DEMO: Demonstrating Practical Known-Plaintext Attacks against Physical Layer Security in Wireless MIMO Systems

Matthias Schulz
Secure Mobile Networking Lab
TU Darmstadt, Germany
mschulz@seemoo.de

Adrian Loch
IMDEA Networks Institute
Madrid, Spain
adrian.loch@imdea.org

Matthias Hollick
Secure Mobile Networking Lab
TU Darmstadt, Germany
mhollick@seemoo.de

ABSTRACT

After being widely studied in theory, physical layer security schemes are getting closer to enter the consumer market. Still, a thorough practical analysis of their resilience against attacks is missing. In this work, we use software-defined radios to implement such a physical layer security scheme, namely, orthogonal blinding. To this end, we use orthogonal frequency-division multiplexing (OFDM) as a physical layer, similarly to WiFi. In orthogonal blinding, a multi-antenna transmitter overlays the data it transmits with noise in such a way that every node except the intended receiver is disturbed by the noise. Still, our known-plaintext attack can extract the data signal at an eavesdropper by means of an adaptive filter trained using a few known data symbols. Our demonstrator illustrates the iterative training process at the symbol level, thus showing the practicability of the attack.

1. INTRODUCTION

Physical layer security schemes claim to be time-proof. In contrast to conventional security schemes, security at the physical layer does not rely on cryptographic mechanisms which may be broken in the future. In such conventional schemes, attackers may record protected frames in the hope of being able to decrypt them later. Physical layer security prevents this by not allowing attackers to successfully receive protected frames at all. In other words, attackers cannot even decode the data at the physical layer. This idea has quickly evolved from theory to practice and is getting closer to become a product. For instance, start-up companies have recently started to offer physical layer security solutions for key establishment and secure pairing.

Following the above evolution, orthogonal blinding was first proposed in theory [4] but quickly became a practical mechanism [2]. The underlying idea is to transmit artificial noise to prevent eavesdroppers from successfully decoding protected frames. To this end, the transmitter Alice uses multiple antennas—this allows her to transmit signals in multiple spatial dimensions. In particular, she transmits data into one of the dimensions, and artificial noise on all other orthogonal dimensions. The intended receiver Bob records the transmission using a single antenna. Hence, he only receives one of the dimensions. Alice precodes the data based on the unique channel state information (CSI) of her link to Bob such that it falls exactly into the dimension Bob can receive. As a result, Bob does not receive any of the orthogonal noise. An eavesdropper Eve with one antenna also receives one dimension. However, since she is located at a different position than Bob, Eve receives a combination of data and noise, and thus cannot decode.

Orthogonal blinding is based on two strong assumptions, namely, that Eve (a) only has one antenna, and (b) does not know any part of the protected frames. In earlier work [3], we have shown that orthogonal blinding is vulnerable if (a) and (b) do not hold. Intuitively, if Eve has as many antennas as Alice, she can receive all dimensions. Further, if Eve knows a certain amount of plaintext, such as frame headers, she can determine which of the dimensions contains the data. To this end, she trains an adaptive filter based on the known-plaintext, which she can then use to decode the rest of the frame. In [3], we perform a thorough analysis on how much known-plaintext is needed to train such a filter, and show the feasibility of the approach based on practical testbed traces. Recent work in this area improves our attack on orthogonal blinding even further. For instance, the training of the adaptive filter can converge faster when exploiting the similarity of adjacent subcarriers in an orthogonal frequency-division multiplexing (OFDM) system [5]. Moreover, instead of only exploiting known plaintext, an attack on orthogonal blinding can also guess the content of low entropy fields in wireless packets, thus enabling ciphertext-only attacks [6].

In this demonstration, we show the above attack interactively using the Wireless Open-Access Research Platform (WARP) software-defined radio (SDR) [1]. That is, in contrast to our trace-based study in [3], we run the attack online on the actual wireless channels at the conference location. This allows conference attendees to experiment with the positioning of the antennas of each of the three parties in our scenario, that is, Alice, Bob, and Eve. Moreover, attendees can observe the performance of our attack on orthogonal blinding on an intuitive graphical user interface. This includes detailed physical layer information, such as CSI and quadrature amplitude modulation (QAM) constellations. For more details, see the Appendix. In the remainder of this demo proposal we explain our attack in detail and provide more details on our interactive implementation.

WiSec'16 , July 18-22, 2016, Darmstadt, Germany
© 2016 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-4270-4/16/07.
DOI: http://dx.doi.org/10.1145/2939918.2942418

2. SYSTEM OVERVIEW

Our system consists of three nodes: (1) Alice who intends to securely communicate with (2) Bob and an eavesdropper (3) Eve, who passively listens on the wireless communication between Alice and Bob. To protect the communication between Alice and Bob, Alice makes use of orthogonal blinding, a physical layer security scheme that hampers correct signal decodings at non-intended receivers while allowing Bob to only receive the data signal. To make it work, Alice needs at least one more transmit antenna than Bob to be able to use an additional spatial dimension to transmit artificial noise into the null space of the channel between Alice and Bob. Receiving the same transmission over a different channel destroys the orthogonality between the spatial streams containing data and artificial noise. Hence, an unintended receiver always gets a superposition of artificial noise and data as thoroughly described in [2] and [3]. In our demo, we set the number of Bob's receive antennas to one, Alice has two, what allows her to transmit up to two spatial streams. To be able to receive all of Alice's spatial streams, Eve also requires two antennas. An exemplary demonstrator setup is illustrated in Fig. 1.

3. IMPLEMENTATION

Our demonstrator is implemented using WARPLab, which is an interface between MATLAB and the WARP SDR. It allows to generate and analyse baseband signals in MATLAB and only use the WARP nodes as radio interfaces to transmit signals on a WiFi channel in the 2.4/5 GHz bands. For transmission, WARPLab loads baseband signals into buffers in the WARP nodes and triggers a transmission over Ethernet. The receiving WARP nodes trigger a reception at the same time and store the received signals in buffers from which WARPLab picks up the signals for further processing in MATLAB. Even though, this implementation is real-time incapable, the delay between receptions and transmissions is low enough to stay below the coherence time of the wireless channel in static environments. This is important as Alice first measures the channel state information between her and Bob by transmitting an empty frame whose preamble is used for the measurement. Then, she generates a transmit filter based on the measurement, filters data and artificial noise with this filter and transmits the resulting frame. If the wireless channel had changed between the two transmissions, the null space of the channel would have changed, too, resulting in Bob's reception being disturbed by artificial noise. Eve's attack performance, however, is not influenced, if the channel changes as she only requires to receive the second frame containing the disturbed data.

Our baseband filter implementation is done according to [3]. As we use OFDM as underlying physical modulation scheme, we separate each of our frames into OFDM symbols in the time domain. Each of these symbols splits a 40 MHz wide band into 128 subcarriers of which 110 are usable for data transmissions. For each of these 110 subcarriers Alice generates separate transmit filters using the Gram-Schmidt algorithm [2, 3]. Those filters are fed with uniformly distributed random 4-QAM data symbols and uniformly distributed artificial noise symbols. To separate the noise from the data at the eavesdropper, she separately trains normalized least mean squares (NLMS) filters on each subcarrier. In each training iteration, Eve accesses an additional set of 110 of Alice's data symbols (one per subcarrier) and uses it as known plaintext to train the adaptive filter. The filter convergence is mainly influenced by the step-size μ, the wireless channel conditions and Eve's signal-to-noise ratio.

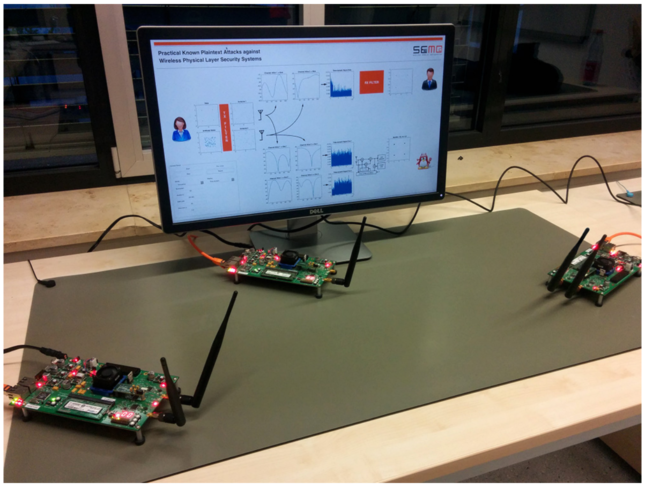

Practical Known Plaintext Attacks against Wireless Physical Layer Security Systems

Figure 1: Exemplary setup of the demo with WARP nodes for Alice (two antennas), Bob (one antenna) and Eve (two antennas) and a monitor displaying the user interface.

4. ACKNOWLEDGMENTS

This work has been funded by the German Research Foundation (DFG) in the Collaborative Research Center (SFB) 1053 “MAKI – Multi-Mechanism-Adaptation for the Future Internet”, by LOEWE CASED, and by BMBF/HMWK CRISP.

5. REFERENCES

[1] Rice university WARP project, 2016.

[2] N. Anand, S.-J. Lee, and E. Knightly. Strobe: actively securing wireless communications using zero-forcing beamforming. In *Proceedings of the 31st Annual IEEE International Conference on Computer Communications (IEEE INFOCOM 2012)*, 2012.

[3] M. Schulz, A. Loch, and M. Hollick. Practical known-plaintext attacks against physical layer security in wireless MIMO systems. In *Proceedings of the Network and Distributed System Security Symposium (NDSS 2014)*, 2014.

[4] Y. Yang, W. Wang, H. Zhao, and L. Zhao. Transmitter beamforming and artificial noise with delayed feedback: secrecy rate and power allocation. *IEEE Trans. Commun., Netw.*, 14:374–384, 2012.

[5] Y. Zheng, M. Schulz, W. Lou, Y. Hou, and M. Hollick. Highly efficient known-plaintext attacks against orthogonal blinding based physical layer security. *IEEE Wireless Communications Letters*, 4(1):34–37, Feb 2015.

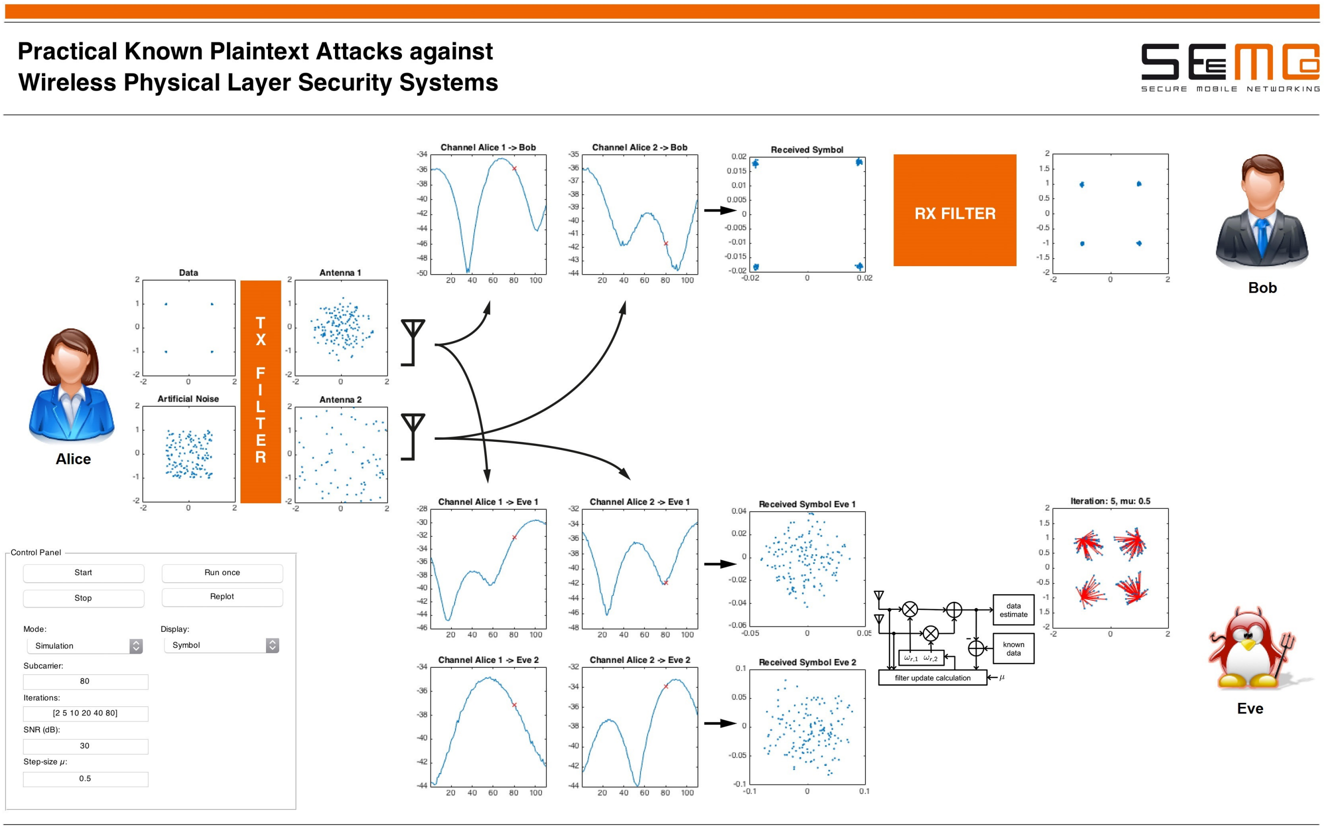
[6] Y. Zheng, M. Schulz, W. Lou, Y. Hou, and M. Hollick. Profiling the strength of physical-layer security: A study in orthogonal blinding. In *Proceedings of the 9th ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec 2016)*, 2016.

APPENDIX

Our demonstrator consists of three WARP SDR nodes. Each represents one communication party, in this case: Alice, Bob and Eve. All three nodes are connected by Ethernet to a computer that coordinates the experiments. It generates the baseband signals for the transmitters and analyzes the received baseband signals of the intended receiver and the eavesdropper. For the latter, the computer trains the adaptive filter.

The experiment is controlled by a graphical user interface illustrated in Fig. 2. On the left side, there is the transmitter, Alice, who generates 4-QAM data symbols and artificial noise symbols illustrated in the corresponding plots. All symbol plots contain all symbols of one OFDM frame at one subcarrier. The illustrated subcarrier can be selected in the control panel. Alice combines both symbols in the transmit filter ("TX FILTER") to generate symbols for each of her two antennas. After OFDM modulation, the antenna signals are either transmitted using WARP SDRs (mode set to "WARP Testbed" in the control panel) or simulated channels ("Simulation" mode) that do not require any radio hardware. The channel state information—measured between each of Alice's and each of the receivers' antennas—is illustrated as amplitudes over subchannel numbers in the plots labeled with "Channel . . . ". The red "x" marks the subcarrier used for the symbol plots. Right of the channel plots are either time-domain signals (currently not shown, as "Display" is set to "Symbol" instead of "Time-domain" in the control panel), or received symbol plots. One observes that Bob's symbols are very similar to Alice's data symbols with a small amount of additive white Gaussian noise (AWGN). In simulation, the amount of noise can be adjusted with the signal-to-noise ratio ("SNR") setting. Bob's receive filter "RX FILTER" just adjusts amplitude variations introduced by attenuation on the channel. Unlike Alice's symbols, Eve's symbols are additionally affected by artificial noise and cannot be correctly mapped to the transmitted 4-QAM symbols. To get out the transmitted symbols, Eve trains an adaptive filter with known-plaintext symbols. The filter output after a preselected number of training iterations is animated in the figure labeled with "Iterations: . . . " indicating the currently displayed training iteration. The red lines are error vectors and point to the locations, where the symbols are supposed to be, when filtering succeeds. How fast the filter adjusts its weights can be controlled by the step-size μ. In this example, it takes roughly 5 training iterations to be able to correctly decode the 4-QAM constellation.

One can control the experiment execution in the control panel in the lower left corner. The settings are already mentioned in the previous paragraph. Using the buttons, one can start and stop repeating experiment runs ("Start" and "Stop" buttons) or only run one experiment per button click ("Run once" button). Each run updates the graphs in the user interface. The "Replot" button restarts the plot function for the last experiment, which will reanimate the "Iterations . . . " plot and use updated settings regarding the analyzed subcarrier, the iterations to be plotted and the step-size.



Practical Known Plaintext Attacks against Wireless Physical Layer Security Systems

Control Panel

Mode: Simulation

Display: Symbol

Subcarrier: 80

Iterations: [2 5 10 20 40 80]

SNR (dB): 30

Step-size μ: 0.5

Figure 2: Screenshot of the graphical user interface used to control the experiments.