Trust The Wire, They Always Told Me! On Practical Non-Destructive Wire-Tap Attacks Against Ethernet

Matthias Schulz,
Patrick Klapper, Matthias Hollick
Secure Mobile Networking Lab
TU Darmstadt, Germany
{mschulz,pklapper,mhollick}
@seemoo.tu-darmstadt.de

Erik Tews
School of Computer Science
University of Birmingham
United Kingdom
erik@datenzone.de

Stefan Katzenbeisser
Security Engineering Group
TU Darmstadt
Germany
katzenbeisser@seceng.
informatik.tu-darmstadt.de

ABSTRACT

Ethernet technology dominates enterprise and home network installations and is present in datacenters as well as parts of the backbone of the Internet. Due to its wireline nature, Ethernet networks are often assumed to intrinsically protect the exchanged data against attacks carried out by eavesdroppers and malicious attackers that do not have physical access to network devices, patch panels and network outlets. In this work, we practically evaluate the possibility of *wireless* attacks against *wired* Ethernet installations with respect to resistance against eavesdropping by using off-the-shelf software-defined radio platforms. Our results clearly indicate that twisted-pair network cables radiate enough electromagnetic waves to reconstruct transmitted frames with negligible bit error rates, even when the cables are not damaged at all. Since this allows an attacker to stay undetected, it urges the need for link layer encryption or physical layer security to protect confidentiality.

1. INTRODUCTION

Since the late 1980s, Ethernet has been the dominant wired network technology. As of today, it connects all kind of networked devices in home and enterprise networks. Also for industrial machine-to-machine communication, EtherCAT [3] interconnects devices in the domain of process automation to exchange real-time control messages. Ethernet variants such as IEEE 802.3bw are targeting automotive applications.

Despite constant evolution in terms of performance and application-specific solutions, the security of Ethernet installations is rarely questioned. Due to the wireline nature, Ethernet networks are often assumed to intrinsically protect data transmissions from attackers in close proximity that do not have physical access to the end-systems, the wiring and switching closets, or network outlets. In this paper, we challenge this assumption and investigate eavesdropping attacks against Ethernet. We assume an attacker in close proximity to Ethernet cables, who operates non-destructively, not physically tampering with the cable. Our goal is to demonstrate in how far Ethernet is prone to wireless eavesdropping and that an attacker getting close enough to an Ethernet cable is able to extract private information without damaging the cable.

Even though Wi-Fi transmissions are generally encrypted, hence, hard to eavesdrop, the backhaul network is still wired and, most importantly, often not secured by link-layer encryption. Additionally, access to network cables is often as easy as opening a removable floor or a hung ceiling where cables are installed in many companies. Cutting those cables to place physical wire-taps is effective but also conspicuous. Hence, in this work, we focus on non-destructive (*wireless*) eavesdropping attacks against cable-based networks, using wireless near field probes.

That information leak by electromagnetic radiation (EMR) was discovered by Bell Labs in the 1940s and documented under the name TEMPEST in [1]. In the following years, countermeasures were designed. Bell Labs proposed to apply shielding against radiation of magnetic fields, filtering against signal leakage through power and signal lines, and masking against radiated signals. Budget-limited consumer products usually do not implement any of those countermeasures and are therefor vulnerable to those attacks.

The purpose of this work is to demonstrate how information can be extracted from Ethernet networks based on twisted-pair cables with different degrees of shielding. To summarize, our contributions are as follows:

- we capture and analyze signals radiated by Ethernet cables
- we implement an software-defined radio (SDR)-based Ethernet eavesdropper and evaluate its performance
- we discuss countermeasures against our attack.

We structure this work as follows: In Sec. 2 we present the system and attack model, followed by background information in Sec. 3 and the experimental setup in Sec. 4. Then, we describe the implementation of our eavesdropper in Sec. 5, present our practical evaluation in Sec. 6, followed by a discussion in Sec. 7 and countermeasures against our attack in Sec. 8. Finally, we conclude the paper with related work in Sec. 9 and a conclusion in Sec. 10.

WiSec'16 , July 18-22, 2016, Darmstadt, Germany

DOI: http://dx.doi.org/10.1145/2939918.2940650

2. SYSTEM AND ATTACK MODEL

In our system model, we consider an Ethernet link consisting of twisted-pair cables, an optional patch panel and two connected devices. In general, these can be any kind of device with an Ethernet port, such as computers, machine control units, or switches. For our experiments, we consider two directly interconnected computers that exchange information over this Ethernet link, as illustrated in Fig. 1.

Our attacker's intend is eavesdropping on the information transmitted over the Ethernet link. We assume that the attacker can get close to the cable to install probes that capture wireless signals. The attacker is, however, not allowed to damage the cable itself, for example, by opening the cable to attach mechanical wire taps.

3. BACKGROUND

We start with an introduction into the IEEE 802.3 physical layer with respect to waveforms and cable types to better follow the attack and countermeasures sections in this paper.

3.1 IEEE 802.3 waveforms

For this work, we focus on Ethernet standards using twisted-pair cables. Depending on transmission speed, IEEE 802.3 defines different modulation schemes. For 10 Mbps (10BASE-T, 802.3i) Manchester encoding is used on two twisted wire pairs. It encodes bits in transitions between two voltage levels. This allows easy clock extraction and robust signal decoding, but doubles the bandwidth requirements. For 10 Mbps with 1 bit per symbol, a bandwidth of 20 MHz is required. 100BASE-TX (802.3u) increases the transmission speed by a factor of ten by increasing the bandwidth to 125 MHz, while simultaneously using a more bandwidth efficient MLT-3 line encoding than Manchester coding. In combination with 4B5B block coding, speeds of 100 Mbps can be reached with 20 percent overhead for error correction coding. 1000BASE-T (802.3ab) increases its speed by using four wire pairs simultaneously, transferring 250 Mbps on each of them. To keep the 100BASE-TX's bandwidth of 125 MHz, a five level pulse amplitude modulation (PAM-5) is used in combination with more efficient forward error correction (FEC), that leads to less than 14 percent overhead. Eavesdropping 1000BASE-T is especially complicated as four simultaneous transmissions need to be separated.

3.2 Differential signaling over twisted-pairs

In 802.3 systems, twisted pair cables are used and fed by differential signals. These signals allow to eliminate interfering signals that couple equally into both wires. On the receiver side, subtracting both signals of a wire pair from each other, amplifies the differential signal components, while reducing the common-mode interfering signals. To additionally reduce the interference between wire pairs, signal emissions should be avoided. This is achieved by twisting wire pairs. In [16], Stolle shows that perfectly balanced twisted-pair cables with optimal terminations do not radiate differential signals traversing the wires. Common-mode signals, on the other hand, are radiated. In theory wireless eavesdropping in such a perfect setting is therefor not possible. As a wireless eavesdropper, we rely on receiving radiations, hence we aim at imperfections in practical wires as well as the effect of longitudinal conversion loss, that allows the conversion of differential-mode to common-mode signals due to asymmetries in a cable.

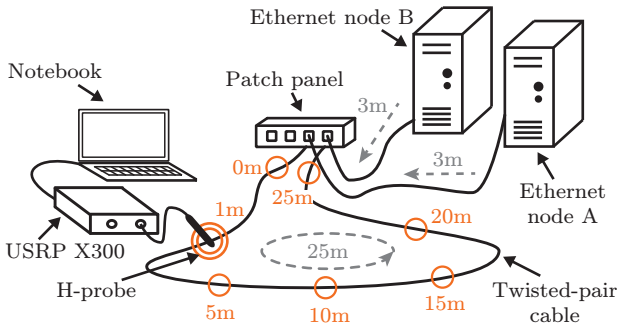


Figure 1: Lab environment for the eavesdropping attack evaluation

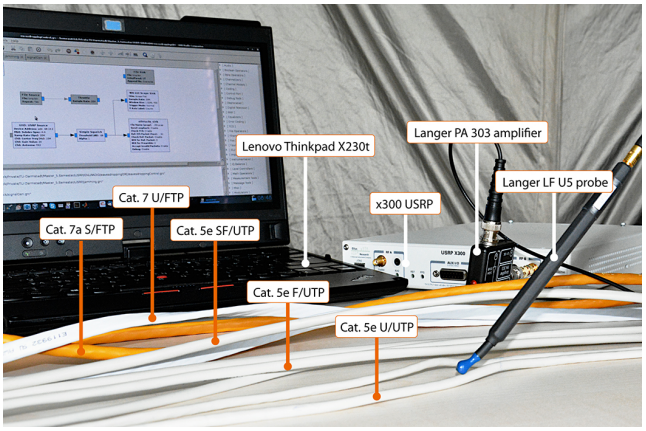


Figure 2: Lab environment including the cables under test, the Universal Software Radio Peripheral (USRP) and the H-field probe.

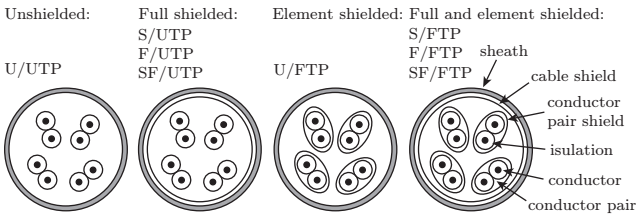


Figure 3: Differently shielded twisted-pair cables

3.3 Shielding

To additionally reduce the emission of electromagnetic radiation, different kinds of cable shieldings are used. The International Electrotechnical Commission (IEC) defines the naming scheme a/bTP in [10] to describe the overall shielding (a) and the individual shielding of twisted pairs (b) as unscreened (U), foil screened (F) or braid screened (S). In this work, we focus our analysis on U/UTP (patch cable, Cat. 5e), F/UTP, SF/UTP (both installation cables, Cat. 5e), U/FTP (flat cable, Cat. 7) and S/FTP (installation cable, Cat. 7) cables (see Fig. 2 and Fig. 3).

4. EXPERIMENTAL SETUP

In this work, we attack the wire link between two Ethernet participants that are connected via twisted-pair cables according to different shielding standards. The setup is il-

lustrated in Fig. 1 and 2. The two participants under test are Ethernet nodes A and B. To coordinate our experiments and to evaluate eavesdropped frames, we used a notebook that is connected to a USRP X300, which is a SDR with sampling rates of up to 200 M Samples per second. That is sufficient for 10BASE-T but not for 100BASE-TX and 1000BASE-T.

To capture emissions of a cable without damaging it, we tried wide-band antennas for electromagnetic compatibility (EMC) measurements, magnetic-loop antennas, as well as magnetic near-field probes[1]. We evaluated the ability to capture signals with a spectrum analyzer and realized that only the near-field probes were able to capture enough signal power for further analysis. Even though 100BASE-TX and 1000BASE-T signals were observable the bandwidth limitation of 50 MHz of our near-field probes were not sufficient to capture with 125 MHz bandwidth required for faster standards. Due to these hardware restraints, we focus our analysis in this work on 10BASE-T and leave faster standards for future work.

5. IMPLEMENTATION

In this section, we describe the implementation of the eavesdropper for 10BASE-T signals. The same components are required 100BASE-TX but with higher bandwidth requirements. For 1000BASE-T four receive paths are needed to separate the signals that are simultaneously transmitted over four wire pairs. This system is comparable to a 4×4-MIMO system in wireless communications. Focusing on 10BASE-T, we decided to use a USRP X300 with BasicRX daughterboard that allows direct sampling of received signals. We use the USRP's digital down-converter to convert the received Ethernet signal into a complex baseband signal, which we process in GNU Radio on a notebook, as illustrated in Fig. 4. Here our *Ethernet Decoder Sink* is used to decode Ethernet signals and store the result in pcap files or forward them to Wireshark.

An exemplary frame capture is illustrated in Fig. 6 with a clearly visible preamble at the left, followed by the start frame delimiter (SFD), which marks the beginning of the Medium Access Control (MAC) header. Our decoder performs an energy detection to find the start of a frame. To reduce noise during idle periods, a squelch block is used. As soon as a frame is recognized, we count samples above and below a given threshold and thereby detect the preamble bits. Counting samples allows us to automatically extract the clock signal so that our decoder works independent of the sampling frequency, which equals 20 MHz in our setup with a down-conversion center frequency of 10 MHz. The preamble detection runs, until the SFD is found indicating the start of a frame. The frame bits are decoded according to the extracted clock signal.

6. EVALUATION

In the following, we present the challenges of our analysis, the preparation of the experiments as well as a performance evaluation. The main challenge of eavesdropping Ethernet frames without damaging the cable is the low amount of longitudinal conversion loss, that converts differential-mode

[1]As H-probe, we use the Langer EMV low-frequency magnetic near-field probe LFU5 together with a 30 dB preamplifier Langer EMV PA303.

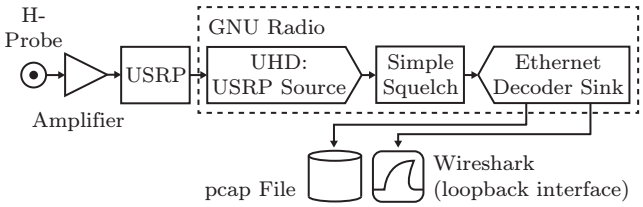


Figure 4: Diagram illustrating our eavesdropper implementation. The USRP captures signals from a probe and passes them to a computer to extract the transmitted frames.

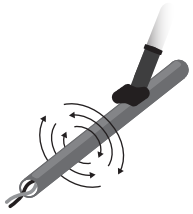


Figure 5: Near Field/H-Probe used to capture the radiated electromagnetic fields around an Ethernet cable.

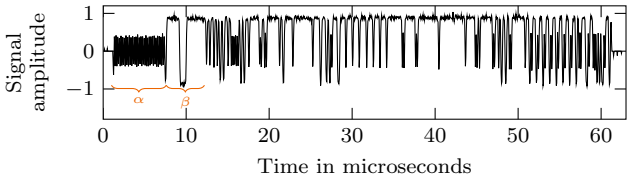


Figure 6: Received frame after down-conversion with $f_c = 10$ MHz. The preamble with SFD is clearly visible on the left (α), followed by the MAC address 00:00:FF:00:00:00 (β).

signals into common-mode signals. The more precise and uniform the twisting of the wires, the less signals can be captured. If shielding is used, less signal power can be collected by an antenna or near-field probe to perform a successful attack, which limits the distance between attacker and cable.

In all of our experiments, we evaluated cables with different shielding, as described in Sec. 3.3, namely: U/UTP, F/UTP, SF/UTP, U/FTP and S/FTP cables. As most of these cables are installation cables, we took 25 meters of each of them and attached both ends to a patch panel. Each end of a cable under test is connected to a computer using an S/FTP patch cable, as illustrated in Fig. 1. On each of the cables under test, we placed an H-probe, as illustrated in Fig. 2. An optimal placement of the probe matters, as the radiated fields are small and only receivable in the near vicinity of a cable, which means between zero to two centimeters away from the cable. This constraint has the upside of being able to eavesdrop on a cable bundle by precisely selecting which cable or even wire-pair to listen to. For example, we observed that optimizing the probe placement to receive signals from one node leads to a significant reduction in signal energy from the other node, that uses different wire-pairs to transmit. Hence, we suggest using two probes to allow individual optimizations for full-duplex eavesdropping. In addition, this result shows that it is possible to differentiate between emissions of different wire-pairs, which is the foundation of eavesdropping on 1000BASE-T that si-

multaneously uses four wire-pairs. In another experiment, we moved the probe along the cable, but the measurements showed no crucial variations in receivable signal energy.

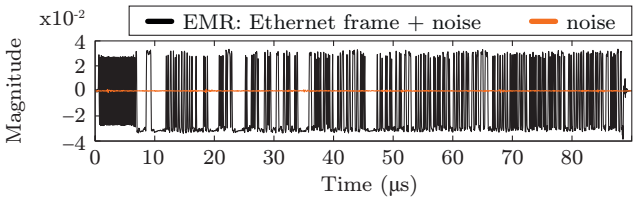
A much greater effect on the eavesdropping performance has the shielding of the cables. In Fig. 7 and 8 we, hence, focus on the measurement of the signal-plus-noise-to-noise ratio ((S+N)/NR) for different cable types. The results in Fig. 8 are based on the analysis of 700 Ethernet frame transmissions with random payload. We choose to use the (S+N)/NR as the received frames are always superpositioned by noise. To get (S+N)/NR measurements, we took the average power during a frame transmission and divided it by the average power of a long noise sample which did not contain any Ethernet signal transmission.

7. DISCUSSION

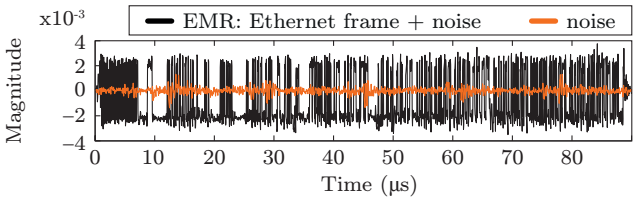
In this section, we interpret the measurements and discuss their influence on our eavesdropping results, also with regard to 100BASE-TX and 1000BASE-T. As illustrated in Fig. 8, the (S+N)/NR of completely unshielded cables (U/UTP) is very high (roughly 40 dB) and allows frame decodings with low error rates (see Fig. 8). Fig. 7a shows the recording of a Manchester signal (10BASE-T). The noise margin is sufficiently high, that even decoding MLT-3 (100BASE-TX) or PAM-5 (1000BASE-T) should lead to low error rates. Cables with only shielding around each twisted pair (U/FTP), as well as, those cables with only shielding around all twisted pairs have a medium (S+N)/NR of roughly 20 dB. Nevertheless, it is sufficient to receive more than 60 percent of 10BASE-T frames without any bit errors (valid FCS). The strongest shielded cable contains a foil shield around each twisted pair, as well as, an additional braid shield around all pairs (S/FTP). This combination reduces the (S+N)/NR to under 10 dB, which makes it hard to even correctly differentiate a frame transmission from noise.

In the following we focus on the types of errors that occurred. Instead of considering bit error rates, we evaluated if our receiver implementation can (a) correctly detect a frame, and (b) extract the frame without any bit errors, which was checked by validating the frame check sum (FCS). The results are presented in Fig. 9. The trend of increasing reception errors at cables with more shielding is clearly observable. While our implementation reliably detects the existence of all frames on the wire for U/UTP, U/FTP, F/UTP and SF/UTP cables, only half of the transmitted frames are detected on S/FTP. Regarding error-less frame decodings, for U/UTP cables, more than 70 percent of the transmitted frames are received without errors. This rate drops down to roughly 50 percent on SF/UTP cables and vanishes for S/FTP cables. We already predicted the result of the latter by analyzing the (S+N)/NRs above and considered it unlikely to decode those Ethernet frames without any error due to the high amount of noise power compared to the available signal power.

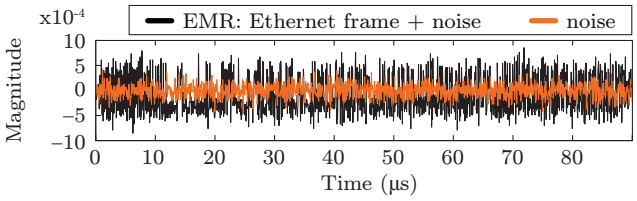
We additionally evaluated the different reasons for unsuccessful frame decodings and illustrate the results in Fig. 10. Here, we consider three types of errors (a) invalid frames, (b) undetected SFD, and (c) undetected frames. *Invalid frames* contain frames that were correctly detected but decoded with bit errors. This is the main error reason for cables having up to SF/UTP shielding. This error rate increases for heavier shielded cables. In the case of S/FTP cables, it is also responsible for more than 60 percent of the



(a) U/UTP cable with an (S+N)/NR of 41.45 dB



(b) F/UTP cable with an (S+N)/NR of 18.80 dB



(c) S/FTP cable with an (S+N)/NR of 8.89 dB

Figure 7: Observed waveforms of the same Ethernet frame and noise. Due to shielding, the signal amplitude reduces which results in decreased signal-to-noise ratios.

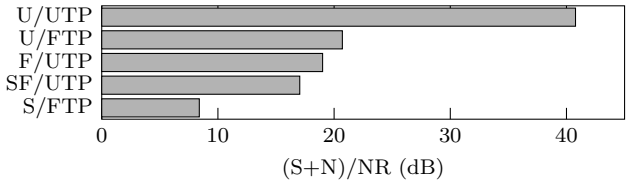


Figure 8: Comparison of the (S+N)/NRs of different twisted-pair cable types

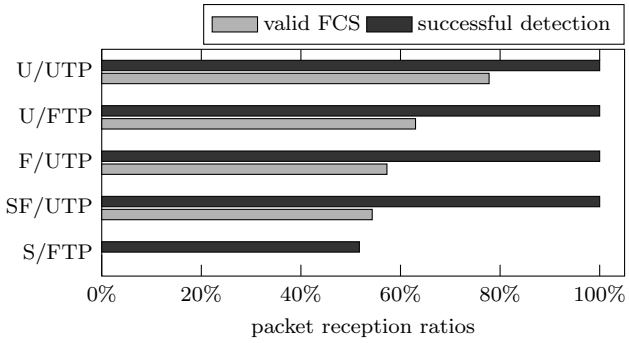


Figure 9: Ratios describing how many packets were correctly detected and how many were decoded with a correct FCS.

frame errors that are not caused by *undetected frames*, which did not trigger the energy detector. The remaining reasons for errors in the case of S/FTP cables are *undetected start frame delimiters*. Those errors occur, if a frame is detected,

but no SFD is found. Those errors are negligible for the less shielded cables.

Concluding the discussion, we demonstrated that it is indeed possible to launch a non-destructive attack on Ethernet transmissions by simply attaching a wireless H-field probe to the outside of an Ethernet cable. Especially unshielded cables are very vulnerable to this attack, but also the U/FTP, F/UTP, and SF/UTP cables allow to achieve error-less frame decodings of at least half of the frames transmitted. Only S/FTP cables helped to avoid the error-free decoding with out implementation. Nevertheless, even though error-free receptions might not be possible, one can at least use our eavesdropper to decode frames with certain bit error rates and thereby extract partially correct information.

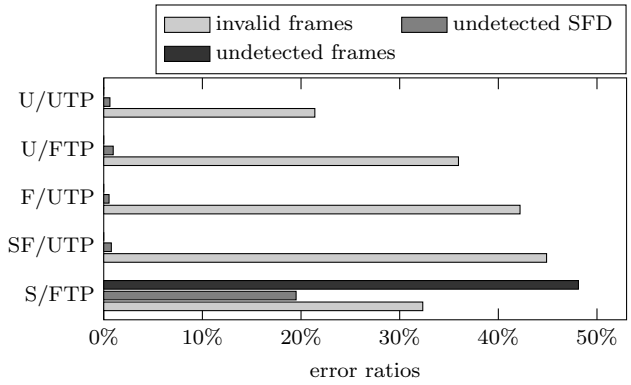


Figure 10: Reasons for unsuccessful frame detections for different cable types.

8. COUNTERMEASURES

As the eavesdropping attack described above is concerning, in this section we present possible countermeasures. The only way to avoid an eavesdropper from getting direct access to the exchanged plaintext information is to use encryption. End-to-end encryption between two communicating end points would be optimal, however, not all applications support it. IPSec in transport mode and encapsulating security payload (ESP) could address this problem by providing end-to-end encryption. However, it comes with a high management overhead, particularly if used across security domains. A more suitable solution to avoid eavesdropping would be link-layer encryption, that is transparent to upper layer protocols in all Ethernet installations. 802.1AE or MACsec is a standard that provides confidentiality and integrity on the link layer, which helps to avoid eavesdropping attacks on the payload. Nevertheless, MAC addresses of the communicating stations are still exchanged in plaintext, so that attackers can create statistics about who communicates with whom in a local network.

One way to reduce the risk of eavesdropping is to use network cables with a maximum amount of shielding in the whole network, for example, Cat. 7 S/FTP cables. However, these cost roughly 2.4 times more[2] than simple Cat. 5e U/UTP cables. Due to budget limitations the latter one might be preferable, even though it lowers the security of the whole network installation by allowing eavesdropping attacks.

An additional defense against eavesdropping is the introduction of a "masking" signal (following the terminology of the TEMPEST paper [1]). Using this additional signal, one can hide the existence of an information signal. On Ethernet's physical layer, only differential-mode signals carry information that are evaluated by a receiver. Solely due to the longitudinal conversion loss that converts differential-mode to common-mode signals, Ethernet frames are radiated and can be received with a wireless device. To mask the radiation, one could inject random common-mode signals with a spectral mask of Ethernet signals. An eavesdropper would fail to extract the actual data frames if their power is sufficiently lower than the "masking" signal. Though possible, the radiation of a masking signal might not comply with electromagnetic compatibility requirements.

[2]Based on the price of 49.99 EUR/100 m of Cat. 7 S/FTP and 20.69 EUR/100 m of Cat. 5e U/UTP cables.

9. RELATED WORK

This work mainly relates to research in the domain of wireless eavesdropping and side-channels, the radiation characteristics of twisted pair cables and countermeasures against presented attacks. In the following we give an overview of those domains. TEMPEST attacks in our field of interest rely on electromagnetic emanations that leak confidential information to an eavesdropper. Those attacks were implemented for many different categories of devices. In the area of attacks against displays Van Eck uses cathode ray tube (CRT) radiations to reproduce screen content in [20]. This attack is extended by Kuhn by intercepting emitted light in [13]. He also investigated the security of flat-panel displays in [11]. Hayashi et al. present an approach to reconstruct display images of tablets using SDRs in [9]. Besides displays, various wired devices are attackable. The security of RS-232 cable radiations, for example, is investigated by Peter Smulders in [15]. Vuagnoux et al. attack wired and wireless keyboards in [21]. Another prominent area for TEMPEST attacks are power lines. In [4], Degauque et al. demonstrate that unintentional power line radiations can be eavesdropped to listen to communication systems. Electromagnetic interference (EMI) of television sets also leaks information about their display content according to Enev et al. [5]. Signature based EMI attacks are described in [8] by Gulati et al. who also use SDRs. Especially for side-channel attacks against cryptosystems, electromagnetic emanations can be used to extract RSA keys according to Genkin et al. [6]. Enforced emanations through memory access patterns are also usable for data exfiltration as presented by Zajić et al. in [22].

Very relevant for this work are analyses of twisted-pair cable based systems. According to Murai et al. twisted-pair cables in an imbalanced system radiate electromagnetic fields [14]. In [16], Stolle analyzes the electromagnetic coupling of twisted-pair cables. Grassi et al. make differential-mode to common-mode conversions responsible for electromagnetic radiations [7].

Besides attacks, also countermeasures against TEMPEST are presented in the literature. While Van Eck relies on metal shielding in [20], Hayashi et al. propose transparent conductive shielding films to protect tablet computers [9]. An evaluation of conventional countermeasures is given by Suzuki et al. in [17, 19, 18]. Kuhn et al. reduce monitor emanations using software-based techniques [12, 2].

10. CONCLUSION

As a wired system, Ethernet is often considered immune to attackers operating wireless and eavesdropping network traffic is only possible by attaching a probe to the wires of a cable or a connector. In this paper, we have shown that this assumption is not correct and eavesdropping traffic is possible without leaving any traces on the cable for 10BASE-T Ethernet. We have also shown that this attack will likely also succeed for 100BASE-TX Ethernet and possibly also for faster modes of operations. The success rate of the attack depends on the shielding of the cable. Cat.7 S/FTP provides good protection against eavesdropping while all weaker shielding such as Cat.5e SF/UTP, Cat.5e F/UTP, Cat.7 U/FTP and Cat.5e U/UTP result in a higher success rate. To provide an adequate protection against such adversaries, better shielded cables should be deployed and whenever possible, link layer encryption should be used. Just protecting the physical access to network cables such as locking them in a cabinet or in a small plastic conduit without shielding is not sufficient.

11. 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.

12. REFERENCES

[1] TEMPEST: A signal problem.

[2] R. Anderson and M. Kuhn. Soft Tempest - An Opportunity for NATO, 1999.

[3] I. E. Commission et al. IEC 61158: Digital data communications for measurement and control-Fieldbus for use in industrial control systems, 2003.

[4] P. Degauque, P. Laly, V. Degardin, and M. Lienard. Power line communication and compromising radiated emission. In *Proceedings of the International Conference on Software, Telecommunications and Computer Networks – SoftCOM'10*, pages 88–91, 2010.

[5] M. Enev, S. Gupta, T. Kohno, and S. N. Patel. Televisions, Video Privacy, and Powerline Electromagnetic Interference. In *Proceedings of the 18th ACM Conference on Computer and Communications Security – CCS'11*, pages 537–550, 2011.

[6] D. Genkin, L. Pachmanov, I. Pipman, and E. Tromer. Stealing Keys from PCs using a Radio: Cheap Electromagnetic Attacks on Windowed Exponentiation. In *Proceedings of the Cryptographic Hardware and Embedded Systems Workshop – CHES'15*, pages 207–228, 2015.

[7] F. Grassi, G. Spadacini, and S. Pignari. The Concept of Weak Imbalance and Its Role in the Emissions and Immunity of Differential Lines. *IEEE Transactions on Electromagnetic Compatibility*, 55:1346–1349, 2013.

[8] M. Gulati, S. Ram, and A. Singh. An in Depth Study into Using EMI Signatures for Appliance Identification. In *Proceedings of the 1st ACM Conference on Embedded Systems for Energy-Efficient Buildings – BuildSys'14*, pages 70–79, 2014.

[9] Y. Hayashi, N. Homma, M. Miura, T. Aoki, and H. Sone. A Threat for Tablet PCs in Public Space: Remote Visualization of Screen Images Using EM Emanation. In *Proceedings of the 21st ACM SIGSAC Conference on Computer and Communications Security – CCS'14*, pages 954–965, 2014.

[10] IEC. Information technology – generic cabling for customer premises, Sep 2002.

[11] M. Kuhn. Electromagnetic Eavesdropping Risks of Flat-panel Displays. In *Proceedings of the 4th International Conference on Privacy Enhancing Technologies – PETS'04*, pages 88–107, 2005.

[12] M. Kuhn and R. Anderson. Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations. In *Proceedings of the 2nd Information Hiding Workshop – IHW'98*, pages 124–142, 1998.

[13] M. G. Kuhn. Optical time-domain eavesdropping risks of CRT displays. In *Proceedings of the 23rd IEEE Symposium on Security and Privacy – IEEE S&P'02*, pages 3–18, 2002.

[14] K. Murai, N. Hasebe, and I. Yokoyama. Analysis of the induced voltage on a twisted pair cable in an electromagnetic field. *Electronics and Communications in Japan*, 82:32–44, 1999.

[15] P. Smulders. The Threat of Information Theft by Reception of Electromagnetic Radiation from RS-232 Cables. *Computer Security*, 9:53–58, 1990.

[16] R. Stolle. Electromagnetic coupling of twisted pair cables. *Selected Areas in Communications, IEEE Journal on*, 20(5):883–892, 2002.

[17] Y. Suzuki and Y. Akiyama. Jamming technique to prevent information leakage caused by unintentional emissions of PC video signals. In *Proceedings of the IEEE International Symposium on Electromagnetic Compatibility – IEEE EMC'10*, pages 132–137, 2010.

[18] Y. Suzuki, M. Masugi, H. Yamane, and K. Tajima. Countermeasure Technique for Preventing Information Leakage Caused by Unintentional PC Display Emanations. In *Proceedings of the IEEE International Symposium on Electromagnetic Compatibility – IEEE EMC'09*, pages 9–12, 2009.

[19] Y. Suzuki†, M. Masugi, K. Tajima, and H. Yamane. Countermeasures to Prevent Eavesdropping on Unintentional Emanations from Personal Computers. *NTT Technical Review*, 6, 2008.

[20] W. van Eck. Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk? *Computer Security*, 4:269–286, 1985.

[21] M. Vuagnoux and S. Pasini. Compromising Electromagnetic Emanations of Wired and Wireless Keyboards. In *Proceedings of the 18th Conference on USENIX Security Symposium – USENIX SSYM'09*, pages 1–16, 2009.

[22] A. Zajic and M. Prvulovic. Experimental Demonstration of Electromagnetic Information Leakage From Modern Processor-Memory Systems. *IEEE Transactions on Electromagnetic Compatibility*, 56:885–893, 2014.