, ESP
- IPv6 Programming
- new protocols, new threats?

Source:

- Rick Graziani: *IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6, 2nd Edition*, CISCO Press, 2017 **(eBook, ordered)**
- Christian Frieben: *IPv6 im Wandel - Analyse der IPv6-Standardisierung unter Sicherheitsaspekten*, Masterarbeit (Lehramt), Uni Potsdam, 2014. **(in German)**
- Florian Seele: *IPv6 Flow Label: Neue Möglichkeiten für Lastverteilung in Netzwerken*, Masterarbeit, Uni Potsdam, 2015. **(in German)**
- Lots of RFCs!
- Jörg Zinke: *Portierung von Anwendungen nach IPv6*, Uni Potsdam, 2008 **(Slides in German with additional references)**
- Frank Herberg: *IPv6 Security* (slides), 30th Annual FIRST Conference, Kuala Lumpur, 2018

8. Topic: Secure IPv6: The idsv6 Benchmark

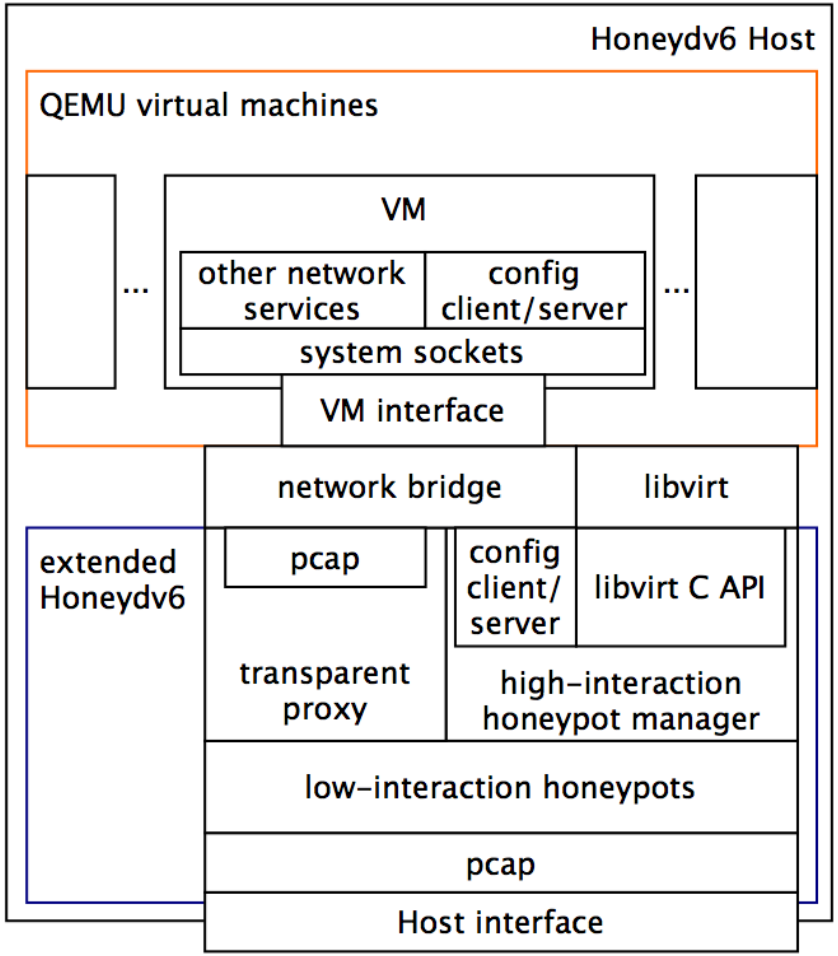
How to defend an IPv6 network?

- van Hauser: The Hacker's Choice THC-IPv6 Attack Tool 3.6
  THC-IPv6 is a toolkit that attacks the inherent protocol weaknesses of IPv6 and ICMP6 and it includes an easy to use packet factory library.
- Intrusion Detection Systems (IDS)
- The idsv6 Benchmark for Intrusion Detection Systems
- optional experiment: Benchmark of Suricata (Stable) version 5.0.2; released February 13, 2020. The SECRYPT-paper evaluates Suricata 3.2.1.

Source:

- Max Schrötter, Thomas Scheffler and Bettina Schnor: *Evaluation of Intrusion Detection Systems in IPv6 Networks*, 16th International Conference on Security and Cryptography (SECRYPT), 2019
- Max Schrötter: *Entwurf und Implementierung einer IPv6 Erweiterung* , Bachelorarbeit, Uni Potsdam, 2018 **(in German)**
- Tool IDSv6 in our Redmine

9. Topic: Secure IPv6 with Hyhoneydv6
How to defend an IPv6 network?



- The IPv6 honeypot Hyhoneydv6
- Optional: 1-month Hyhoneydv6 experiment
  What is an *interesting* set-up?

Source:

- Sven Schindler: *Hyhoneydv6: A hybrid Honeypot Architecture for IPv6 Networks*, International Journal of Intelligent Computing Research (IJICR), 2015
- Sven Schindler: *Honeypot Architectures for IPv6 Networks*, PhD Thesis, Uni Potsdam, 2016.
- honeydv6 in our Redmine

Miscellaneous

10. Topic: C-Roads and C-ITS services

The German carmaking giant promised late Thursday that new models of its Golf passenger car would be installed with Wi-Fi-based hardware that allows cars to communicate with road-based infrastructure and other similarly equipped vehicles, calling it Car2X. (11'2019)

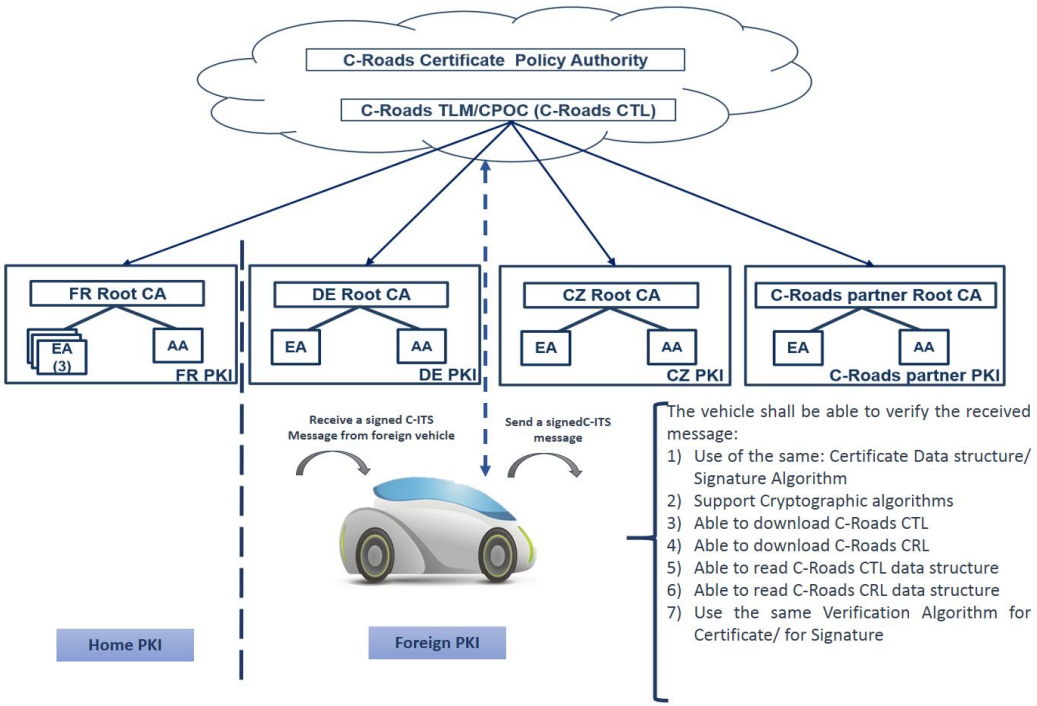


Figure 1: C-Roads Interoperability Process

Reference: C-ROADS Draft Version 1.4

C-ROADS: The platform of harmonized C-ITS deployment in Europe

C-ITS:=

C-ROADS: The platform of harmonized C-ITS deployment in Europe

C-ITS:=Cooperative ITS:=

C-ROADS: The platform of harmonized C-ITS deployment in Europe

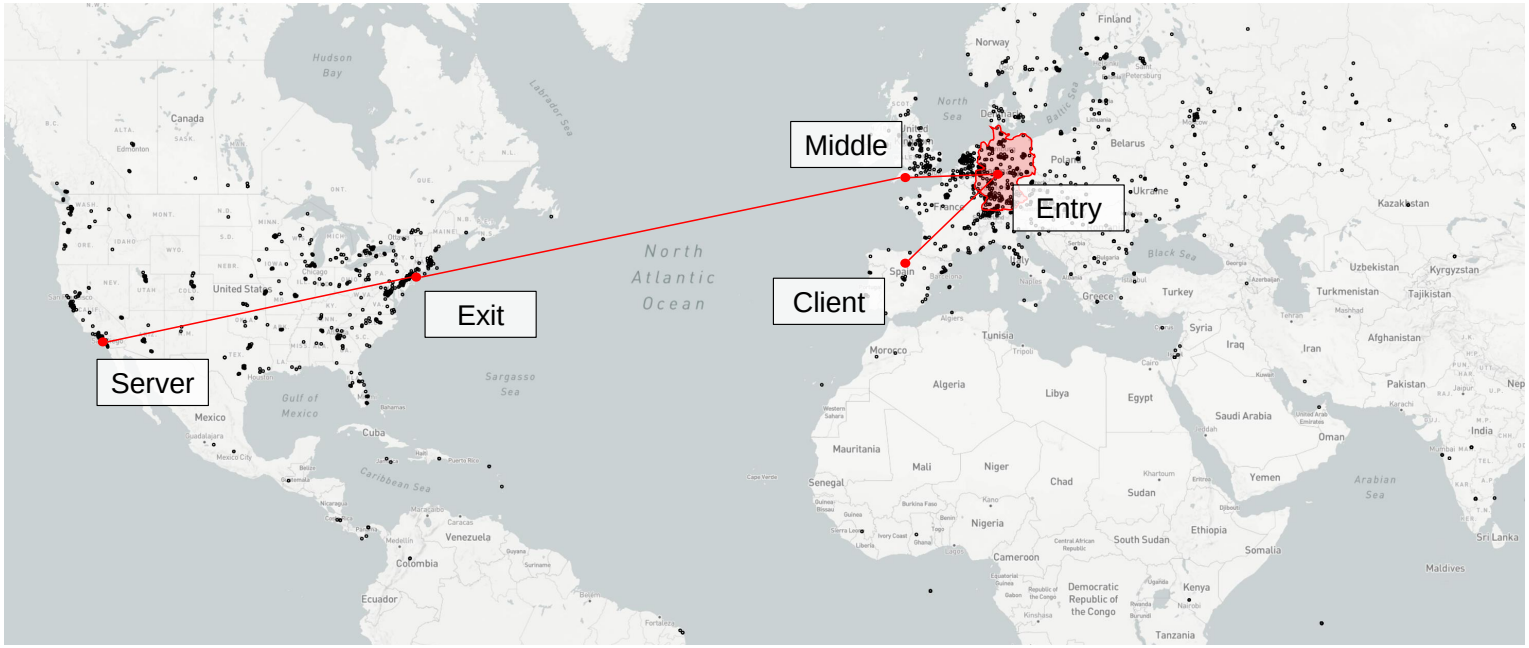
C-ITS:=Cooperative ITS:= Cooperative Intelligent Transport System

- services: Emergency vehicle notification systems, Collision avoidance systems, ...
- CAM and DENM messages
- Overview of European Security Mechanism

Source:

- José Santa, Fernando Pereniguez-Garcia, Antonio Moragón, Antoni Skarmeta: *Experimental evaluation of CAM and DENM messaging services in vehicular communications*, Journal Transportation Research Part C: Emerging Technologie, 2014.
- C-ROADS documents, see for example the C-ITS deployment and evaluation workshop November 2019
- C-ROADS, Draft Report on European Security Mechanism, Version 1.4, Working Group 2, Task Force 1 Report 25th January 2019
- Volkswagen Golf supports Car2X via ITS-G5, but ..., 4.11.2019

11. Topic: Tor for anonymous communication

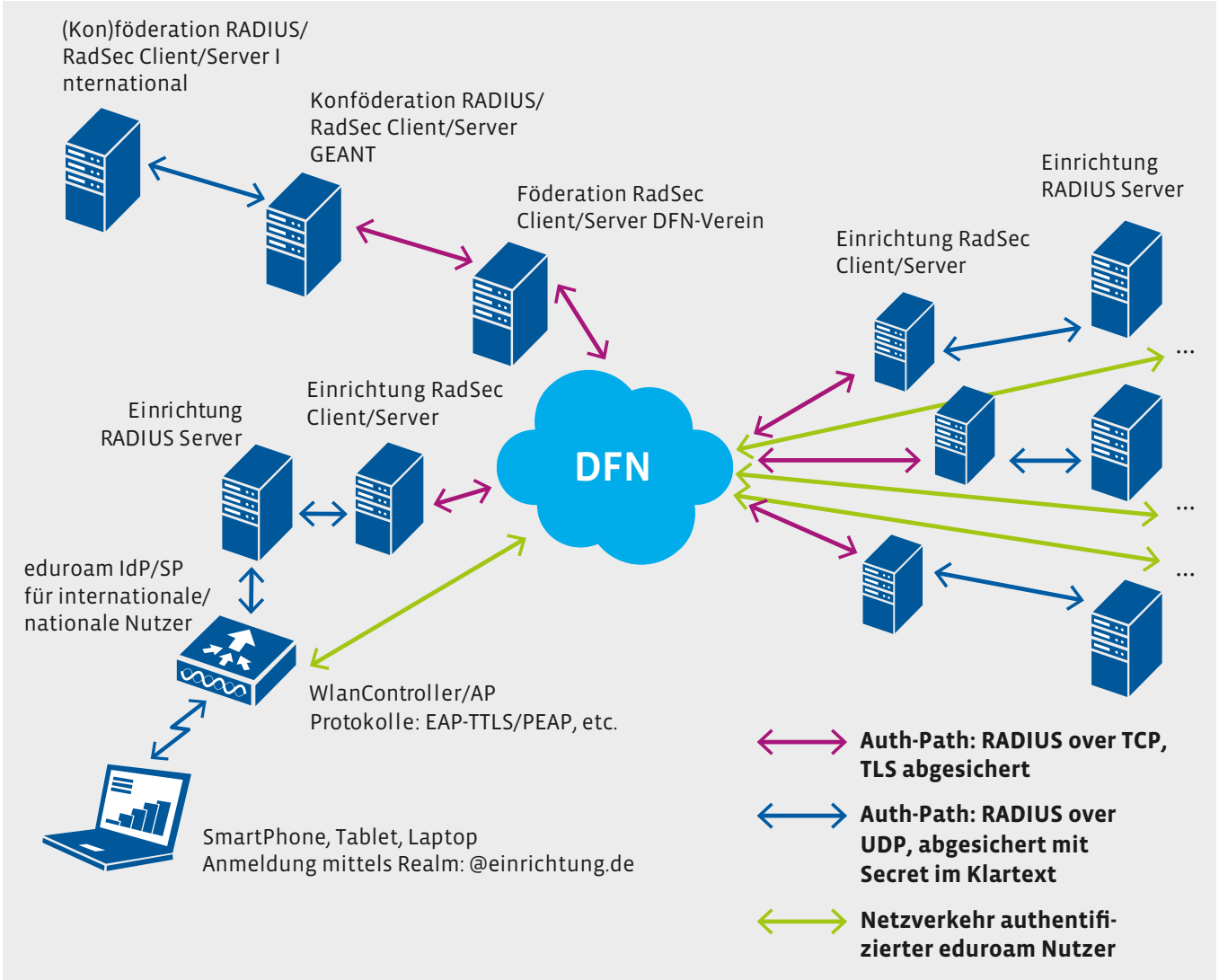


Source: Kohls et al.

Source:

- Katharina Kohls et al.: *On the Challenges of Gepgraphical Avoidance for Tor*, Network and Distributed System Security Symposium (NDSS 2019), San Diego, California, USA, February 2019, pdf + slides
- 31C3 Talk: Dr. Gareth Owen, 2014: *Tor: Hidden Services and Deanonymisation*
- 32C3 talk: Roger and asn, *Tor onion services: more useful than you think*, 2015

12. Topic: RADIUS: The protocol behind Eduroam



Source: DFN Mitteilungen Ausgabe 94, Dezember 2018, p. 13

Source:

- Remote Authentication Dial In User Service (RADIUS), RFC 2865 (updated by RFC 2868, 3575, 5080, 6929, 8044)
- Remote Authentication Dial-In User Service (RADIUS) Protocol Extensions, RFC 6929, 2013 (erster RFC 2058, 1997)
- TLS benuzt Zertifikate. Was passiert, wenn eine Einrichtung ihr Serverzertifikat widerruft? Jan-Frederik Rieckers (studentischer Mitarbeiter am Zentrum für Netze der Universität Bremen): (Probleme beim) Widerruf von Zertifikaten für RADIUS-Server, 71. DFN-Betriebsstagung, 9'2019 **(in German)**
- FAQ zu eduroam vom DFN **(in German)**

Topic List I

1. Wireless Communication: WLAN and WPA2 (IEEE 802.11 and IEEE 802.11i)
2. Wireless Communication: Bluetooth - The architecture and protocol stack
3. Wireless Communication: Bluetooth - Security
4. Mobile Communication: 4G Broadband Cellular Networks: Long Term Evolution (LTE) and the IMP4GT attacks
5. Security aspects of 5G
6. Data over Sound - Übertragung per Ultraschall
7. (Secure) IPv6
8. Secure IPv6: The idsv6 Benchmark
9. Secure IPv6 with Hyhoneydv6

Topic List II

10. **C-Roads and C-ITS services (Infrastructure-to-Vehicle Communication)**
11. **Tor for anonymous communication**
12. **RADIUS: The protocol behind Eduroam**

"Present to inform, not to impress; if you inform, you will impress."
- Frederick P. Brooks, Jr.