Opinion: PHY-Layer Security is no Alternative to Cryptography

Pieter Robyns
UHasselt - tUL - imec
Wetenschapspark 2
Diepenbeek 3590, Belgium
pieter.robyns@uhasselt.be

Peter Quax
UHasselt - tUL - imec
Wetenschapspark 2
Diepenbeek 3590, Belgium
peter.quax@uhasselt.be

Wim Lamotte
UHasselt - tUL - imec
Wetenschapspark 2
Diepenbeek 3590, Belgium
wim.lamotte@uhasselt.be

ABSTRACT

In recent works, numerous physical-layer security systems have been proposed as alternatives to classic cryptography. Such systems aim to use the intrinsic properties of radio signals and the wireless medium to provide confidentiality and authentication to wireless devices. However, fundamental vulnerabilities are often discovered in these systems shortly after their inception. We therefore challenge the assumptions made by existing physical-layer security systems, and postulate that weaker assumptions are needed in order to adapt for practical scenarios. We also argue that if no computational advantage over an adversary can be ensured, secure communication cannot be realistically achieved.

CCS CONCEPTS

•Security and privacy → Information-theoretic techniques; Mobile and wireless security;

KEYWORDS

PHY-layer security; cryptography; opinion

ACM Reference format:
Pieter Robyns, Peter Quax, and Wim Lamotte. 2017. Opinion: PHY-Layer Security is no Alternative to Cryptography. In *Proceedings of WiSec '17, Boston, MA, USA, July 18-20, 2017,* 3 pages.
DOI: 10.1145/3098243.3098271

1 INTRODUCTION

In Physical (PHY)-layer security schemes, secure wireless communication between multiple entities is achieved by solely relying on intrinsic properties of radio signals and the wireless medium. Here, the work entitled "The Wire-Tap Channel" and presented by Wyner in 1975 [18] is considered as the information-theoretic foundation of such systems [21], and has been cited in more than 3,900 related works over the past decades. Building upon the ideas of Wyner's seminal paper, several PHY-layer security systems have been proposed; each with their own methodology for providing secrecy by making use of PHY-layer properties of the wireless channel. Some example use cases for these PHY-layer security systems can be found in the domains of authentication [8, 10, 16], key generation [17, 20], and secure communications [2, 7]. Unfortunately, these systems are often designed under assumptions that do not hold true in practice, e.g. that the Channel State Information (CSI) of all entities (including the adversary) is known, and that multiple nodes are willing to cooperate in order to achieve secrecy [19]. As a consequence, many PHY-layer security schemes have been proven to be broken in practice after a closer examination in subsequent research. Several examples of attacks on PHY-layer security systems can be found in [4, 14, 15, 21]. As such, we believe there is a need for a more rigorous evaluation of PHY-layer security systems under weaker and thus more realistic assumptions. In this opinion paper, we hope to start a discussion surrounding these assumptions in practical scenarios, and posit that systems which operate under impractical assumptions should not be suggested as alternatives to classic cryptography.

978-1-4503-5084-6/17/07…$15.00
DOI: 10.1145/3098243.3098271

2 CONFIDENTIALITY ON THE PHYSICAL LAYER

The work of Wyner demonstrates how a reliable and secure communication channel can be established between two entities, Alice and Bob, in the presence of an eavesdropper Eve without exchanging any prior secret credentials. This is accomplished under the condition that Eve's channel is different and degraded compared to Bob's channel. In this case, the usage of stochastic code words allows Bob to decode the message, whereas Eve observes only a corrupted message that is indistinguishable from uniform random noise [18]. Should the channel from Alice to Bob be worse than the channel from Alice to Eve, then secure communication is not possible [19].

Many works have since built upon this idea by improving the relative *channel advantage* over Eve. This can be achieved by deliberately transmitting noise to Eve in order to further degrade her channel, which in turn increases the secrecy between Alice and Bob. Examples of such techniques are cooperative jamming [6], friendly jamming [7], and orthogonal blinding [2]. Although these systems can indeed provide provable security under ideal circumstances, recent works have shown that they can be broken under weaker adversarial assumptions. For instance, Tippenhauer et al. found that friendly jamming techniques are vulnerable if an adversary can discern and filter out the jamming signals, e.g. by using multiple antennas [15]. Similar attacks have been performed by Yao and Schulz et al. to break confidentiality in systems that implement orthogonal blinding [14, 21].

Besides jamming, other works have employed different strategies for achieving secrecy. For example, the reciprocity property of the wireless channel can be used in order to derive a secret key for subsequent communications [17, 20]. In a reciprocal channel, the channel impulse response is assumed to be identical at the sender and receiver. Consequently, when Alice and Bob measure each other's CSI through probing signals, the resulting observations are highly correlated. However, in practice, subtle manufacturing-induced hardware differences between the sender and receiver necessitate

either a prior calibration between both entities or an error correction on the received signals. Here, the former makes the approach less pragmatic, whereas the latter leaks information to Eve. Furthermore, Eve must be at least half a wavelength away from the communicating entities in order to guarantee a degradation of her channel due to fading and noise [17, 20].

Discussion

Based on the examples discussed above, we have seen that when Eve possesses multiple antennas or transceivers, she can increase her channel advantage and subsequently break the confidentiality provided between Alice and Bob. We therefore posit that for the evaluation of PHY-layer confidentiality in practice, a determined adversary with better hardware capabilities than the cooperating entities should be assumed. Furthermore, the adversary should be assumed to be active, i.e. they can manipulate or jam the channel with arbitrary transmissions.

Another fundamental assumption is the distance between Eve and Alice or Bob. In practical scenarios, one would prefer a system that is secure regardless of the distance between an adversary and any communicating entities. That is, it should be assumed that an adversary can roam freely and interact with the channel from any physical location. However, as the distance between for example Eve and Alice decreases, their channel conditions become more similar to each other, which breaks Wyner's condition that Eve's channel must be degraded in comparison to Alice's channel. Now, Bob's attempts at degrading Eve's channel through jamming become futile, as Alice's channel will undergo the same effects. Furthermore, if Eve possesses identical or better radio hardware than Alice, the same information can be extracted from the wireless channel, which thwarts PHY-layer key derivation mechanisms that rely on fading effects. Although work has been done on investigating the effect of the proximity to the adversary (see for example [2]), it would be beneficial to combine this investigation with weaker assumptions about CSI knowledge and the adversary's available hardware or behavior.

In Figure 1, we illustrate an example setup that can be considered as a worst-case scenario for PHY-layer security systems. Here, both Alice and Eve utilize the same radio hardware and antenna array, which provides I/Q samples over a wired link to their respective host machines. Such setups can be trivially realized in practice through the usage of Software Defined Radios (SDRs). Now, both Alice and Eve receive the same information about the channel, but are otherwise individually responsible for processing the I/Q samples on their host machines. Under these circumstances, we hypothesize that any PHY-layer security scheme intended to provide secrecy between Bob and Alice is practically broken, if Alice and Bob have no computational advantage over Eve. More specifically, given that Eve has knowledge about the algorithms used in the PHY-layer security scheme, she can use the information contained within the channel to break confidentiality. Observe that for traditional cryptographic approaches based on *computational advantage*, secrecy can be obtained in the setup of Figure 1 by letting Alice and Bob engage in a secure key exchange protocol or by pre-installing secret keys on their devices.

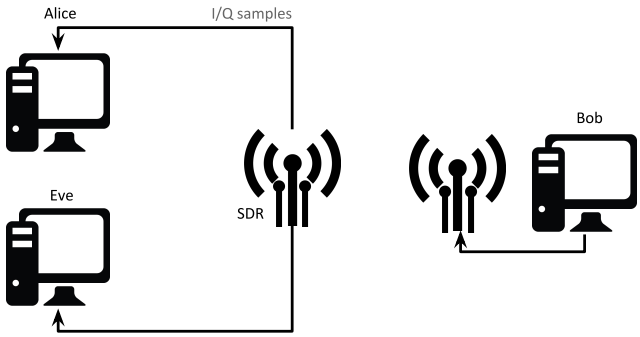

Figure 1: An example setup where Eve is guaranteed to have the same information as Alice about the wireless channel, although both are independently responsible for processing this information. The closer this situation is approximated in practice, the more vulnerable a PHY-layer security system will be to attacks.

3 PHYSICAL-LAYER IDENTIFICATION

Identification on the physical layer generally involves two entities, namely the prover and verifier, where the verifier must determine the identity of the prover based on information from the wireless channel. The goal of the adversary is then to impersonate the prover by transmitting spoofed frames to the verifier. PHY-layer identification systems have been proposed in the domains of authentication [8, 10, 16], relay and replay attack countermeasures [9, 11], and others [1, 3, 13].

A typical PHY-layer identification system comprises of two stages: a training and testing phase. In the training phase, the system trains on uniquely identifying features observed from the prover's radio transmissions in order to construct a fingerprint. In the testing phase, said fingerprint can be used to authenticate transmissions of the prover. The adversary is assumed to be unable to impersonate the prover, since they were not present during the training phase, and since the intrinsic features of the adversary's radio would modify the resulting transmission such that an attack can be detected [12].

Discussion

In some works, PHY-layer identification approaches are related to biometric authentication systems due to their similar modus operandi [5, 10, 12]. However, a notable difference is that a PHY-layer fingerprint is broadcast over the wireless medium, whereas in biometric authentication, the unique fingerprint is transmitted via a side channel that cannot be observed by the adversary. Consequently, the adversary has an advantage in PHY-layer authentication systems: they can observe a (degraded) version of the prover's fingerprint.

As shown by Danev et al., PHY-layer identification systems are vulnerable to attacks for the above reason. An adversary can obtain the PHY layer fingerprint with a high sample rate signal analyzer, modify the signal in the digital domain and then replay the resulting signal in order to impersonate other wireless devices [4]. Therefore, one can argue that the assumption that the adversary's radio hardware causes a detectable modification of the fingerprint upon transmission does not hold in practical scenarios.

Furthermore, a conflicting tradeoff between the noise resistance and spoofing resistance can be identified in systems that rely on PHY-layer identification for authentication. That is, a PHY-layer identification system with high noise tolerance will be easier to spoof when the small changes introduced to the signal by the adversary's hardware are under the noise floor. Conversely, a system that is capable of detecting these small changes might be unable to recognize legitimate devices when the channel conditions change. Even so, an adversary might still be able to spoof a message with low probability due to fluctuations in the wireless channel. We hypothesize that due to these limitations, PHY-layer identification systems do not increase the security in practical scenarios if an adversary can obtain and analyze a transmission from the prover.

4 PHY-LAYER SECURITY SYSTEM DEPLOYMENTS

Now that we have considered a number of weaker assumptions for PHY-layer security systems, the question remains of how a well-designed PHY-layer deployment would compare against a classic cryptographic deployment in terms of cost and performance. For this discussion we assume that a PHY-layer security system exists where an adversary cannot obtain a channel advantage under any circumstance.

In terms of the manufacturing cost, PHY-layer security systems would not require additional hardware to perform cryptographic operations. However, in order to create a channel advantage, the CSI of intended receivers must be measured continuously to account for changes in the channel and movement of participating nodes. Furthermore, if jamming is used to degrade the adversary's channel, each transmission requires the expense of additional power. These operations thus introduce additional operational costs in terms of power and performance for every transmission.

On the other hand, classic cryptographic solutions would require specialized hardware to perform the cryptographic operations in a timely manner. Additionally, keys would need to be installed or agreed upon between devices before communication can take place. Nevertheless, there would be no need to continuously evaluate the CSI of other receivers or jam the adversary's channel, and operational costs would therefore be lower.

With these assumptions about cryptographic and PHY-layer security systems in mind, we believe the cost of maintaining PHY-layer security systems would be greater than that of a cryptography-based system. The incentive for adoption by the industry would therefore be low, although a combination between PHY-layer security and cryptography could be considered for the protection of critical infrastructure in this scenario.

5 CONCLUDING REMARKS

In this opinion paper, we have briefly discussed some of the assumptions made in PHY-layer security systems with regard to confidentiality and authentication. We believe that a *combination* of weaker assumptions about knowledge of the CSI, adversarial hardware, adversarial knowledge and behavior, and distance should be considered more attentively in future PHY-layer security research. Although proving security under these weaker assumptions is difficult, we conjecture that researchers should at least consider practical scenarios in the design phase of the PHY-layer security system. We have further touched upon deployments of PHY-layer security systems, and argue that the cost of such systems should be decreased in order to compete with classic cryptography.

ACKNOWLEDGEMENTS

This research was funded by a Ph.D. Grant of the Research Foundation Flanders (FWO).

REFERENCES

[1] O. R. Afolabi, K. Kim, and A. Ahmad. On secure spectrum sensing in cognitive radio networks using emitters electromagnetic signature. In *Proceedings of 18th Internatonal Conference on Computer Communications and Networks*, pages 1–5. IEEE, 2009.

[2] N. Anand, S.-J. Lee, and E. W. Knightly. Strobe: Actively securing wireless communications using zero-forcing beamforming. In *INFOCOM*, pages 720–728. IEEE, 2012.

[3] B. Danev, T. S. Heydt-Benjamin, and S. Capkun. Physical-layer Identification of RFID Devices. In *Usenix Security Symposium*, pages 199–214, 2009.

[4] B. Danev, H. Luecken, S. Capkun, and K. El Defrawy. Attacks on physical-layer identification. In *Proceedings of the third ACM conference on Wireless network security*, pages 89–98. ACM, 2010.

[5] B. Danev, D. Zanetti, and S. Capkun. On physical-layer identification of wireless devices. *ACM Computing Surveys (CSUR)*, 45(1):6, 2012.

[6] L. Dong, Z. Han, A. P. Petropulu, and H. V. Poor. Cooperative jamming for wireless physical layer security. In *IEEE/SP 15th Workshop on Statistical Signal Processing*, pages 417–420. IEEE, 2009.

[7] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu. They can hear your heartbeats: non-invasive security for implantable medical devices. *ACM SIGCOMM Computer Communication Review*, 41(4):2–13, 2011.

[8] J. Hall, M. Barbeau, and E. Kranakis. Enhancing intrusion detection in wireless networks using radio frequency fingerprinting. In *Communications, Internet, and Information Technology*, pages 201–206, 2004.

[9] B. W. Ramsey, T. D. Stubbs, B. E. Mullins, M. A. Temple, and M. A. Buckner. Wireless infrastructure protection using low-cost radio frequency fingerprinting receivers. *International Journal of Critical Infrastructure Protection*, 8:27–39, 2015.

[10] B. W. Ramsey, M. A. Temple, and B. E. Mullins. PHY foundation for multi-factor ZigBee node authentication. In *Global Communications Conference (GLOBECOM)*, pages 795–800. IEEE, 2012.

[11] K. B. Rasmussen and S. Capkun. Implications of radio fingerprinting on the security of sensor networks. In *Third International Conference on Security and Privacy in Communications Networks*, pages 331–340. IEEE, 2007.

[12] S. U. Rehman, K. Sowerby, and C. Coghill. RF fingerprint extraction from the energy envelope of an instantaneous transient signal. In *Australian Communications Theory Workshop (AusCTW)*, pages 90–95. IEEE, 2012.

[13] D. R. Reising, M. A. Temple, and M. J. Mendenhall. Improving intra-cellular security using air monitoring with RF fingerprints. In *Wireless Communications and Networking Conference (WCNC)*, pages 1–6. IEEE, 2010.

[14] M. Schulz, A. Loch, and M. Hollick. Practical Known-Plaintext Attacks against Physical Layer Security in Wireless MIMO Systems. In *NDSS*, 2014.

[15] N. O. Tippenhauer, L. Malisa, A. Ranganathan, and S. Capkun. On limitations of friendly jamming for confidentiality. In *IEEE Symposium on Security and Privacy (SP)*, pages 160–173. IEEE, 2013.

[16] O. Ureten and N. Serinken. Wireless security through RF fingerprinting. *Canadian Journal of Electrical and Computer Engineering*, 32(1):27–33, 2007.

[17] Q. Wang, K. Xu, and K. Ren. Cooperative secret key generation from phase estimation in narrowband fading channels. *IEEE Journal on selected areas in communications*, 30(9):1666–1674, 2012.

[18] A. D. Wyner. The wire-tap channel. *Bell Labs Technical Journal*, 54(8):1355–1387, 1975.

[19] A. Yener and S. Ulukus. Wireless physical-layer security: lessons learned from information theory. *Proceedings of the IEEE*, 103(10):1814–1825, 2015.

[20] K. Zeng. Physical layer key generation in wireless networks: challenges and opportunities. *IEEE Communications Magazine*, 53(6):33–39, 2015.

[21] Y. Zheng, M. Schulz, W. Lou, Y. T. 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 & Privacy in Wireless and Mobile Networks*, pages 21–30. ACM, 2016.