



# Breaking LTE on Layer Two

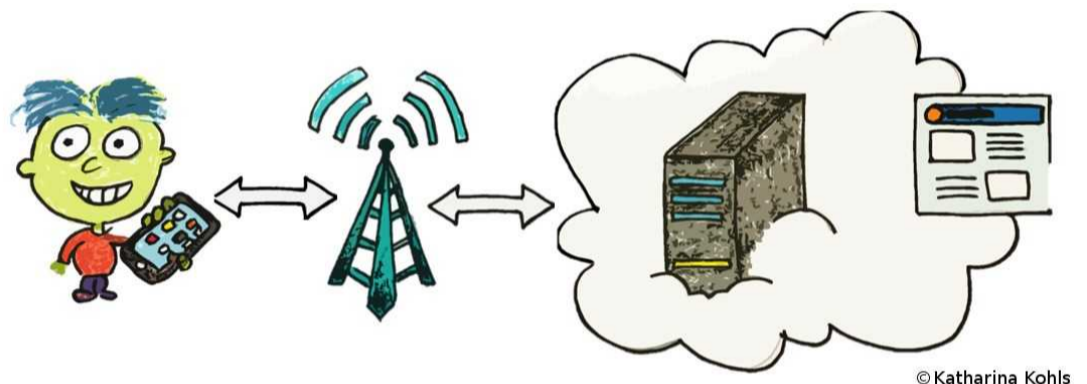
David Rupprecht, Katharina Kohls, Thorsten Holz, and Christina Pöpper

Ruhr-Universität Bochum & New York University Abu Dhabi

## Introduction

### Security Analysis of Layer Two

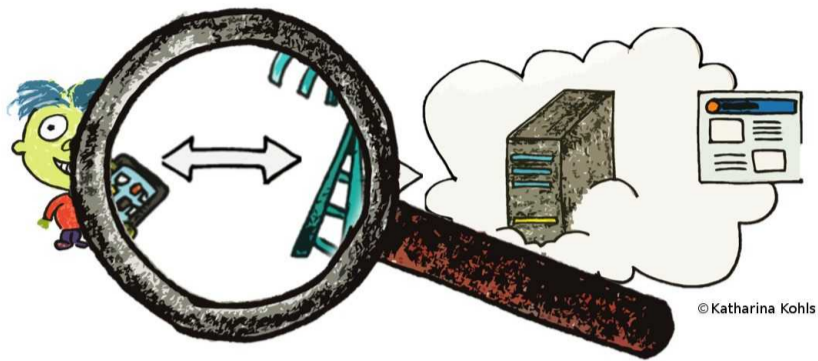
Our security analysis of the mobile communication standard LTE ([Long-Term Evolution](#), also known as 4G) on the data link layer (so called *layer two*) has uncovered three novel attack vectors that enable different attacks against the protocol. On the one hand, we introduce two passive attacks that demonstrate an *identity mapping* attack and a method to perform *website fingerprinting*. On the other hand, we present an active cryptographic attack called *aLTER attack* that allows an attacker to redirect network connections by performing DNS spoofing due to a specification flaw in the LTE standard. In the following, we provide an overview of the website fingerprinting and aLTER attack, and explain how we conducted them in our lab setup. Our work will appear at the [2019 IEEE Symposium on Security & Privacy](#) and all details are available in a [pre-print version of the paper](#).



### Consequences

- **How practical are the attacks?** We conducted the attacks in an experimental setup in our lab that depends on special hardware and a controlled environment. These requirements are, at the moment, hard to meet in real LTE networks. However, with some engineering effort, our attacks can also be performed in the wild.
- **What can happen?** We present three individual attacks: For mapping user identities in the radio cell (see [paper for details](#)), for [learning which websites a user accessed](#), and for performing an [alteration attack](#) (e.g., on DNS traffic) that can be used to redirect and thus hijack network connections.
- **Can this happen to me?** In theory yes, *but expect the effort to be high*. The most likely victims of such targeted attacks in practice are persons of special interest (e.g., politicians, journalists, etc.).
- **Who knows about the attacks?** We informed relevant institutions such as the GSM Association ([GSMA](#)), 3rd Generation Partnership Project ([3GPP](#)) and telephone companies in a responsible disclosure process before publishing this work.

# Background



## Data Link Layer (Layer Two)

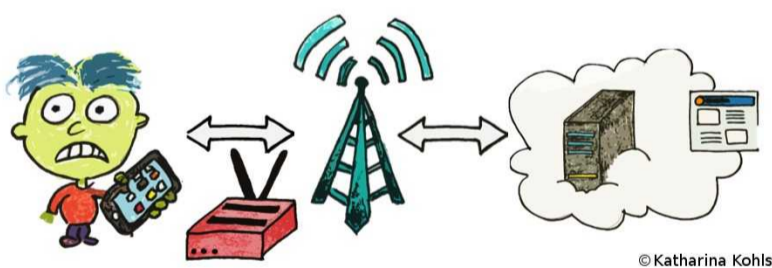
LTE is a complex collection of protocol specifications that define how the network functions. In general, there are two types of traffic: *control traffic* and *user traffic*. Control traffic organizes how the user traffic is sent and received, whereas the user traffic is the actual payload, e.g., the content of the visited website. In our analysis, we focus entirely on the second layer (layer two) of the LTE specification. This *data link layer* lies on top of the physical channel, which maintains the wireless transmission of information between the users and the network. Layer two organizes how multiple users can access the resources of the network, helps to correct transmission errors, and protects data through encryption.

## Security Mechanisms

To provide a secure transmission, LTE uses several security mechanisms. When Bob's phone connects to the network, it establishes mutual authentication and derives a shared key. Mutual authentication means that the network and the phone can verify the identity of the partner, respectively. In the following communication, the derived key is used to encrypt the control and user traffic. Furthermore, the control traffic is integrity protected, which means that the attacker is not able to manipulate the traffic during the transmission. Despite these security mechanisms, we found passive and active attacks that allow to observe which websites Bob accessed and even to redirect him to a fake website.



## Passive Attacks

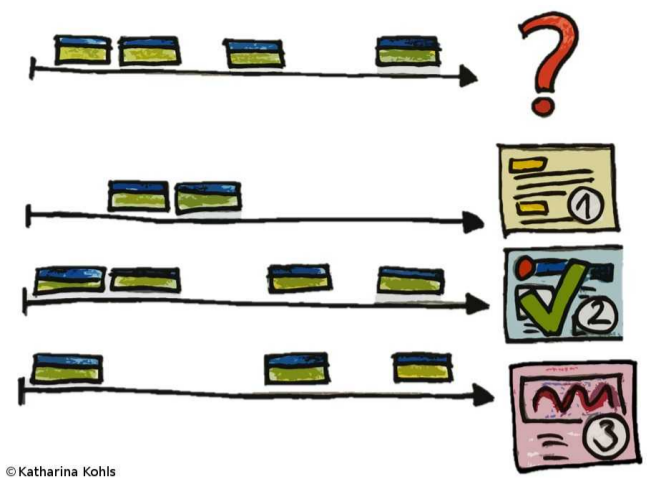


## What are Passive Attacks?

In a passive attack, the adversary does not interfere with the network, but only eavesdrops on a connection. The eavesdropper Eve accomplishes this by deploying a sniffing device close to Bob. As a result, she has access to all information that Bob sends to the network and receives in response, e.g., the website he wants to access. The data Link Layer protects transmissions through encryption. Nevertheless, an attacker can still obtain meta-information about the communication process (e.g., when and how often data is transmitted).

## Website Fingerprinting

Meta-information on the data link layer leak information about the consumption of data per time unit. For example, if Bob watches a video, he uses more traffic compared to when he accesses a simple website. As a preparation step of the attack, Eve records popular websites and their layer two patterns. During the attack, she eavesdrops the meta-information and looks for similar patterns. In case she finds a match, she knows which website the victim visited -- with a certain probability.



© Katharina Kohls

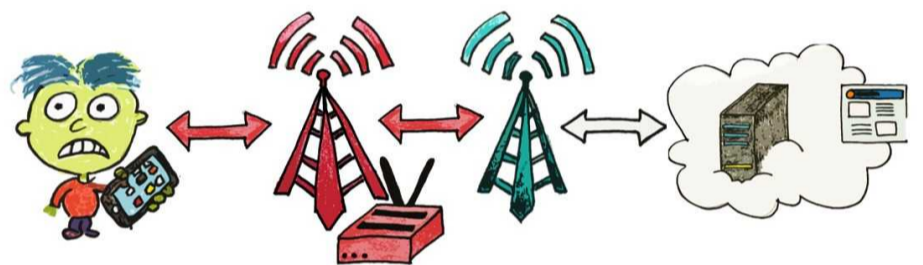


## Experiments and Results

We conducted a website fingerprinting attack in our lab setup of an LTE network and tested different devices on a selection of the 50 most popular websites on the Internet. We use this experimental evaluation to demonstrate the general feasibility of website fingerprinting on encryption data link layer traffic in LTE. Our results indicate that such attacks, in fact, are possible: we achieve an average success rate of about  $89\% \pm 10$ . In future experiments, we plan to conduct the same experiments within a commercial network, which complicates the attack due to background noise and uncontrolled network dynamics.

# Active Attack: aLTER

In an active attack, the adversary sends signals to the network or to the device by using a specific device that is capable of simulating the legitimate network or user device. In our case, the adversary does both and intercepts all transmissions between Bob and the network. Thus, Bob perceives the adversary as his usual network provider and connects to the simulation device. Towards the real network, the adversary acts like she was Bob.



© Katharina Kohls



© Katharina Kohls

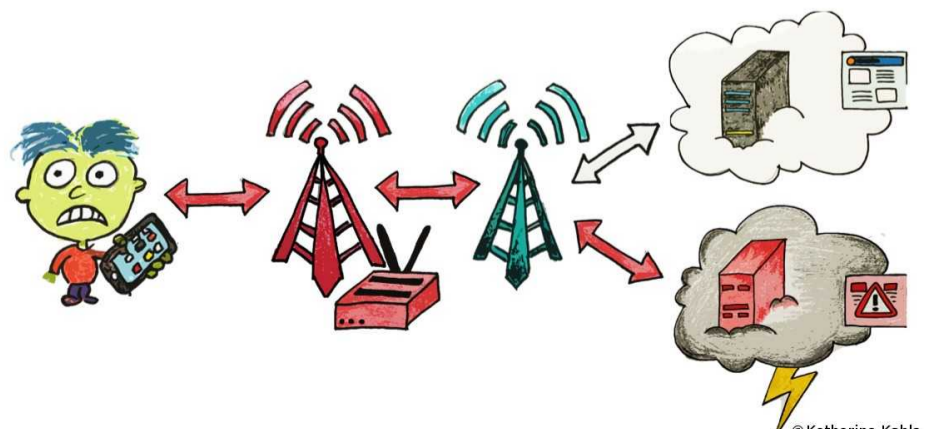
## User Data Redirection

LTE uses mutual authentication on the layers above the data link layer to prevent Bob's phone from connecting to a fake network. However, the layers below are unprotected and an attacker can forward high-layer messages. Bob's phone still assumes that he is connected to the original network. For the user data redirection attack, we exploit that the user data is not integrity protected. Thus an attacker can modify the content of a packet if she knows the original plain text, even the packet is encrypted. In the case of DNS packets, we know the destination address of the original DNS server. For the redirection, the attacker adds a specific offset, thus the DNS request is redirected to a DNS server under the adversary's control.

More technical speaking: User data is encrypted in counter mode (AES-CTR), where the encryption algorithm is used as a keystream generator, and the ciphertext is computed by XORing the keystream with the plaintext. In fact, this helps us to perform our attack given that the cipher is malleable.

## DNS Spoofing

The malicious DNS server performs DNS spoofing, meaning that the domain is resolved to a fake, malicious IP address. As a result, the phone sends a requests the wrong IP address. If the application layer protocol does not detect this malicious redirection, Bob gets redirected to a malicious website. DNS spoofing is a common attack on the Internet and can be performed when the attacker is for example under the control of



© Katharina Kohls

one hop to the original DNS server. Comparing the user data redirection attack, the attacker only needs to be in the proximity to the victim to perform such an attack.

## Results

To demonstrate the practical feasibility of the aLTER attack, we have implemented a full end-to-end version of the attack within a commercial network and commercial phone within our lab environment. We have implemented the LTE relay based on the open source LTE Software Stack [srsLTE](#) by [Software Radio System](#). We used a shielding box to stabilize the radio layer and prevent unintended inference with the real network. In addition, we set up two servers to simulate how an attacker can redirect network connections: our own DNS server that answers specific DNS queries with a malicious IP address and an HTTP server that replicates a login site to act as a phishing website. The following videos demonstrates the different steps of an aLTER attack.

### Demonstration of the aLTER attack in a commercial LTE network



## Technical Paper

---

Our work will appear at the [2019 IEEE Symposium on Security & Privacy](#). A [pre-print of the paper](#) that contains all details is already available ([PDF file](#)).

### Abstract

Long Term Evolution (LTE) is the latest mobile communication standard and has a pivotal role in our information society: LTE combines performance goals with modern security mechanisms and serves casual use cases as well as critical infrastructure and public safety communications. Both scenarios are demanding towards a resilient and secure specification and implementation of LTE, as outages and open attack vectors potentially lead to severe risks. Previous work on LTE protocol security identified crucial attack vectors for both the physical (layer one) and network (layer three) layers. Data link layer (layer two) protocols, however, remain a blind spot in existing LTE security research.

In this paper, we present a comprehensive layer two security analysis and identify three attack vectors. These attacks impair the confidentiality and/or privacy of LTE communication. More specifically, we first present a passive identity mapping attack that matches volatile radio identities to longer lasting network identities, enabling us to identify users within a cell and serving as a stepping stone for follow-up attacks. Second, we demonstrate how a passive attacker can abuse the resource allocation as a side channel to perform website fingerprinting that enables the attacker to learn the websites a user accessed. Finally, we present the ALTER attack that exploits the fact that LTE user data is encrypted in counter mode (AES-CTR) but not integrity protected, which allows us to modify the message payload. As a proof-of-concept demonstration, we show how an active attacker can redirect DNS requests and then perform a DNS spoofing attack. As a result, the user is redirected to a malicious website. Our experimental analysis demonstrates the real-world applicability of all three attacks and emphasizes the threat of open attack vectors on LTE layer two protocols.

### BibTeX

If you want to cite the paper, please use the following BibTeX entry:

```
@inproceedings{rupprecht-19-layer-two,  
  author = {Rupprecht, David and Kohls, Katharina and Holz, Thorsten and P\"{o}pper, Christina},  
  title = {Breaking {LTE} on Layer Two},  
  booktitle = {IEEE Symposium on Security \& Privacy (SP)},  
  year = {2019},  
  month = may,  
  publisher = {IEEE}  
}
```


# Frequently Asked Questions

---

[Can this happen to me?](#) 


[What does \*high effort\* mean?](#) 


[What does \*close proximity\* mean?](#) 

[What is the difference to \*IMSI catchers\*?](#) 

[Why are these attacks possible?](#) 

[What are possible countermeasures?](#) 

[Did you responsibly disclose the attacks?](#) 

[What is the current status of countermeasures in 5G?](#) 

[Is there a logo for the attacks?](#) 

BREAKING LTE ON LAYER TWO

David Rupprecht, Katharina Kohls, Thorsten Holz, and Christina Pöpper  
Ruhr-Universität Bochum & New York University Abu Dhabi

CONTACT

PRIVACY