Approaches to establish a classification and comparison of wireless side-channel attacks

Timo Thräm
Technische Universität Darmstadt
Darmstadt, Germany
timo.thraem@stud.tu-darmstadt.de

***Abstract*— Different side-channel attacks examined in the last years are incomparable until now. In this work different approaches are treated to close this gap and invent an objective metric to compare different side-channel attacks. Side-channels are information transmitting channels which result from unintended side effect during processing or I/O operations. Three different approaches were taken to compare wireless side-channel attacks: First a cost-benefit analysis, second by analyzing the effort of different attacks targeting the same information and third a risk analysis based on ISO27001.**

I. Introduction

Side-channel attacks exploit data leakages via channels, which are not intended to transport information. By attacking a target computer a large variety of side-channels can be made use of. Attack vectors used in side-channels are widespread. Such side-channels can be temperature, EM emission, noise, reflection, power consumption and time, just to name a few. Not only the attack vectors differ but also the different levels of leaked data. Some attacks target user interfaces, some attack error messages and others attack hardware issues e.g. cache based side-channel attacks. This work focuses on wireless side-channel attacks.

Already used for decades by intelligence agencies side-channel attacks have been shown to be a good technique to gather secured information without access privileges. In today's world side-channels are not only important for intelligence agencies to gather information and avoid being spied on but even for business espionage. Depending on the side-channel and the used attack technique no evidence is left behind. This paper focuses on wireless side cannels in order to compare the different attack vectors and techniques. The comparison in this paper is based on papers in which different wireless side-channel attacks are researched. Before side-channels can be considered more in detail a distinction of side-channel attacks, especially wireless side-channel attacks, and related topics must be made to create an equal baseline.

Related to the side-channel attacks there are covert channels, which can be used to gather information from a target system. The major difference between covert channel and side-channel attacks is that in covert channels malicious software is installed on the target device with the purpose of leaking information.[7] In side-channels the leaked information is not intended to be leaked by the system (software or hardware) leaking it. Side-channel attack is an umbrella term for information leakage via unintended channels. In this paper we focus on wireless side-channel attacks. Wireless side-channel attacks are a special category of side-channel attacks. They exploit emissions from the target system. Due to the exploitation of the emissions a main characteristic of wireless side-channel attacks is that the attacker must be located near the target or even have physical access to the machine.

A. Related Work

Side-channel emanations are already investigated on by militaries since World War 1 [14]. The first use of electromagnetic emanation was in 1962, when the Japanese spied on american crypto systems [12]. This information has been declassified. In 1985 the first publications concerning side-channel attacks were published. The electromagnetic emanations of monitors were exploited. Since then, a large number of different side-channel attacks was published and the number of attack vectors has grown. A lot of papers focus on extracting cryptographic keys from systems during decryption [1]. Most attacked cryptosystems are asymmetric systems like RSA and Elliptic Curve Cryptography. These systems are considered secure but their implementations are vulnerable to side-channel attacks [1] [8]. Not only computers can be attacked with side-channel attacks, but also printers emanate compromising acoustic signals [6]. Side-channels like light reflections can be used to compromise information. Brumley et al. [15] studied server error messages and were able to recover passwords from the delay time of the error messages. By analyzing the cache behavior Yarom et al. [3] were able to extract information about the proceeded data. Agrawal et al. [5] studied the electromagnetic emanation of smartcards and were able to extract cryptographic information from smartcards with closed source and open source implementations. With recorded signals of acoustic emanation of keyboards Berger et al. [4] were able to reproduce or reconstruct the typed word with a success rate of 73%. This work does not examine all attacks listed in the related work chapter. The selected attacks, thematized in this work, are chosen due to the vectors and the description in the original work.

B. Reasons for side-channel leakages

The information leakage is most often a side effect of data processing. Side-channels arise from unintended behavior of hardware or software or errors with too much information content during data processing. The goal of the side-channel attacks is to extract information about the processed data from that unintended behavior. Most side-channels are no result of bad implementations, most stem from conditions the developer of the leaking process respectively component cannot affect or a mixture of both. During the development of components, even one with focus on security and privacy, side-channels cannot always be considered or covered in total. Side-channel leakage often arises from interactions between hardware and software. In some cases e.g. the padding oracle attack [15] the leakage is caused by error messages respectively the response time. In the case of the padding oracle one can debate whether it is a side-channel or not due to the fact that the response is intended to be sent. For the reason, that the information leakage in the time based padding oracle attack is the time and not the response itself this leakage is considered as a side-channel but not a wireless side-channel attack.

C. Wireless side-channel attack vectors

As mentioned in the beginning of the introduction there is a large number of vectors and possibly some not yet discovered vectors. In this work the vector denotes the medium, entity or unit the leakage is transported by or extracted from. In the past the following vectors have been discovered: electromagnetic waves, temperature, acoustic emanation, light waves, brainwaves, time. The following vectors are treated in this work: electromagnetic waves, acoustic signals and light. The attack vectors differ in their quality, the effort for the attack itself and the effort for the pre- and post-processing. Quality in this case means how good the leaked information content can be used to conclude performed computations or proceeded information on the target machine. Furthermore the attack vectors can be categorized by their range, duration, setup complexity and goal. The goal obviously is to obtain information from a system. If, for example, the goal of an attack is to gain the user's password and you are only able to extract username of the target user your attack does not fulfill its goal. For that reason it is difficult to compare different attacks presented in publications, since most publications aim to gather different information. This work treats the goal first as intended by the authors of the analyzed papers in a second step as a fixed goal and in a third step on a meta level. Likewise the goal of different attack vectors and other characteristics of the different attacks cannot be reduced to the vector. It is possible that by making use of the same vector one attack has a maximum distance of 5 meters and another attack has a maximum distance of 30 meters. It strongly depends on the extracted information beside the vector.

D. Limits of wireless side-channel attacks

The main characteristic of wireless side-channel attacks is that wireless channels, the attack vectors, emanate the leaked information. The upper limit of each vector is its physical emission limit. As upper limit the free space attenuation can be assumed. The free space attenuation of the emission is rather a theoretical limit than a maximum limit for the side-channel attacks. Side-channel attacks performed near the theoretical upper limit seem not to result in usable leaked information because of interference, noise, blending and some more. The closer the attacker's receiver is located to the used vector's emanating source, the better the leaked signal's recording and thus information can be extracted better. It is not feasible to specify a vector specific upper limit for different emanations. The upper limit depends on the accuracy of the attack setup, the accuracy of the hardware, the attack scenario itself, the amplitude, frequency, wavelength, the implementation of the leaking process and signal strength of the emanation. However, it can be specified that the upper limit for a side-channel attack is the range, which allows the receiver to a) determine the origin of a signal and b) extract enough information from the signal to conclude information about the processed data. In some cases the determination of the origin is not limited to a single component, due to some attacks making use of combinations of multiple signals emanated by the target machine. Depending on the attack the multiple signal recording is more efficient than focusing on a single emanation signal [5]. Beside the attack vectors the budget can be seen as limiting factor. The lower the attacker's budget, the lower the computation power, manpower and the equipment quality. This leads to a less powerful wireless side-channel attack than a high budget.

This work is structured as follows: Section two treats the three approaches to compare wireless side-channel attacks. Section three describes high-level countermeasures applicable for all wireless side-channel attacks. Section four summarizes the results and gives an outlook.

II. Classification

As described above it is hard to classify or compare the different attacks or attack vectors. This section first extracts different properties, which could be used to classify different wireless side-channel attacks. In a first analysis the different attacks are compared to each other according to these properties. In a second step the attacks are analyzed with a fixed goal to provide a consistent target in order to compare the different parameters needed by the different attacks. In a third analysis the attacks are categorized according to the ISO27001. All analyses are performed from the point of view of the attacker and respectively or the victim. It is assumed that the victim is a company or an authority.

A. Properties of side-channel attacks

A classification is needed to be able to compare the different wireless side-channel attacks. Therefor properties, characteristical for side-channel attacks, are used to categorize them. To find the relevant properties the related work,

technical properties and one's own research must be considered. In the related work range, leaked information, equipment price, training phases and attack vectors are mentioned. Beside these properties it is important for a classification to know the preparation time, computation power and –time, and if a training phase is needed for each new attack. The preparation time is important in order to be able to estimate the time effort. Computation time and -power both are important to be able to estimate time respectively monetary aspects. Training phase per attack is a property, which can be measured in time or nominally. If it is measured in time it increases the effort for the attack. If it is measured nominally it is an indicator of weather the attack can be generalized or not. As a result of the property determination the following properties seem to be relevant for a classification of wireless side-channel attacks: range, leaked information (LI), preparation time (PT), equipment price (EP), computation power (CP), computation time (CT), training phase (TP), attack time (AT), attack vector (AV), training phase per attack (TPA). These properties are used to categorize the attacks. Unfortunately most of the properties cannot be determined in detail from the paper due to most paper not providing detailed information. For example, the pre- and postprocessing is not explained in detail and therefor no cost estimation for time nor money can be performed for this property.

Tab. 1 Valuation of the properties

Property				
Range	<10 cm extremely near	<30 cm near	< 5 m medium-distance	>= 5 m distance
LI	Not classified	Classified	Secret	Top secret
PT	low	medium	medium	High
EP	low	medium	medium	High
CP	low	medium	medium	High
CT	low	medium	medium	High
TP	low	medium	medium	High
AT	<10 sec (low)	<10 min (medium)	<30 min (medium-high)	>=30 min high
AV				
TPA	false			true

In a first step a soft categorization for the single properties is used. The categorization levels can be seen in table Tab1. Many papers use terms like "low cost", for the EP property, and "more expensive". These terms are adopted for the costs as "low" or "high". As illustrated in Tab. 1 if only three categories are used for the categorization the second and third category are summarized to medium. The most important category is the LI category, which consists of "not classified", "classified", "secret" and "top secret". To distinguish these classifications the view of a company is assumed. For most businesses unclassified information is content, which is publically available. If the only content leaked can also be accessed via the company's or a third parties' websites, apps, flyers etc. the attack leads only to "unclassified" information leaking. "classified" information is content, which is not publically available but available for a large group of people. Classified information is content which should not be available for people outside this group of people but if the information is known to outsiders the effect for the company is minimal to not existent. Secret information is information, which is addressed to a smaller group of people than the classified information. Information categorized as secret is sensitive for the company's success but not core information, which would cause a fatal risk for the company. For example, this information could be client data or a business prognosis. Top-secret information is information, which would pose a fatal threat to the company if an adversary gets access to that information. For example, an RSA private key, planned inventions, construction plans or unpatented inventions. From the point of view of an individual the classification differs for the reason that an individual tries to keep his private data private or only accessible to trustworthy people/companies. For example a user data leak would be top-secret information for an individual and thus be categorized as "secret". The effect that data leakage has on the public image of a company is not considered. In this work the categorization from the point of view of companies is used. Some wireless side-channel attacks leak information of all four categories. The attacks, which leak information of all categories, are listed with different LI values. The other properties are categorized according to the available information from the paper and the estimations of the authors. Tab. 2 shows the categorization of the properties. As can be seen in Tab. 2 if the same attack can be performed with different equipment and provides different results the different approaches are listed as separate attacks with different properties. The same applies for different properties. One must be aware of the fact that most attack properties are assumed, calculated or extracted from the paper, due to there being no consistent valuation standard and the used attack descriptions in the papers not being consistent.

B. Soft categorization of properties

The soft categorization is done with a Cost-Benefit Analysis (CBA) from the point of view of an attacker. The costs are preparation time, equipment price, computation power, computation time, training phase, attack time and training phase per attack. The benefit is the leaked information. The range is a factor, which modifies the costs. If wireless side-channel attack a. with a range of 100m leaks less sensitive data than wireless side-channel attack b. with a range of 20cm the wireless side-channel attack a. is less useful for the attacker. But it must be considered that an attack with a large range can be performed over a large amount of time without a high risk of being detected. In most cases the range correlates with the EP. A high-range maximizes the costs (equipment price) and a low range decreases the costs for an attacker. By weighing the range and the costs like that the pros and cons of assumptions according to the range are satisfied. As can be seen in Tab. 2 some attacks are listed several times. Once with a low range and once with a high range. In order to be able to compare the costs and the benefits the cost categorizations "low", "moderate" and "high" as well as

benefit classifications “unclassified”, “classified”, “secret” and “top-secret” must be transformed in a comparable context. Therefor a three- respectively four-step metric is used. Tab.3 shows how the different property categories are valued and Tab. 5 shows the attacks with the values for each category.

Tab. 2 Soft categorization (range, leaked information (LI), preparation time (PT), equipment price (EP), computation power (CP), computation time (CT), training phase (TP), attack time (AT), attack vector (AV), training phase per attack (TPA

Property	Range	LI	PT	EP	CP	CT	TP	AT	AV	TPA	Open Source	Device
[1]	30	RSA private Key	low	low	low	low	low	medium	acoustic	low	yes	PC
	100	RSA private Key	medium	medium	low	low	low	medium	acoustic	low	yes	PC
	400	RSA private Key	medium	medium-high	low	low	low	medium	acoustic	low	yes	PC
	10000	RSA private Key	medium	high	low	low	low	medium	acoustic	low	yes	PC
[2]	10	Every printed Text	high	medium	medium	high	high	medium	acoustic	high	no	Printer
	10	Every printed Text	high	medium	medium	medium	high	medium	acoustic	high	no	Printer
[6]	10000	Everything visible on the Screen	medium	low	low	low	low	low	light	low	no	Display
	30000	Everything visible on the Screen	medium	high	low	low	low	high	light	low	no	Display
[5]	20	RSA,DES, COMP128, tokens, SSL accelerator	medium	low	high	high	low	low	EM	low	yes/ no	Smart Cards
	457.2		medium	high	medium	medium	low	low	EM	low	yes/ no	Smart Cards
	1 219.2		medium	high	medium	medium	low	low	EM	low	yes/ no	Smart Cards

Tab. 3 Weight of the properties

Property category	Value
Low	1
Moderate/ medium	2
Medium-High	3
High	4
Unclassified	0

Classified	1
Secret	2
Top-Secret	3
Extreme-near	4
Near (<100cm)	3
Middle-distance (<5m)	2
Distance(>=5m)	1

From the view of an adversary the best attack is one with low costs and a high benefit. From the point of view of the target (system administrator, company, etc.) the costs for an attack should at least be high enough for the attack's cost to outweigh its benefits. In a first step all cost values are summed up. The sum is divided by the number of properties. This is the cost-index. The cost-index is compared to the benefit value. If the benefit value is larger than the result of the first calculation the attack is useful for the attacker. The results for each attack from Tab. 5 can be seen in Tab.4. The categories are useful when comparing the attacks visually.

1) Evaluation

In Tab. 4 the cost-indexes and the benefit values are listed. As can be seen in most cases the costs are lower than the benefit. Only in two cases the costs are higher than the benefits. The CBA clarifies that wireless side-channel attacks are viable in most cases. Especially if the benefit is high (secret or top-secret) the costs do not increase in a way that makes the benefit no longer viable. Only in one case the cost-index and the benefit value are equal. In this case it is assumed that the benefit neutralizes the costs and the attack is viable.

Tab. 4 Attack CBA

Attack	Cost-index	Benefit value
[1]	1.375	3
	1.625	3
	1.75	3
	1.625	4
[2]	3.25	1
	3	3
[6]	1.125	1
	1.875	3
[5]	2,125	3
	1.875	3
	1.75	3

Tab. 5 Property valuation (range, leaked information (LI), preparation time (PT), equipment price (EP), computation power (CP), computation time (CT), training phase (TP), attack time (AT), attack vector (AV), training phase per attack (TPA).

Property	Range	Leaked information	Preparation time	Equipment price	Computation power	Computation time	Training phase	Attack time	Training phase per attack	Open Source	Device
[1]	3	RSA private Key	1	1	1	1	1	2	1	yes	PC
	3	RSA private Key	2	2	1	1	1	2	1	yes	PC
	2	RSA private Key	2	3	1	1	1	2	1	yes	PC
	1	RSA private Key	2	4	1	1	1	2	1	yes	PC
[2]	4	Every printed Text	4	2	2	4	4	2	4	no	Printer
	4	Every printed Text	4	2	2	2	4	2	4	no	Printer
[6]	1	Everything visible on the Screen	2	1	1	1	1	1	1	no	Display
	1	Everything visible on the Screen	2	4	1	1	1	4	1	no	Display
[5]	1	RSA,DES, COMP128, tokens, SSL accelerator	2	1	4	4	1	1	1	yes/ no	Smart Cards
	2	RSA,DES, COMP128, tokens, SSL accelerator	2	4	2	2	1	1	1	yes/ no	Smart Cards
	3		2	4	2	2	1	1	1	yes/ no	Smart Cards

The issue in this analysis is, that most values are calculated and assumed. Since there is no consistent information about the costs the CBA cannot result in a meaningful result. It must be considered, that wireless side-channel attacks have different goals and are described in such an inconsistent way, that the analysis of so many properties cannot lead to a

consistent result. The used soft categories seem to be a good point to start a categorization of side-channel attacks. One of the greatest issues is the individual perspective according to the described costs. Soft words like "cheap" cannot be categorized objectively since it depends on the subsidence or the basic effort. Since the benefits and the costs are to soft a harder categorization must be considered in order to compare different attacks with different goals, assumptions, preconditions and described properties.

C. Comparison with standardized conditions

The comparison of the soft categories did not result in a valid comparable metric. Therefore a new approach is taken. To be able to compare the different attacks the leaked information must be a fix amount. Due to many attacks being focused on leaking RSA keys it is assumed that a RSA key or the content, which is protected by the RSA key, is leaked. The specific scenario is as follows:

Person A sends a secret message to Person B via e-mail. The attacker is interested in the content of the email. The email is encrypted with asymmetric cryptography (RSA). Person B, who receives the email, has a teapot on the desk which reflects the victims screen. The receiver prints all emails after he received them. The attack model is an extended Dolev-Yao-Model. In addition to the Dolev-Yao-Model the attacker gets access to the building person A's and person B' workstations are located in. The attacker knows when the message is send, printed, read and the decryption is performed via smartcard.

Another way to standardize the leaked information would be to value the information content with the corresponding bit values. Such an evaluation would lead to an objective evaluation but does not regard the impact variety of the different leaked information.

The chosen scenario, even if a lot of assumptions are met, theoretically allows us to compare the attacks from [1][2][6][5] in a standardized way. The information content must not be classified and is identical for all attacks. It is content classified as "top-secret". To be able to compare the cost categories it is not sufficient to assume the labels used in the corresponding work by the authors or to use a soft categorization. Beside the fixed scenario described above hard properties must be used to classify the attacks. All properties, which are not measureable cannot be compared in a meaningful way. Therefore, assumptions must be made to minimize or eliminate the non-measurable properties. The range is already a hard category and can be measured in meters. By assuming the attacker to have unlimited computation and monetary resources the equipment price, computation power and the computation time can be neglected. The training phase can be seen as a subcategory of the preparation time, due to the training that needs to be finished before the attack is performed. The preparation time is difficult to estimate because depending on the distance to the target, the used equipment and the training phase, the preparation time differs from attack to attack. Therefore it is assumed that preparation is a prerequisite for a successful attack. Placing receivers (probes) and adjusting them is included in the training and thus preparation. After these assumptions are made the different attacks can be compared according to the attack time (AT), attack vector (AV), training phase per attack (TPA) and range. Even though the training phase per attack is a factor that should be measured in time a nominal measurement is chosen to reduce estimation complexity. The training phase per attack is true if the algorithm, extracting information, must be trained for each target setup. For example: If the recorded signal differs from machine to machine in a way, that the extraction algorithm must be explicitly trained for each machine the training phase per attack is true. If the algorithm can determine the differences without a dedicated training phase within the first five minutes of the attack, the training phase per attack is false. In some cases humans must assist the analysis of the recorded signal. This is not listed separately since it increases the attack time. The attack time is split into the recording time and the post processing time. Due to the risks involved in recording being higher than the risks during post-processing-time, the recording time should be increased by a prefactor greater than 1. Even though evidence could still be recovered by the victims during post-processing time, as used equipment may still need to be removed, the prefactor is omitted. Tab.6 shows the comparison with the new assumptions in the defined attack scenario. The attacks leaking the RSA key can eavesdrop on the mail and decrypt it. The time for eavesdropping and decrypting the message is neglected. So all attacks leak the same information. In contrary to the estimation with soft categories the results cannot be compared with a simple cost-benefit analysis. The benefit of all attacks is the same leaked information. Only the costs (TPA, Range, AT) differ. A benefit of the RSA key extracting attacks is that all intercepted mails can be decrypted or the target can be impersonated (if the same key used for decrypting is used for signing). A benefit of the printer and screen reading attack is that the attacks can extract information which is not sent via mail. All attacks are useful to extract the information.

1) Range

First we focused on the range. Fortunately the range is specified in cm, m or feet in the papers [1][2][6][5]. So no estimation must be made to get the range. The range varies from one wavelength [5] respectively 10 cm up to 30 meters with decreasing quality. As mentioned in the introduction the best results are achieved the closer the recording is performed. Due to no equipment price being analyzed in this section the costs for higher ranges are not considered. Regardless of money required, the attack with the highest range [6] (30 meter) results in less quality because the email can be read only partially. The same problem occurs for [2] in which the printed mail is only reconstructable in parts. Of course the RSA extracting attacks [1] [5] are at an advantage, because their intention is to leak an RSA key and the attacks, which leak the content, are more general. Some attacks only being capable of leaking information partly are ignored in this work and it is assumed that the attack could leak the whole information.

2) Attack time

Now we focus on the attack time. The attack time differs from 2 up to 60 minutes. The attack times for [2][6] are estimated. The estimation of attack times can be done very accurately for these two attacks. In the acoustic attack against printers the time needed to perform the attack is the time needed to print the text. A dot-matrix printer with 48 needles can achieve up to 1000 characters per second. Most common 9 to 12 needle printers are used which print at about 200 characters per second. A printed normpage (a German standard called "Normseite") has 1800 characters per page. A document with 5 pages has 1800 * 5 = 9000 characters. This is 45 seconds needed to print 5 pages. Assuming the printer needs acceleration time a maximum of 2 minutes is assumed. The attack described by [6] is based on the time the receiver needs to read the text. One character has an information content of 4.7 to 5 bit. The average read time of a German adult is 15bit/s. An average adult needs 9000/15 = 600 seconds to read a 5-page text. The attack time for [5] is assumed according to [1]. In [5] no information according to the attack time is provided. It is assumed that the key can only be extracted bitwise. A 4096 key bit would thus take up to 60 minutes (with a small postprocessing phase [1]).

3) Training phase per attack

Only in the attack against printers a training phase per attack is needed. This is caused by the individual acoustic emanation of each printer. For each printer a dedicated training phase is needed. The training phase per attack is a disadvantage of the attack but the attack against printers is also the attack with the lowest attack time. Due to the nominal scale being chosen, the attack time cannot be integrated in the TPA. According to the description of the attack it is assumed that the TPA is at least 60 minutes.

Tab. 6 Standardized comparison of the attacks

Property	Range	LI	AT	AV	TPA
[1]	30	RSA private Key	60	acoustic	false
	100	RSA private Key	60	acoustic	false
	400	RSA private Key	60	acoustic	false
	10000	RSA private Key	60	acoustic	false
[2]	10	Printed mail	2	acoustic	true
	10	Printed mail / in parts	2	acoustic	true
[6]	10000	Mail on the screen	10+	light	false
	30000	Mail on the screen (in parts)	10+	light	false
[5]	20	RSA private Key	60	EM	false
	457,2	RSA private Key	60	EM	false
	1219,2	RSA private Key	60	EM	false

4) Summary

The categorization of the attacks in a standardized scenario results in a more objective comparison with less estimation. As can be seen in Tab. 6 the 4 considered attacks differ mainly in range and/ or attack time. Beside the attack on printers [2] all attacks need no training phase per attack. A ranking of the attacks according to this approach cannot result in a valid ranking of the attacks. By abstracting so many aspects respectively properties of the attacks the comparison does not result in an utilizable categorization. The range, attack time and training phase per attack are important properties for a classification but by only considering these properties and ignoring the other properties the validity of classification comes into question. It seems to be quite difficult to compare such individual attacks to each other according to the defined properties that another approach must be taken.

D. The risk of wireless side-channel attacks

By analyzing the attacks themselves it is difficult to find a satisfying metric to classify the different attacks. ISO27001 is used as a way to classify the attacks in this subsection. ISO27001 is a baseline for companies, authorities and governments (from now on only the term "company" is used as synonym for all three) to protect their digital assets. ISO27001 considers the company at large.

The weakness and the vulnerability are the same for all side-channel attacks: emanation and confidentiality. The threat and the risk strongly correlate to the information which is leaked and the range of the attack. Remember, the threat is the extraction of confidential information. The risk is the potential occurring of the threat. [10]

By abstracting the different attacks from the detailed properties to a more high-level view it might be feasible to compare them in a more utilizable way. To be able to specify the threat and risk the parameters must be set. Threats are potential attacks using single or multiple vulnerabilities with the goal of endangering protected goals. Risks are the probability of a threat's occurrence and the consequences. The approach documented in ISO27001 considers the whole company and not only the IT infrastructure. For the categorization of side-channel attacks this approach seems to be the best due to wireless side-channel attacks making use of the whole environmental area and not only of the IT-infrastructure. By considering the whole environment of the company the main goal is minimizing the risks by maximizing the security arrangements. Each attack can be seen as a risk. But risks are measured as the product of the probability of occurrence (P) and damage (D).

By assuming the attack scenario of "C" the damage is that a secret email can be read by unauthorized people. The probability of occurrence differs even with the assumptions met in C. In addition to the conditions met in C it is assumed that the costs rise with larger distance. In contrast to the soft categorization the costs are not fine grained into different properties but just increase with the distance. One main part of ISO27001 is that the company complexes (building, campus) must be secured. It is assumed that the access to the building, where the email sender and receiver are located is secured with employee access control. This maximizes the risk for the attacker to be detected when using attacks with low range. Assuming this, the attack's goal must be worth the risk of being detected or the costs for a higher range. For a better

distinction the risk for the attacker is from now on denoted as a-risk. Preparation and preparation time are further property, which can be linked to the distance and the risk of being detected. If an attack with a low range is performed the signal receiver must be arranged near the target e.g. in the building. This increases the risk of being detected and the time to prepare the attack. If an attack with a large range is performed the preparation time increases because the setup must be adjusted more precisely onto the target. Depending on the target location the attacker must use an attack with a high range but be located in the secured building, for example if the target is located in the middle of the building and the attack cannot be performed from the outside. This case is not considered. The training phase per attack is attack specific. If an attack with a training phase is chosen the costs for the attack are higher. Therefore the training phase can be linked to the costs. A training phase increases the baseline of the attack costs. The optimum attack from the view of an attacker is an attack with maximal moderate costs and maximal moderate a-risk to be detected. From the point of view of the company the risk to be detected by a low range attack must be high enough so no attacker tries to infiltrate the company and the cost for a high range attack must be high enough so it is not worth it or the leaked information from a high range attack is worthless. Fig. 1 illustrates the relation between accuracy, a-risk, cost and distance. The costs are preparation time, manpower and monetary expenditures. According to Fig. 1 the company's goal is to keep the attacker as far away as possible from the building. Companies cannot affect the whole environment around the buildings. Cars near the building or other offices located near by are out of their leverage. From their exterior wall the company can assume a maximum of 5 meters as effectible. All attacks with a range higher than 6 meters (5 meters + 1 meter for the target's workplace) are uncontrollable by the company. More than half of the listed attacks have a range less than 6 meters. So the companies minimize the risk of being attacked via wireless side-channel attacks by more than 63% with physical access control. Alongside the minimization of the risk the distance is increased which causes a higher cost and lower accuracy for the attacker. By increasing the distance to the target machine the eavesdropping needed to acquire the RSA key becomes more difficult as well. The high-level security approach is based on risk assessment. Depending on the assessment a risk minimization of 63% is enough. In Fig. 1 a grid is drawn. The grid illustrates the different classes of wireless side-channel attacks, which can be performed according to the distance. If a high accuracy is needed e.g. minimum 8 the risk to be detected must be high (min. 8) but the costs are low (max. 2) and the distance is low (max. 2).

If a basic security guideline according to the ISO27001 is implemented and physical access control is used the maximum accuracy which can be reached is 4 with a risk of 4, costs of 6 and a distance of 4. The simple ten-step-scale allows classifying the impact one of the listed properties has on the other properties. Even if this does not suit all attacks, it is still a good way to categorize different attacks according to the risk and threat for the company. It is important to remember that the standards set by ISO27001 do not consider single attacks. ISO27001 categorizes attacks according to the threat and risk and helps implementing countermeasures against attack categories. In the case of wireless side-channel attacks a threshold must be defined in the ten-step-scale which can be used as an indicator for a sufficient protection against side-channel attacks. On the other hand the attacker can use the threshold to estimate the success of the attack. As described in ISO27001 there is always a so-called priori risk, which cannot be eliminated. As already mentioned the company can only affect the distance up to 5 meters. By only considering the distance as a possible prevention property the priori risk would be all attacks with a range higher than five (or six) meters. Typically a risk analysis according to [10] an attack tree is constructed. Attack trees are needed to handle risks, which occur in the second of the risk quadrants. The risk quadrants are categorized according to [11]. In quadrant one the risks with high impact and probability are located, while quadrant three holds the risks with low impact and low probability. Quadrant four represents the risks with a high probability and low impact. Quadrant two, which is the quadrant wireless side-channels attacks are located in, are risks with a high impact but a "moderate/small" probability. Quadrant two divides into two different sub categories, "fatal/frequently" and "never/significant" impact. More details can be seen in [11]. For the risk analysis it is required to have vulnerability, available exploit and a benefit as prerequisites. The vulnerability is given by the attacks, the exploit is available (even with different costs) and the benefit is the top-secret email as shown in the second analysis (C). In Fig. 2 a simplified attack tree is constructed. The attack tree only contains the risks for the four attacks studied in the first and second categorization. Unfortunately a detailed risk analysis is only meaningful if the effort (so far "costs") can be valued with costs (monetary, time) [11]. But the attack tree gives more information about the prevention of wireless side-channel attacks from a high level view. The broken lines in Fig. 2 illustrate the gaps between the different steps. Countermeasures established in the gaps can decrease or even eliminate the chance of success. Increasing the distance, as already mentioned in this section, increase the effort for the transition of the lowest level to the level above. Noise, transients and shielding increases the gap between the extraction (second from below) and reconstruction (second from the top). Shielding and noise interference already affect the preconditions needed by some attacks such as mirrored windows for the attack performed by Backes et al. [6]. The attack tree describes the different steps needed for each attack to be performed. According to the preconditions the preparation time is not considered. Weighing the different nodes with costs would result in the same issue as the cost benefit analysis. Using Fig. 1 the impact of the properties on the nodes and the gaps between the nodes can be established. Assuming all high-level countermeasures are implemented, the recording and the processing of the data can be affected. By classifying the countermeasures, the attacks can be

classified according to the countermeasures. Minimizing the accuracy for example decreases the risk of attacks. But, depending on the attack, one attack is more influenced when minimizing the accuracy than another. The attack with the highest c-risk after implementing high-level countermeasures seems to be the most effective. By decreasing the countermeasures step by step (and thereby increasing the risk) the attacks can be ranked by their start value in the ranking. In Tab. 7 such a ranking is shown. Tab. 7 considers only the distance as a countermeasure. In addition to the range such a ranking can be established for each property. These rankings can be used for risk analysis and determine which countermeasures should be taken to protect the digital assets.

Tab. 7 Ranked by distance

Attack	Distance	Rank (distance)
[6]	30000	1
[1]	10000	2
[6]	10000	2
[5]	1219,2	3
[5]	457,2	4
[1]	400	5
[1]	100	6
[1]	30	7
[5]	20	8
[2]	10	9
[2]	10	9

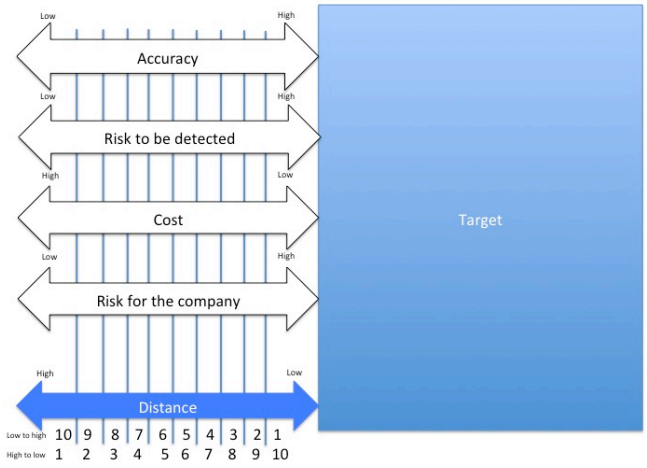

Fig. 1 Dependencies

E. Summary

Three approaches to categorize wireless side-channel attacks are presented in this section. Due to the inconsistencies of the analyzed paper's descriptions and metrics it is not possible to compare the three approaches nor to perform the categorizations in total. The CBA was unsatisfying due to the inconsistent and insufficient description of the attacks. The fixed benefit analysis resulted in a descriptive analyzable result, which must be interpreted. A desirable goal is to get hard indices to compare and categorize wireless side-channel attacks. The risk analysis is a high level approach, which results in a high level classification. Making use of the ISO27001-family made it possible to devise a categorization depending on security benchmarks e.g. distance and shielding. The CBA approach seems to result in expressive benchmarks. The properties extracted in this work can be used to prioritize and categorize wireless side-channel attacks with a CBA. As mentioned before in this section wireless side-channel attacks should use a standardized description. The properties treated in this work can be used as baseline properties for further researches.

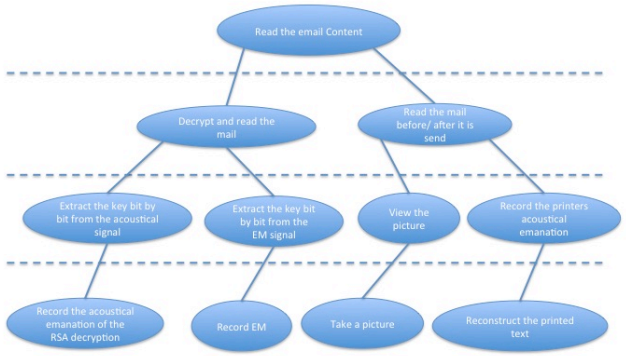

Fig. 2 Attack tree

III. Countermeasures

In most cases it is not feasible to avoid all potential wireless side-channel leakages during the development of systems. The most obvious countermeasure is to avoid all kinds of emanation. So a wireless side-channel resistant system would be located in a soundproof and emanation-preventing room with no windows, only accessible through an anteroom with two soundproof doors, an uninterceptable power and network cable. Such a setup is only feasible for military or top secret areas. Since not only authorities have to protect their information from espionage less radical countermeasures can be put into place to increase the effort and thereby minimize the risk of being the victim of a wireless side-channel attack. The ISO 27001 norm treats IT security arrangements in companies and authorities and provides us with some basic countermeasures to minimize the risk. Physical access control as described in the ISO 27001 minimizes the number of persons who can get access to the machine and thereby the number of potential attackers. Different approaches are

presented to measure the risk and effectiveness of wireless side-channel attacks. When considering specific attacks the countermeasures differ. The risk based approach shows us countermeasures on a high level such as increasing the distance or disturbing the signals. Such high level countermeasures have the advantage of preventing multiple attacks with different attack vectors by implementing them. Further in the scenario the email has to be eavesdropped on and can only be decrypted, due to the RSA key being extracted via wireless side-channel attack. The email content however is leaked through other channels, which are also covered by ISO27001.

IV. Conclusion

Side-channel attacks are risks for companies and individuals. Since the leak of NSA documents everyone should be wary of that. The impact of side-channel attacks depends on the attack properties. Different side-channel attacks assume different preconditions. This paper treats three approaches to classify and analyze wireless side-channel attacks: cost benefit analysis, fixed benefit analysis and risk analysis. The three approaches discussed in this paper do not satisfy the need for an objective categorization. Due to inconsistent information about the attacks, setup and the variety of the goals a consistent categorization is not feasible. The first approach, a cost benefit analysis, tends to be the best approach due to many properties being included. The approach treating the risks can also be utilized to classify different attacks according to their threat and the needed countermeasures. In contrast to implementing attack specific countermeasures the risk analysis based on the ISO27001 results in overarching countermeasures. By increasing the attacker's distance to the target more than 60% of attacks can be prevented. Whether it is needed to eliminate the remaining 40% risk depends on the assets supposed to be protected.

A. Further Work

The treated metrics and categorizations for wireless side-channel attacks do not satisfy in total. This work should be seen as a first approach. To be able to use the introduced metrics future work treating wireless side-channel attacks should use the properties introduced in this work to describe their attack setups. The introduced metrics are high-level and are improvable in their validity. Further work should investigate metrics more in detail.

[1] GENKIN, D., SHAMIR, A., TROMER, E., "RSA key extraction via low-bandwidth acoustic cryptanalysis" Advances in Cryptology – CRYPTO, Springer, 2014, pp. 444-461

[2] BACKES, M., DÜRMUTH, M., GERLING, S., PINKAL, M., SPORLEDER, C.: Acoustic side-channel attacks on printers. In: USENIX Security Symposium, pp. 307–322 (2010)

[3] YAROM, Y., FALKNER, K.E.: Flush+reload: a high resolution, low noise, L3 cache side-channel attack. IACR Cryptology ePrint Archive, 2013:448 (2013)

[4] BERGER, Yigael; WOOL, Avishai; YEREDOR, Arie. Dictionary attacks using keyboard acoustic emanations. In: Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006. S. 245-254.

[5] AGRAWAL, Dakshi, et al. The EM side—channel (s). In: Cryptographic Hardware and Embedded Systems-CHES 2002. Springer Berlin Heidelberg, 2003. S. 29-45.

[6] BACKES, Michael; DURMUTH, Markus; UNRUH, Dominique. Compromising reflections-or-how to read LCD monitors around the corner. In: Security and Privacy, 2008. SP 2008. IEEE Symposium on. IEEE, 2008. S. 158-169.

[7] WANG, Zhenghong; LEE, Ruby B. Covert and side channels due to processor architecture. In: Computer Security Applications Conference, 2006. ACSAC'06. 22nd Annual. IEEE, 2006. S. 473-482.

[8] BRIER, Eric; JOYE, Marc. Weierstraß elliptic curves and side-channel attacks. In: Public Key Cryptography. Springer Berlin Heidelberg, 2002. S. 335-345.

[9] RIZZO, Juliano; DUONG, Thai. Practical Padding Oracle Attacks. In: WOOT. 2010.

[10] CALDER, Alan; WATKINS, Steve G. Information Security Risk Management for ISO27001/ISO27002. It Governance Ltd, 2010.

[11] Amanaza, Attack Tree Fundamentals online at http://www.amenaza.com/downloads/docs/AttackTreeFundamentals.pdf accessed 09/01/15, 16:52.

[12] National Security Agency, TEMPEST: A signal problem, Available online at http://www.nsa.gov/public/pdf/tempest.pdf accessed 09/01/15, 16:55.

[13] HIGHLAND, Harold Joseph. Electromagnetic radiation revisited. Computers & Security, 1986, 5. Jg., Nr. 2, S. 85-93.

[14] BAUER, Arthur; Some aspects of military line communications as deployed by the german armed forces prior to 1945. In The History of Military Communications, Proc. 5th Annual Centre for the History of Defence Electronics, Bournemouth University, 1999.

[15] BRUMLEY, D., BONEH, D.: Remote timing attacks are practical. Computer Networks 48(5), 701–716 (2005)