RESEARCH ARTICLE

Considerations on Visible Light Communication security by applying the Risk Matrix methodology for risk assessment

Ignacio Marin-Garcia[1☯¤*], Patricia Chavez-Burbano[1☯¤], Victor Guerra[2☯], Jose Rabadan[2‡], Rafael Perez-Jimenez[2‡]

1 Telematics Engineering Dept. Facultad de Ingenieria en Electricidad y Computacion, Escuela Superior Politecnica del Litoral (ESPOL), Guayaquil, Ecuador, **2** Instituto para el Desarrollo Tecnológico y la Innovación en Comunicaciones (IDeTIC), Universidad de Las Palmas de Gran Canaria, Las Palmas de Gran Canaria, Las Palmas, Spain

☯ These authors contributed equally to this work.
¤ Current address: Universidad de Las Palmas de Gran Canaria, Las Palmas de Gran Canaria, Las Palmas, Spain
‡ These authors also contributed equally to this work.
* imaringa@espol.edu.ec

Abstract

Visible Light Communications (VLC) is a cutting edge technology for data communication that is being considered to be implemented in a wide range of applications such as Inter-vehicle communication or Local Area Network (LAN) communication. As a novel technology, some aspects of the implementation of VLC have not been deeply considered or tested. Among these aspects, security and its implementation may become an obstacle for VLCs broad usage. In this article, we have used the well-known Risk Matrix methodology to determine the relative risk that several common attacks have in a VLC network. Four examples: a War Driving, a Queensland alike Denial of Service, a Preshared Key Cracking, and an Evil Twin attack, illustrate the utilization of the methodology over a VLC implementation. The used attacks also covered the different areas delimited by the attack taxonomy used in this work. By defining and determining which attacks present a greater risk, the results of this work provide a lead into which areas should be invested to increase the safety of VLC networks.

OPEN ACCESS

Citation: Marin-Garcia I, Chavez-Burbano P, Guerra V, Rabadan J, Perez-Jimenez R (2017) Considerations on Visible Light Communication security by applying the Risk Matrix methodology for risk assessment. PLoS ONE 12(11): e0188759. https://doi.org/10.1371/journal.pone.0188759

Editor: Hua Wang, Victoria University, AUSTRALIA

Received: May 18, 2017

Accepted: November 11, 2017

Published: November 29, 2017

Data Availability Statement: All relevant data are within the paper and its Supporting Information files.

Funding: The author(s) received no specific funding for this work.

Competing interests: The authors have declared that no competing interests exist.

Introduction

Visible Light Communications (VLC), defined by its Institute of Electrical and Electronics Engineers (IEEE) standard [1], similar but mistakenly known as LiFi [2], is one of the newest communication technologies that may be massively used in the next few years [3]. As a broadband communication technology, VLC is expected to be part of the upcoming heterogeneous networks complementing other technologies such as five generation telephony (5G), WiFi and Ethernet [4, 5]. An axiom in network security is that a network is as secure as its weakest link. Among the highlighted strengths of this technology, security is usually listed at the top. The security attributed to VLC is generally associated with the belief of light being confined by walls. Therefore, VLC data streams cannot be easily observed from outside the rooms or premises where they are generated. However, few security studies have been done regarding the intrinsic security of VLC, and therefore a safety concern comes into our mind when implementing VLC based networks. This concern is based on the expected large amounts of data that, in the near future, will be transmitted through VLC networks [6, 7]. In addition to this, the information transmitted through VLC, as the one used on geolocation techniques [8–12], could be exploited for criminal activities, since the transmitted data could be of great interest for potential attackers. For the stated reasons, further understanding of the security limitations of VLC and its exploitation should be studied and understood for the users protection.

Regarding those reasonable concerns about security, some general research into VLC security has been conducted. Mostafa and Lampe studied the use of null-steering and artificial noise strategies to achieve positive secrecy rates against eavesdropping attacks [13]. In [14], the same authors considered using friendly jamming to secure data transmissions. In [15], Blinowski studied the risk of snooping, jamming and modifying VLC-based communications. In [16], Al-Kinani et al. evaluated the power received in a VLC system using simulations and a novel field-of-view (FOV) geometry-based single bounce (GBSB) model which results pointed out that wireless optical channel was highly correlated at the center of the environment and the correlation decreased gradually when moving towards the environment edges. In [17], Classen et al. considered the theoretical eavesdropping possibility of VLC based communications through keyholes and door gaps. In [18], a lab test of VLC sniffing using components-off-the-shelf (COTS) was performed with positive results. Finally, in [19], Prasad et al. compared Ultra-Wide-Band (UWB) and VLC for data intensive and security sensitive applications. This work concluded that VLC was a good option from a cost and interference point of view and complemented other data transfer technologies yet further work in VLC reliability and privacy was needed. All the presented works began to consider and tried to determine some security and secrecy boundaries for VLC transmissions. With the upcoming release of the revision of the standard [20] by the IEEE 802.15.7r1 Task Group, the opportunity to address security concerns present itself. By analyzing standard attacks and using standardized tools or risk assessment, adequate focus in the more insecure characteristics of VLC can be taken.

Notwithstanding a short use on [15], and a few others examples for qualitative risk assessment, Risk Matrices are not usually found in the literature to evaluate risk in wireless communication. However, this approach is widely used in multiple fields where qualitative evaluation is looked for or even required. For instance, matrices were used in [21] to assess the risk on a campus-wide network. In [22] the risk matrix approach was used in a software project risk management assessment. In [23], this methodology was used for supply chain risk assessment, while in [24], it was used to assess the risk while driving. In [25] this approach was used to evaluate the Information Technologies (IT) outsourcing risk, and in [26] it was applied to measure security risks for smartphones. All these examples are just a few of the large set of literature available works in which, for almost all areas of knowledge, Risk Matrices are used to assess hazards and determine which areas, or attacks, should be prioritized for risk mitigation.

Constructing the Risk Matrix for VLC systems

A Risk Matrix is a structured approach to the risk assessment process used in project and security management. Risk Matrices allow the identification of the potential impact and the probability of occurrence in a visual way and assist decision making. The method was proposed by the United States Air Force Electronic System Center (USAF-ESC) in 1995, ant it was included in 2000 as part of the Military Standard (MIL-STD) 882D [27]. The objective of this

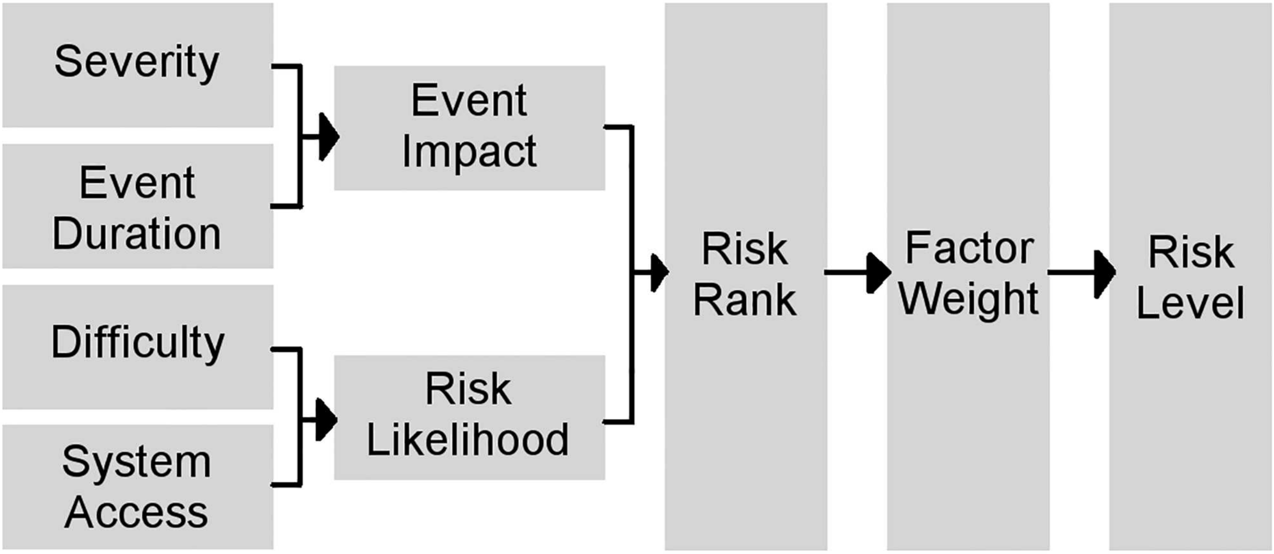


Fig 1. Risk Matrix model. The process of risk modeling starting from four initial inputs (Severity, Event Duration, Difficulty and System Access) to create a Matrix of Experts. The evaluated matrix generates the event's Impact and the Likelihood values that serve to generate the Risk Rank.

https://doi.org/10.1371/journal.pone.0188759.g001

methodology is to determine risk existence. Based on the project needs and technical possibilities, the method gives a qualitative impact level. Finally, this methodology provides a Risk Rank or risk level that allows management to focus the resources on the prevention of potentially disastrous problems rather than in low-level risk events.

In security analysis, a Risk Matrix can evaluate diverse security threats of a specific system based on different parameters as the severity, difficulty, and duration of the event and the relative access to information, not only from the attacker but also from system users. This information identifies the real impact of an attack on the system and the likelihood of this attack's occurrence, which determine the attack's risk level. As shown in Figs 1 and 2, system status, infrastructure information, attack information, and risk characteristics were used in order to form a matrix, which would be ranked as is shown in Fig 3.

Indices and values

The first step was to generate the Matrix of Experts. The values used in the matrix, as shown in Table 1, were provided by a small group of experts in network security with ample experience in network auditing and risk assessment. The Matrix of Experts [24] used in this work had nine indices: Business Performance, Network Latency, Access to Information, Attack Duration, Time To Recover, Technical Difficulty, Technical Knowledge, Resources Relation, and Required Access to System. Each index was evaluated from one to five, being one the lowest and five the highest risk value.

All the variables used to construct the Risk Matrix contribute to four main inputs as described before. These four main inputs for the Impact and Likelihood values are: Severity, Even Duration, Difficulty, and System Access.

Severity. The severity of an attacks represents how stiff the effects of such attack are to the system. In our case the severity of an attacks depended on three values: Business Performance, Network Latency, and Access to Information. Those values were defined as follows:

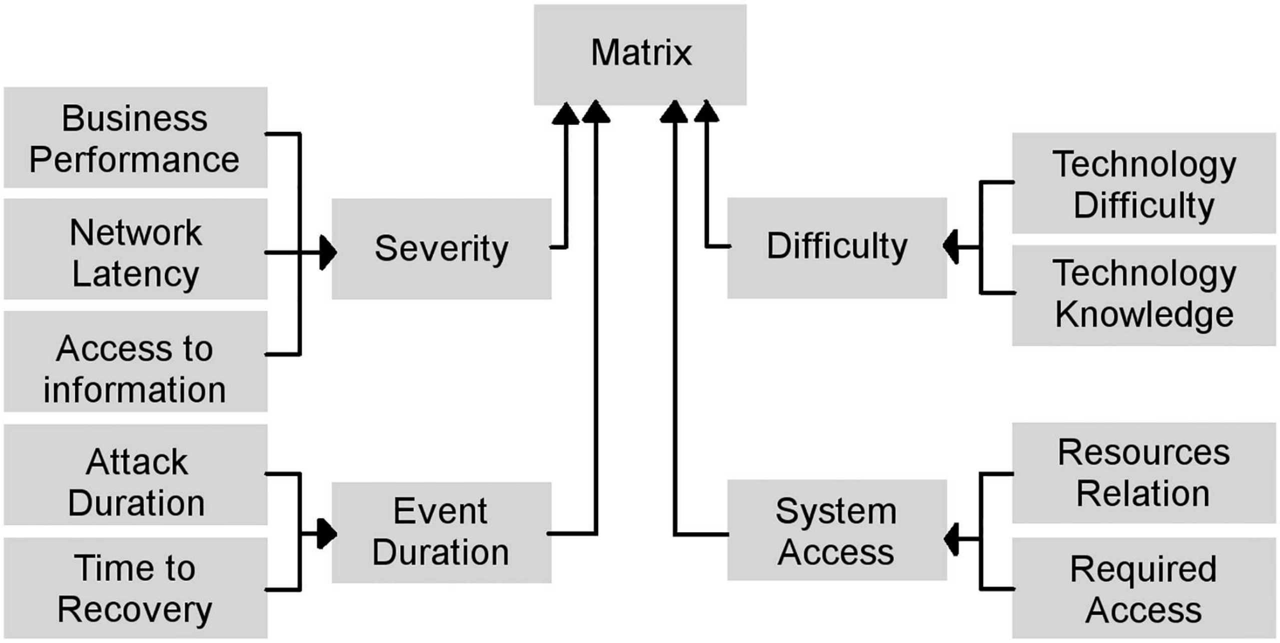
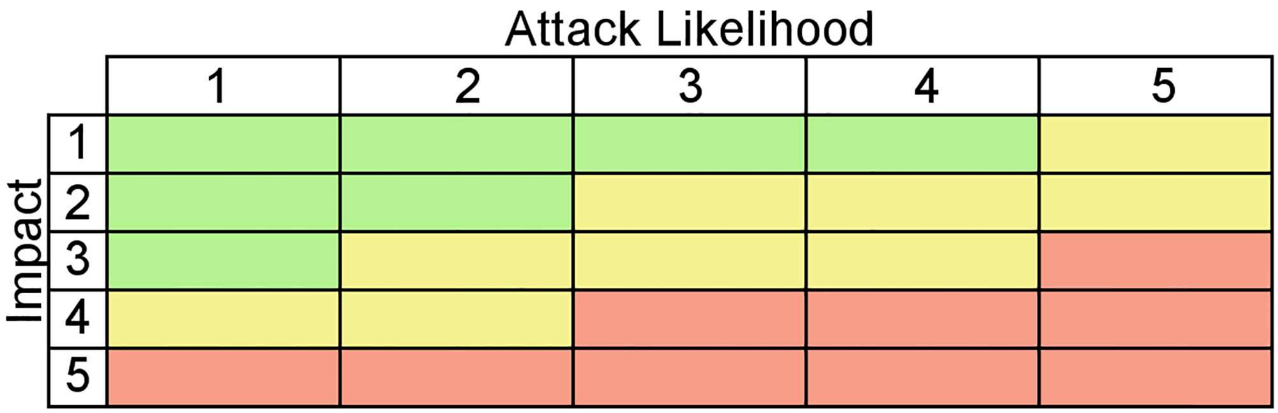


Fig 2. Indexing values. Different indices and values used to create the Matrix of Experts. The different inputs are weighed applying the corresponding correction values.

https://doi.org/10.1371/journal.pone.0188759.g002

The **Business Performance** variable was defined as the effect that an attack had to the expected business operations. Similar metrics can be found in other works such as in [28]. This index was related to how much the attack affected the system from a business point of view. A high value of the business performance index ($BP \geq 4$) meant that the attack affects the business performance, up to the point of stopping normal operations ($BP = 5$). A low index value ($BP \leq 2$) denoted that an attack had little or no effect ($BP = 1$) in regular business operations. Since VLC is defined at the physical (PHY) and data-link (MAC) layers of communication [1], the difference between the use of this technology and other technologies at the physical and data-link layers does not increase nor decrease the effect on the business



Attack Likelihood

Impact	1	2	3	4	5
1	🟩	🟩	🟩	🟩	🟨
2	🟩	🟩	🟨	🟨	🟨
3	🟩	🟨	🟨	🟨	🟥
4	🟨	🟨	🟥	🟥	🟥
5	🟥	🟥	🟥	🟥	🟥

Fig 3. Risk model distribution. The matrix shows the three areas of concern: Red denotes high and medium-high risk; Yellow indicates medium risk and borderline values; Green denotes medium-low and low risk.

https://doi.org/10.1371/journal.pone.0188759.g003

Table 1. Attack values general table.

	Values								
Item	*BP*	*NL*	*IA*	*AD*	*TTR*	*TD*	*TK*	*ReR*	*RA*
Level	1–5	1–5	1–5	1–5	1–5	1–5	1–5	1–5	1–5

Used variables: Business Performance (*BP*), Network Latency (*NL*), Access to Information (*IA*), Attack Duration (*AD*), Time to Recover (*TTR*), Technical Difficulty (*TD*), Technical Knowledge (*TK*), Resources Relation (*ReR*), and Required Access (*RA*). All variables have a minimum of 1 and a maximum of 5.

https://doi.org/10.1371/journal.pone.0188759.t001

performance. However, the use of this variable was required to properly evaluate the risk that the attacks studied posed to the system.

For this work, the **Network Latency** variable was defined as the observed incremented on the time system response when attacked. Metrics such as the ones used in [29] could be applied for greater detail. However, in order to simplify and clarify the analysis, the metric was used as stated applying a more general definition as the one used by [30]. A high ($NL \geq 4$) latency value represented that a large increment of time was required to get any information through the network due to the network state. On the opposite side, a low latency value ($NL \leq 2$) represented that the attack had no observable effect over the time required for the information to access and traverse the network. Since VLC data speed ranges from 11.64 Kb/s to 96 Mb/s [1], with higher bit-rates, the channel is generally more susceptible to noise, and an increase of noise requires re-transmissions among other delaying processes. In the cases of lower data rates, attacks over the VLC channels may have no significant difference from those done in any other technology. However, when considering attacks over a VLC channel that is configured for higher transmission data rates, the effects on the latency of the system may become more important and a higher value should be used in this variable. This consideration should be taken into account when using even higher data rates as proposed in [31].

The **Access to Information** index represented the quality and quantity of information that was accessed by the attacker while performing the attack as defined in [32]. A high value of the access to information ($IA \geq 5$) meant that the attacker had access to a large range of information, including confidential information such as accounting or sales practices. A small value of the access to information index ($IA \leq 2$) meant that the attacker had access to a small range of information with little intrinsic value such as public information or the network's name. As in other technologies, the access to information value depends on the attack and not on the implemented VLC system. Still, this parameter was required to properly gauge risk.

Duration of the Event. The Duration of the Event represented the total time the attack had an effect over the system from the attacks starts until the full system recovery. It depended on two values: Attack Duration and Time to Recover. For this work, those values were defined as follows:

The **Attack Duration** index represented the time length that an attack was considered active. A high value of duration ($AD \geq 4$) represented an attack that was active for extended times such as hours or days. The worse case ($AD = 5$) was that the attack has permanent effects over the system. A small value ($AD \leq 2$) of the duration index represented attacks that were active for short periods of time or were near instant ($AD = 1$) in they duration or effects over the system. Duration as was defined in this work, together with Time to Recover, can be found in other works, such as [33], to measure the impact that an attack would have in a network. As in other technologies, the duration value depends on the attack and not on the implemented VLC system.

The **Time To Recover** index represented the length of time required for the network to recover its normal functions and responds after the end of the attack [32]. A high value of the index ($TTR \geq 4$) represented that the time required to recover was large, hours or days for example. The worse case scenario ($TTR = 5$) would be that the effects of the attack were, or were near, unrecoverable after the end of the attack. A small value ($TTR \leq 2$) of the index represented that the networks recovered from the attack effects after a short time or even instantly ($TTR = 1$) after the attack ended.

In the case of VLC versus other systems such as WiFi, the recovery protocols used in VLC have been less tried, deployed and tested, with the exception of the ones ported from other communication technologies. A decrease in performance from such protocols in VLC could be expected, and further testing is required. If the recovery time increased, a higher index of this variable should be considered. Additionally, due to network design, flooding attacks may affect more than a single VLC access point. This flooding, in turn, may trigger a cascading effect. A cascading effect event would increase the *TTR*, and therefore a higher *TTR* index value should be considered. However, if self healing mechanisms as the ones described at [34], the *TTR* value could be expected to decrease.

Difficulty. The Difficulty represented the global attack difficulty from the point of implementation to the point of interpreting the attack results. As such, it value came from the combination of the Technical Difficulty and the Technical knowledge required to implement and understand the results of such attack. For this work, those values were defined as follows:

The **Technical Difficulty** index represented how laborious was to implement the technological means of the attack as laid by [35]. A high value of the index ($TD \geq 4$) meant that implementing the attack was not only feasible and without difficulties, but trivial ($TD = 5$). A low value of the index ($TD \leq 2$) represented that the technical difficulty of implementing, such as constructing special equipment, an attack was quite high. The reason to use a high index value for low difficulty and low index value for high difficulty was based on the implementation of the Difficulty value ($ADif_x$) of the attack as it was obtained by direct relation of the indexes values.

One of the variables taken into account when evaluating the technical difficulty of the attacks was the almost lack of literature that deals with VLC exploits. The only research related to exploiting the technology that could be directly applied to VLC was related to the Zigbee (Advanced Encryption Standard Counter with CBC-MAC usually referred as AES-CCM*) cryptography [36–38], also used in VLC [1]. Due to the lack of literature, attacks must be designed from the ground up, which in turn, increases the technical difficulty of complex attacks decreasing the index in this variable. In addition to the lack of attack literature, there is also a lack of commercial solutions. The lack of commercial solutions generates a problem when designing broad attacks since each possible VLC implementation may differ from others and therefore a general attack strategy is hard to implement. For these reasons, the *TD* index for VLC attacks should be decreased if compared to similar attacks on other technologies.

The **Technical Knowledge** index represented the expertise and lore required to implement an attack and interpreted the response of the system to such attack as presented in [35]. A high value of the index ($TK \geq 4$) represented that the technical knowledge needed to implement and understand the response of the attack was trivial. A low value in the index ($TK \leq 2$) represented that the technical knowledge required to implement and understand the response of the system to the attack was substantial. The reason for using a high index value for low difficulty and low index value for high difficulty was based on implementation of the Difficulty value ($ADif_x$) of the attack as it was obtained by direct relation of the indexes values.

As in the previous case, the technical difficulty index, there is little to none literature related to VLC security [13–15, 17, 18] which, even when using well-known attacks, increases the knowledge required to perform and evaluate the results of such attacks. Also, as in the previous index, there are no commercial solutions over which test or implement generic attacks. Therefore a lower index value of this variable should be used when we compare the technical knowledge required to implement an attack on VLC vs the one required to implement a similar attack in another well-known technology such as WiFi.

To attack VLC systems is necessary to know of the visible light channel behavior and the influence of the physical and geometrical parameters involved in the data transmission. This requires that the attacker posses ample knowledge of optics and photonics so he can exploit weaknesses in the implementation. This know-how is not usually possessed by the typical attacker which is more familiar with the Radio Frequency (RF) domain used in technologies such as WiFi.

This metric, as well as the Technical Difficulty one, have also been studied in [39] to define the security behavior, an index similar to the ones applied in this work.

System Access. The System Access quantitatively represented how easy is to access the system to be attacked. It resulted from combining the Resources Relation and Required to the System values. For this work, those values were defined as follows:

The **Resources Relation** index represented the relation between the resources that the attacker needed to implement an attack, and the resources the victim needed to prevent or mitigate such attack. A high value of the index ($ReR \geq 4$) meant that the attacker needed considerably fewer resources to implement an attack than the victim to prevent such attack. A low value of the index ($ReR \leq 2$) represented the cases where the attacker required considerably more resources to implement an attack than the victim to prevent that same attack.

On the one hand, due to the low deployment status of VLC, the hardware and software required to implement an attack must be self-made or adapted. Therefore, the value of this variable should be decreased. On the other hand, depending on the attack characteristics, the hardware needed could be easily accessible and cheap, such as photodiodes, while the defense measures may include up to building redesign. In this latest case, the value would increase. Due to these concerns, VLC may have a higher or lower ReR value depending on the attack and the attacks requirements if compared to similar technologies.

The **Required Access to System** index represented the access the attacker needed to the victim's VLC network to successfully perform the attack. This metric, as well as the Resources Relation one, contributed to the System Access metric. Similar metrics are commonly used, such as in [40] to develop security models that validate the robustness of systems. In the case of Required Access to System, a high index value ($RA \geq 4$) denoted that little or minimum access, such as from outside the premises, was required to succeed in the evaluated attack. A low index value ($RA \leq 2$) represented a situation in which the attacker required considerable access, even at data-center level, to pursue successfully the attack.

One of the main limitations of VLC attacks is attenuation of the energy received from a VLC access point (AP) versus the one received from an RF AP. Eq 1 shows the electrical power received (P_{elec}^{RF}) from RF where P_{Tx} is the power emitted, G_{Tx} is the gain of the emitter, G_{Rx} is the gain of the receiver, λ is the wavelength and d is the distance of the receiver from the emitter. From Eq 1 it can be inferred that the electrical power received inversely decreases to the square of the distance. It can be seen through Eq 2 that the electrical power received from VLC (P_{elec}^{VLC}) where P_{Tx} is the power emitted, $S(\theta)$ is the radiation pattern of the emitter, $G(\psi)$ is the optical gain, A_{eff} is the effective area of the receiver, d is the distance and $R(\lambda)$ is the receiver responsivity. From Eq 2 it can be inferred that the power received inversely decreases by the distance to the fourth power.

$$\begin{aligned} P^{RF}_{elec} &\propto P_{Tx} G_{Tx} G_{Rx} \left(\frac{\lambda}{4\pi d} \right)^2 \\ P^{RF}_{elec} &\propto d^{-2} \end{aligned} \tag{1}$$

$$\begin{aligned} P^{VLC}_{elec} &\propto \left[P_{Tx} S(\theta) G(\psi) \frac{A_{eff}}{d^2} R(\lambda) \right]^2 \\ P^{VLC}_{elec} &\propto d^{-4} \end{aligned} \tag{2}$$

As can be observed in Eq 2, the power vs distance relation is inversely proportional ($\propto$) to the fourth power instead of inversely proportional ($\propto$) to the square as is the case for RF emissions (Eq 1). This decrease of system efficiency is based on the optoelectric conversion when transmitting using VLC. The end result is that, in the case of VLC, at the same distance the received energy is less than in the RF case. The main result of the faster loss of power is that, basically, it decreases the range from which an attack can be done compared to regular RF/WiFi attacks. Attack range can be increased by improving the gain of the receiver, as using lenses in the case of the receiver (Fig 4) or focusing the energy on an active emitter (Fig 4). For the purposes of this work, those methods to increase the range have been taken into account in the technical difficulty and therefore included in the *TD* index value.

Furthermore, the use of multiple emitters as well as the environment, as shown on Fig 5 can increase the noise of the system. This noise limits the signal to noise ratio (SNR) and in consequence, it limits the channel capacity, in other words, it limits the amount of information that can be received through the channel.

The environmental noise, natural or generated, limits the received signal. Applying Eq 3 we can determine the real Signal to Interference and Noise Ratio (SINR). Consequently, multiple emitters, as well as natural sources, limit also the range from which a VLC system may be attacked.

$$SINR = \frac{(P_{Tx} H(0) R(\lambda))^2}{\sigma^2_{Th} + \sigma^2_{sh} + \sum_{i \in I} (P_i H_i R(\lambda))^2} \tag{3}$$

On Eq 3, the value P_{Tx} represents the emitted power, $H(0)$ represents the channel gain, $R(\lambda)$ the receiver responsibility, σ_{Tx} is the thermal noise (based on temperature, bandwidth and amplifier noise figure), σ_{sh} is the shot noise (based on photo-generated current, the darkness current and background current), P_i is the power of the interfering signals, H_i is the impulse response, I is the interfering sources set.

Determining Risk Matrix values

The global risk level (NRR_x) for different attacks over a VLC system was determined by a combination of the Likelihood (LK_x) and the event's Impact ($Impact_x$). The evaluation of Likelihood and Impact is based on the indices enumerated above. Their level descriptions are shown on Table 2.

Determining the impact. As can be observed in Figs 1 and 2 the Impact was obtained from several parameters: Business Performance (BP_x), Network Latency (NL_x), Information Access (IA_x), Attack Duration (AD_x), and Time to Recover (TTR_x) from the attack. These elements were divided into two categories: Severity of the event (Sev_x), and Duration of the event

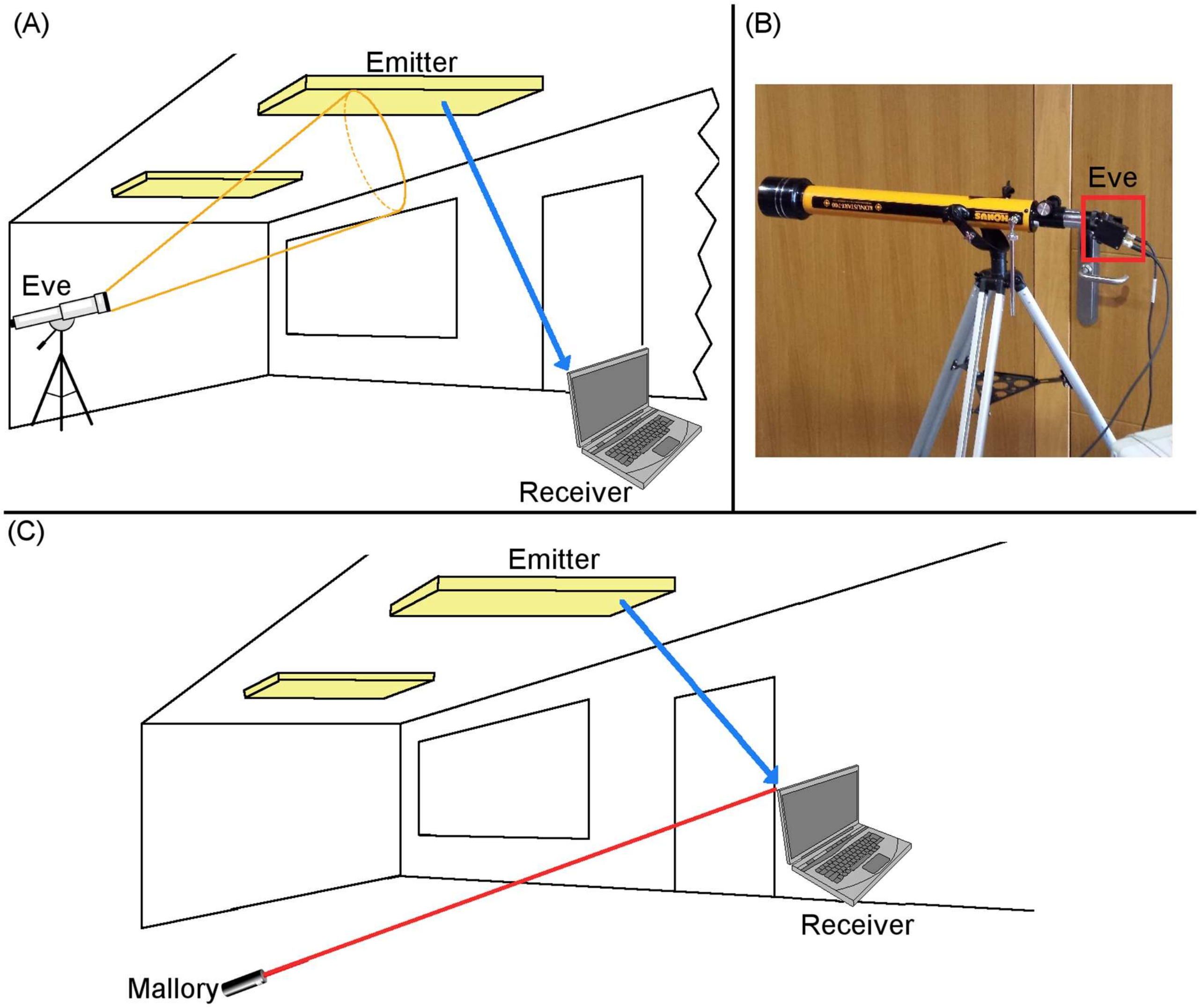


Fig 4. Sniffing and DoS scenarios. (A) Shows an interception of a communication between an emitter (lamp) and a receiver (Computer) by an eavesdropper (Eve) using a photodiode connected to a telescope. (B) Shows the actual assembly of the scenario and the photodiode is highlighted with a red box. The (A) scenario and image (B) were obtained from [18]. (C) Shows a scenario in which an attacker used a Laser to “blind” the receiver (Computer) resulting in a DoS type attack.

https://doi.org/10.1371/journal.pone.0188759.g004

(T_x), which were determined by Eqs 4 and 5. On the equations correction factors, as used in [24, 41–43], α and β were used for severity and duration of the event on Eqs 4 and 5, while the η factors were used for the end impact factor as shown in Eq 6.

$$Sev_x = \alpha_1(BP_x) + \alpha_2(NL_x) + \alpha_3(IA_x) \tag{4}$$

$$T_x = \beta_1(AD_x) + \beta_2(TTR_x) \tag{5}$$

Network latency had a correlation of 1 for the severity of the event (α_2 = 1.00), while the business performance and access to information had a bigger impact (α_1 = 1.05, α_3 = 1.10) for the severity of the event. In the case of event’s duration, when was considered the attack duration and the time to recover from such attack, it was understood that the attack duration had a

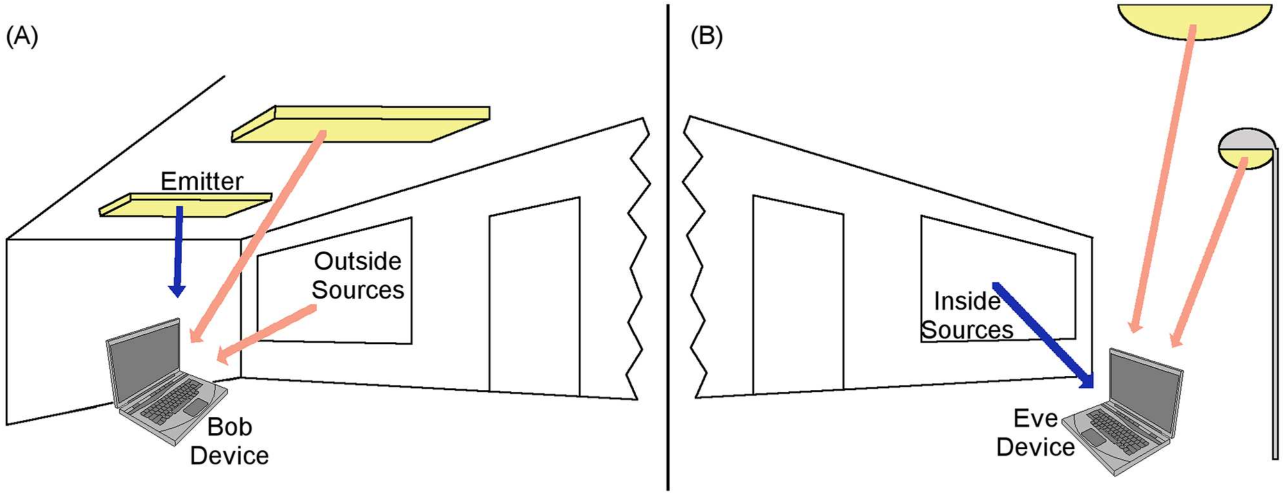


Fig 5. Interference to light channel. Visible light contributions are shown with blue arrows. Noise contributions are shown in red arrows. (A) Indoors scenario where a ceiling light emitting diodes (LED) lamp is the emitter and there are two noise sources: One from the outside through the window and another LED lamp which is not part of the communication with Bob's device. (B) Outdoors scenario where the communication with Eve's device comes from the inside through the window (a leak scenario or an indoor-to-outdoor communication scenario) in which two possible noise sources are present: A street lamp and the sun.

https://doi.org/10.1371/journal.pone.0188759.g005

larger impact in the event ($\beta_1 = 1.05$). Finally, when all variables that affect the attack impact were considered, the severity value had a larger effect ($\eta_1 = 1.10$) than the attack duration ($\eta_2 = 1.00$). Based on all these considerations the correction values are shown in Table 3.

These elements (Sev_x and T_x) contributed to the Impact ($Impact_x$) and were applied using Eq 6. The results were not only numerical but could also be translated into predefined levels. To obtain the values, the correction factors shown on Table 3 were used.

$$Impact_x = \eta_1(Sev_x) + \eta_2(T_x) \tag{6}$$

Determining the likelihood. As can be observed in Figs 1 and 2 the Likelihood (LK_x) was obtained from multiples parameters: Technology Difficulty (TD_x), Technology Knowledge (TK_x), Resources Relation (ReR_x), and Required Access to the system (RA_x). These elements were organized into two sets: Those contributing to the Attack Difficulty ($ADif_x$) value and those contributing to the Access to the System (AS_x) values. These values ($ADif_x$ and AS_x) were obtained by applying Eqs 7 and 8. The correction factors γ and ϕ needed for the equations were determined based on the security expertise of the group as in the Impact correction

Table 2. Level description of risk.

Level	Risk	Impact	Likelihood
5	Critical	Severe	Probable
4	Serious	Significant	Likely
3	Moderate	Moderate	Possible
2	Minor	Minor	Unlikely
1	Negligible	Negligible	Rare

Relation between the level (numerical) value and the risk, Impact and Likelihood of the studied attack.

https://doi.org/10.1371/journal.pone.0188759.t002

Table 3. Impact correction factors.

	Impact Values						
Factor	α_1	α_2	α_3	β_1	β_2	η_1	η_2
Value	1.05	1.00	1.10	1.05	0.95	1.10	1.00

This table shows the correction factors. The α's values are used at the severity evaluation. The β's values are used at the duration of the event evaluation. The η's are used at the Impact evaluation.

https://doi.org/10.1371/journal.pone.0188759.t003

values (α, β and η).

$$ADif_x = \gamma_1(TD_x) + \gamma_2(TK_x) \tag{7}$$

$$AS_x = \phi_1(ReR_x) + \phi_2(RA_x) \tag{8}$$

These elements ($ADif_x$ and AS_x) contributed to the Likelihood using Eq 9 and the results were not only numerical but also translated into predefined levels with the corresponding correction (υ_x) values.

$$LK_x = \upsilon_1(ADif_x) + \upsilon_2(AS_x) \tag{9}$$

Technology difficulty and technology knowledge contributed equally to the attack difficulty index ($\gamma_1 = \gamma_2 = 1.00$). In the case of the Access to System index, the required access had a larger impact than the resources relation between the attacker and the victim so a small correction factor of 5% was applied. Finally, in the overall likelihood index, the attack difficulty had a larger impact than the access to the system index. For that reason, the small correction factor of 5% was also applied. All correlation factor are shown in Table 4.

Level descriptions. Five levels were defined for each of the security parameters used in this work. As a general rule, as shown in Table 2, a value of 1 represented the smaller risk and a value of 5 represented the higher risk to the system. Table 2 presents the equivalence of the risk (NRR_x), Impact ($Impact_x$) and Likelihood (LK_x) values to the numerical value used in Eqs 6 and 9.

The Impact values were obtained from the Severity Value (Sev_x from Eq 4) and the Duration Value (T_x from Eq 5). The corresponding values for the numbers are shown on Table 5.

The Likelihood values (LK_x) were obtained from the Attack Difficulty, $ADif_x$ from Eq 7, and the Access to the System, AS_x from Eq 8, values. The corresponding values for the numbers are shown on Table 6.

Table 4. Likelihood correction factors.

	Likelihood Values					
Factor	γ_1	γ_2	ϕ_1	ϕ_2	υ_1	υ_2
Value	1.00	1.00	1.00	1.05	1.05	1.00

The table shows the correction factors determined by the security expertise of the group. The γ's values are used at the attack difficulty evaluation. The ϕ's values are used at the access to the system evaluation. The υ's are used at the likelihood evaluation.

https://doi.org/10.1371/journal.pone.0188759.t004

Table 5. Level description of impact values.

Level	Severity	Duration
5	Severe	Perpetual
4	Significant	Long Term
3	Moderate	Moderate
2	Minor	Short Term
1	Negligible	Instant

The table shows the relation between the level (numerical) value and the severity and duration of the event.

https://doi.org/10.1371/journal.pone.0188759.t005

Table 6. Level description of likelihood values.

Level	Attack Difficulty	Access to System
5	Negligible	Non required
4	Minor	Public
3	Moderate	Controlled
2	Significant	Restricted
1	Severe	Secured

The table shows the relation between the level (numerical) value and the attack difficulty and the required access to the system of the event.

https://doi.org/10.1371/journal.pone.0188759.t006

Risk Rank and risk level

The Risk Rank (RR_x) was defined, as shown in Eq 10, by combination of the Impact ($Impact_x$) and the Likelihood (LK_x) values.

$$RR_x = \varrho_1 \cdot Impact_x \cdot \frac{LK_x}{\varrho_2} \tag{10}$$

The values for ϱ_1 correction factor were provided by Eq 11 and the values for ϱ_2 correction factor were provided by Eq 12. As can be observed, for all cases, the impact of the attack increases the risk of the event in a more significant way than the likelihood of such event. This was transferred into our equation by applying the ϱ values shown in Eqs 11 and 12. These correction factors also helped to identify the attacks that generated higher risk to the system.

$$\varrho_1 = \left\{ \begin{array}{ll} 1.00 & Impact_x \leq 3 \\ 1.10 & Impact_x = 4 \\ 1.25 & Impact_x = 5 \end{array} \right\} \tag{11}$$

$$\varrho_2 = \left\{ \begin{array}{ll} 1.00 & LK_x \leq 4 \\ 0.90 & LK_x = 5 \end{array} \right\} \tag{12}$$

This value (RR_x) was then normalized, a shown in Eq 13, using the summatory of all the possible Risk Ranks ($\sum_{i=1}^{E} RR_i$) and the total amount of attacks (E) that had been defined for

Table 7. Risk level.

Value	Level
$NRR_x > 1.12$	High
$0.84 < NRR_x \leq 1.12$	Medium-High
$0.56 < NRR_x \leq 0.84$	Medium
$0.28 < NRR_x \leq 0.56$	Medium-Low
$NRR_x \leq 0.28$	Low

The table shows the equivalence between the normalized value (NRR_x) of the attack and the level value of the attack. In the normalization, all the attacks were considered in order to generate the corresponding values. The ranges was obtained from dividing the complete range, itself obtained from the difference between the best case ($LK_x = 1$ and $Impact_x = 1$) and worse case scenarios ($LK_x = 5$ and $Impact_x = 5$), divided in the number of levels considered.

https://doi.org/10.1371/journal.pone.0188759.t007

the system.

$$NRR_x = \frac{RR_x \cdot E}{\sum_{i \in E} RR_i}; \qquad x \in E \tag{13}$$

The obtained normalized value (NRR_x), also known as risk level, was interpreted to one of the five possible levels used thought this work. The correspondence between the normalized value (NRR_x) of the attack and its level is shown in Table 7. The used thresholds were determined in the distribution obtained from the analysis of the considered possible attacks.

As can be observed in Table 7 the used values were modified by the correction factor (ϱ_1 and ϱ_2). This rate helped to identify the attacks that generated higher risk to the system.

Example application

As an example of the use of Risk Matrix to determine the quantitative risk of an attack, an analysis was done to four different attacks: War Driving, Queensland alike Denial of Service (DoS), Preshared Key Cracking, and Evil Twin. These attacks were selected to be described in detail since each of them, according to the taxonomy shown in S1 Appendix, is of a different type (reconnaissance, denial, and cracking) of attack and helps understand the methodology used as well as the limitations of VLC technology.

War driving

The first evaluated attack was the War driving (WD_x) one. War Driving is the act of searching for wireless networks by a person in a moving vehicle or walking, using a portable device connected to a network interface in promiscuous mode. The objective of the attack is to detect the existence or not of a data network and its basic configuration parameters. Fig 5 represents a comparable scenario. The index values, normalized average, provided by the groups of experts for the War Driving attacks are shown in Table 8.

Table 8. War Driving values.

	Values								
Item	*BP*	*NL*	*IA*	*AD*	*TTR*	*TD*	*TK*	*ReR*	*RA*
Level	1	1	2	2	1	5	4	4	5

Summary of the variable values for a War Driving attack.

https://doi.org/10.1371/journal.pone.0188759.t008

As a reconnaissance attack, the effect of war driving into business performance was low ($BP = 1$). The attack did not increase the latency ($NL = 1$) of the network since it is a passive attack (S1 Appendix). The range of information captured by the war driving attack was low, but it was considered that included information like the use or not of cryptography in the VLC communication as well as the network characteristics. Therefore a medium-low value was given to the Information accessed index ($IA = 2$). The attack duration might be short but it might be repeated thought time so a medium-low value was assigned ($AD = 1$). The required time for the network to recover is usually almost null since, as stated before, war driving is a passive reconnaissance attack ($TTR = 1$). Regarding technical knowledge, easily accessible hardware [18] is required to do this kind of attack so it got a high index ($TD = 5$) value. The information that can be recovered from the attack is also easy to evaluate ($TK = 4$). Since the attacker does not require specialized hardware or many resources and the defender would require physical means to be protected from such an attack, the resources relation was weighted on the attacker side ($ReR = 5$). Finally, since this attack may be done from outside the building or from public areas, the required access index was also high ($RA = 5$). If those emitters could not be observed, then the value should have decreased to zero, making the attack impossible. However, it should be considered the possibility of transmission through transparent elements such as windows.

The value of the attack Impact (2.10) was equivalent a Level 1 (Table 2) Impact value (negligible) due to normalization. The likelihood value (10.25) was equivalent to a level 5 (Table 2) or Probable. These values resulted in a Risk Rank of 5.55. Therefore, the risk level (NRR_{WD}) of the War Driving attack was 0.52, a level 2 equivalent or minor risk attack.

Queensland alike DoS

The second evaluated attack was the Queensland alike DoS ($QDoS_x$). This attack is a Denial of Service Attack, and therefore a denial phase attack according to the taxonomy used (S1 Appendix). In the Queensland alike DoS, the attacker utilizes a computing device connected to a powerful emitter that makes reception by authorized users impossible due to the interference generated. In the VLC system case, an example of this could be an attacker using a laser, a torch/flashlight or meddling with the existing lamps as illustrated on Fig 4C. The evaluated index values for the Queensland alike DoS attack are shown in Table 9.

As a DoS attack [44], the effect of the Queensland alike DoS attack in the business performance is high ($BP = 4$) since it disturbs the access and all translations being done through the VLC system. The attack also significantly increases the latency ($NL = 5$) of the network since it is an active attack and the noise generated decreases the channel capacity. The range of information captured by such attack is negligible, since, by its nature, it only denies access ($IA = 1$). The attack duration can be long and be repeated through time, so a very high value was assigned ($AD = 5$) to the duration. The required time for the network to recover can be expected to be relatively small ($TTR = 2$) and take place moments after the attack stops. In this scenario no self-healing mechanisms were considered since those recovering techniques, as

Table 9. Queensland alike Denial of Service attack.

	Values								
Item	*BP*	*NL*	*IA*	*AD*	*TTR*	*TD*	*TK*	*ReR*	*RA*
Level	4	5	1	5	2	4	4	4	4

Summary of the variable values for a Queensland alike Denial of Service (DoS) attack.

https://doi.org/10.1371/journal.pone.0188759.t009

shown in [34], have not been included in the VLC standard [1] or current implementations so the *TTR* value can not be improved. Regarding technical knowledge, the readily available hardware is required to do this kind of attack, so it got a high index value ($TD = 4$). The required knowledge to create and understand the attack is small ($TK = 4$). Since the attacker does not require specialized hardware, as in the case of a flashlight, or many resources, as in a laser, and the defender will require physical means to protect such an attack from outside, the resources relation was weighed on the attacker side ($ReR = 4$). Finally, since this attack may be made from outside the building or public areas, the necessary access index was also high ($RA = 4$).

The value of the attack Impact (7.30) was equivalent a Level 4 (Table 2) Impact value (significant) due to normalization. The likelihood value (8.20) was equivalent to a level 4 (Table 2) or Likely. These values resulted in a Risk Rank of 17.60. Therefore, the risk level (NRR_{QDoS}) of the DoS attack was 1.64, a level 5 equivalent or critical attack.

Preshared Key Cracking

The third evaluated attack was the Preshared Key Cracking (PSK_x) attack. This attack was an exploitation phase attack according to our taxonomy. In this case, the attacker obtains the preshared key from any authorized user or from the existing communication channel. Methods that go from social engineering to code cracking can be used to obtain the key. The evaluated values for the PSK attack are shown in Table 10. Of the listed methods to obtain the key the most difficult one to implement is the one in which the VLC's cartographic system is broken. VLC uses a variation (CCM*) of the "Counter with CBC-MAC" (CCM) mode for operation on AES [1], as an authentication encryption algorithm. This variation, CCM*, is also used in the ZigBee [45] implementation of the IEEE 802.15.4 standard [46]. CCM* has widely been believed to provide a truly secure method for authentication. However, there have been some demonstrations that prove it is insecure in some specific cases [36–38] that might be exported and exploited in VLC implementations.

As a cracking/exploitation attack, the effect of the PSK Cracking attack in the business performance had a medium ($BP = 3$) value. This attack may increase the latency slightly due to the extra traffic generated to test the keys ($NL = 2$). The range of information potentially obtainable if the attack success is very high ($IA = 5$). The attack duration can be long and be repeated through time, being limited only if detected by other means or by having the key changed, so a very high value was assigned ($AD = 5$) to the duration index. The required time for the network to recover can be high since once the shared key is obtained the attacker will be able to access the system until the key is changed and all users will need to update their shared knowledge ($TTR = 5$). Regarding technical knowledge, the required hardware will be, or difficult to access or expensive, so the level will be low to do this kind of attack ($TD = 1$). The required knowledge to create and understand the attack is high, so a low value was assigned ($TK = 1$). As noted before, the attacker may require specialized hardware and many resources ($ReR = 1$). Finally, since this attack may be done from outside the building or public areas, the required access index was high ($RA = 4$).

Table 10. Preshared Key Cracking.

	Values								
Item	*BP*	*NL*	*IA*	*AD*	*TTR*	*TD*	*TK*	*ReR*	*RA*
Level	3	2	5	5	5	1	1	1	4

Summary of the variable values for a Pre-Shared Key (PSK) cracking attack.

https://doi.org/10.1371/journal.pone.0188759.t010

Table 11. Evil Twin.

	Values								
Item	*BP*	*NL*	*IA*	*AD*	*TTR*	*TD*	*TK*	*ReR*	*RA*
Level	3	3	5	5	4	2	4	3	3

Summary of the variable values for a Evil Twin attack.

https://doi.org/10.1371/journal.pone.0188759.t011

The value of the attack Impact (8.30) was equivalent a Level 4 (Table 2) Impact value (significant) due to normalization. The likelihood value (3.05) was equivalent to a level 1 (Table 2) or rare. These values resulted in a Risk Rank of 4.40. Therefore, the risk level (NRR_{PSK}) of the pre-shared key attack was 0.41, a level 2 equivalent or minor attack.

Evil Twin

As an exploitation attack, the effect of the Evil Twin attack (ET_x) in the business performance is medium ($BP = 3$). The attack increases the latency but not in high values due to the extra traffic ($NL = 3$). The range of information potentially obtainable if the attack success is very high ($IA = 5$). The attack duration can be long and be repeated thought time so a very high value was assigned ($AD = 5$). The required time for the network to recover can be high since once the twin has been detected the full network needs to be reconfigured or reset ($TTR = 4$). Regarding technical knowledge, the required hardware will be, or difficult to access or expensive, so the level will be low to do this kind of attack ($TD = 2$). The required knowledge to create and understand the attack is high, so a low value was assigned ($TK = 4$). As noted before, the attacker may require specialized hardware such a VLC AP ($ReR = 3$). Finally, even if this attack can be done from outside, generally, the evil twin device would be located inside the premises. Therefore, the required access index would be medium ($RA = 3$). All the evaluated values of the Evil Twin attack are shown in Table 11.

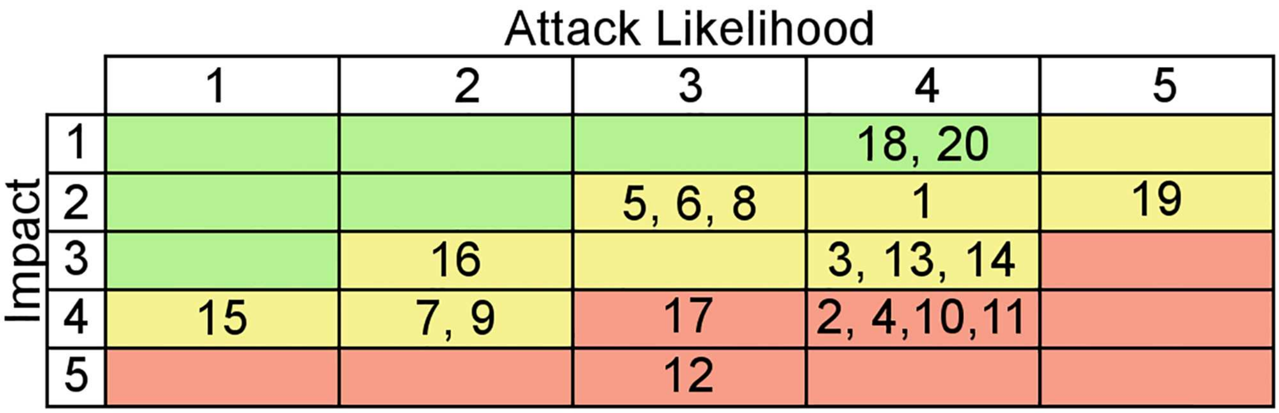
The value of the attack Impact (9.40) was equivalent a Level 5 (Table 2) Impact value (severe) due to normalization. The likelihood value (6.15) was equivalent to a level 3 (Table 2) or possible. These values resulted in a Risk Rank of 18.75. Therefore, the risk level (NRR_{ET}) of the Evil Twin attack was 1.75, a level 5 equivalent or critical attack.

Risk classification assessment using a Risk Map

The final step of the Risk Matrix approach was the use of a Risk Map for spatial allocation of the attacks. A Risk Matrix that includes all the attacks is shown in Fig 6.

As shown in Fig 7 the 20 possible attacks were positioned in four quadrants depending on their Likelihood (LK_x) and their attack's Impact ($Impact_x$) levels. The use of a Risk Map was vital in determining which attacks needed immediate attention and where the efforts to secure a network should be focused. In our case, it helped to determine strategies, that once implemented, decrease the risk improving the security efficiently.

The potentially most dangerous attacks are located within Quadrant I. Therefore special attention should be paid to minimize the risk those attacks presents to our VLC networks. Since the risk is composed by Likelihood (LK_x) and Impact ($Impact_x$), in general, and without taking into account the normalization applied, the farther from the central point of the figure the attack is, the riskier the attack will potentially be. In our work, examples of an attack located in this quadrant were the Queensland alike DoS attack and the Evil Twin Attack. Both attacks are tagged with the *QDoS* and *ET* marks on Fig 7.



Impact	Attack Likelihood 1	2	3	4	5
1				18, 20	
2			5, 6, 8	1	19
3		16		3, 13, 14	
4	15	7, 9	17	2, 4,10,11	
5			12		

Fig 6. Risk Matrix. The figure shows were each of the considered attacks is located on the Risk Matrix. The values from which the indices are obtained are on the table available at: S1 Table. The attacks are: Beacon Flood (1); De-authentication Flood (2); Authentication Flood (3); Queensland alike DoS (4); Data Reply (5); Frame Injection (6); EAP Downgrade (7); EAP Failure (8); Identity Theft (9); Password Speculation (10); AP Theft (11); Evil Twin (12); MAC Spoofing (13); Man in the Middle (14); PSK Cracking (15); Rogue Access Point (16); Shared Key Guessing (17); Active War Driving (18); Eavesdropping (19); War Driving (20).

https://doi.org/10.1371/journal.pone.0188759.g006

The attacks with high impact ($Impact_x$) but low likelihood (LK_x) are located in the second quadrant. In general, mostly cracking and exploitation attacks will be located here. The reason for their location is due to its difficult implementation, which generates a low likelihood value, and the huge impact they achieve once they are implemented. In our work, an example of an attack located in this quadrant was the Preshared Key Cracking attack. This attack is tagged with the *PSK* mark on Fig 7.

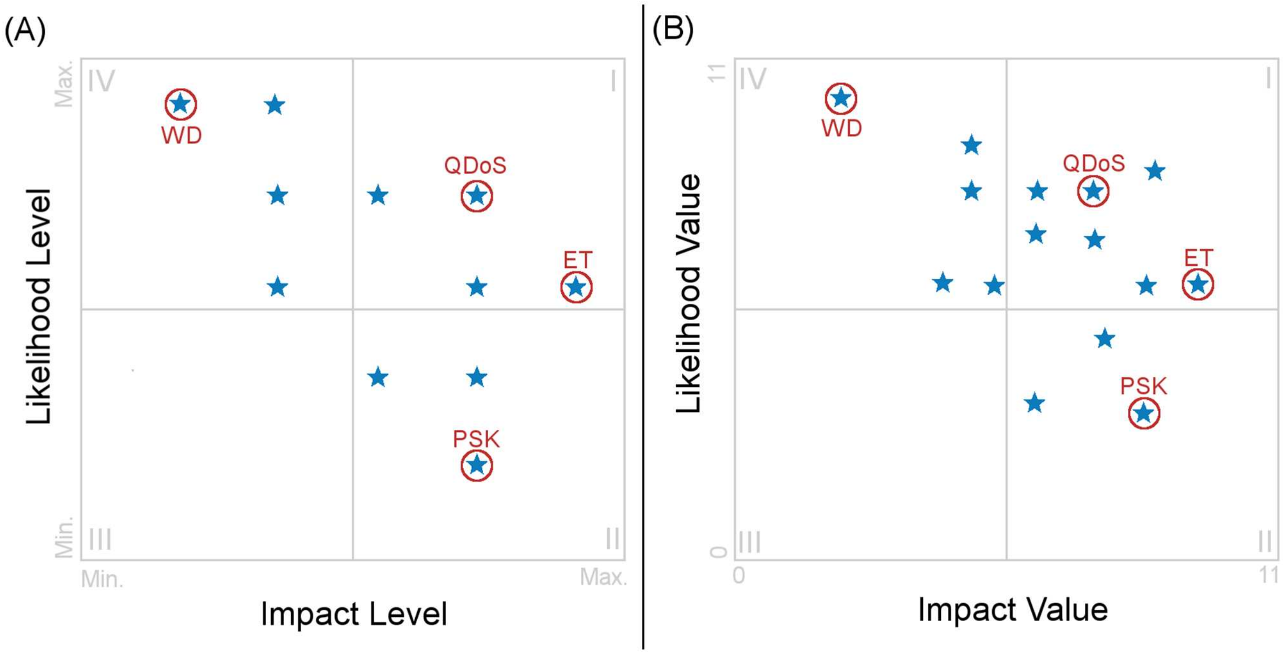


Fig 7. Risk Map. (A) Shows the Risk Map using the Impact and Likelihood levels with normalized values. (B) Shows the Risk Map using the Impact and Likelihood raw values. The different attacks are located in four different quadrants based on their likelihood and impact. Four attacks are circled and identified by their name contractions: War Driving attack (WD); Queensland alike Denial of Service attack (QDoS); Evil Twin attack (ET) and Preshared Key cracking attack (PSK). All the values used are in S1 Table.

https://doi.org/10.1371/journal.pone.0188759.g007

The attacks with low impact ($Impat_x$) and low likelihood (LK_x) are located in the third quadrant. Due to their low impact and likelihood, those attacks present a low risk for the network. Therefore, only if other attacks have been deal with, effort should be invested in them. In our work, no attack end up located in this quadrant as can be seen on Fig 7.

Finally, the attacks with a high likelihood (LK_x) but low impact ($Impact_x$) are located in the fourth quadrant. In general, reconnaissance attacks will be located on this quadrant. Even if they are easy to implement and use, and therefore have a high likelihood (LK_x) they have a, comparatively, low Impact. Nevertheless, attacks located in this quadrant should be addressed, for the reason that, as in the case of reconnaissance attacks, they may be precursors of further and more complex attacks, or so easy to implement that can become a nuisance. In our work, an example of an attack located in this quadrant was the War Driving attack. This attack is tagged with the *WD* tag on Fig 7.

Discussion

All the indices used during the example application were deduced for a VLC implementation. The physical differences of these networks with other wireless systems, such as WiFi, had been taken into account as well as the media access techniques that they use. Among these considerations were the channel limitations, the medium characteristics, the lack of literature available, the small level of deployment of this technology or the current state of VLC equipment development. All this results in the values obtained through the Risk Matrix methodology as can be shown bellow.

When comparing the values of the four examples, as shown in Table 12, it is observed that the risk of the War Driving and PSK Cracking attacks were almost the same even when they were based in opposite premises: In the case of war driving this was due to its easy implementation which resulted in a high likelihood ($LK_{WD} = 10.25$) value but with and low impact ($Impact_{WD} = 2.10$). In the case of Preshared Key Cracking attack, the value was due to the attack's low likelihood ($LK_{PSK} = 3.05$) but high Impact ($Impact_{PSK} = 8.30$) value. Table 12 list the different $Impact_x$, LK_x, RR_x and NRR_x of the evaluated attacks.

As can be observed on Table 12, in the case of the DoS attack, even if it had lower impact ($Impact_{QDoS} = 7.30$) than the Preshared Key Cracking ($Impact_{PSK} = 8.30$) attack, due to its higher likelihood, ($LK_{QDoS} = 8.20$) versus ($LK_{PSK} = 3.05$), it got a higher risk ($NRR_{QDoS} = 1.64$).

The Evil Twin attack had the almost the same risk ($NRR_{ET} = 1.75$) as the DoS attack ($NRR_{QDoS} = 1.64$) having a higher impact ($Impact_{ET} = 9.40$) but a lower likelihood ($LK_{ET} = 6.15$). The same situation happened, but for opposite reasons, when comparing the Queensland alike DoS with the Ware Driving attack: ($Impact_{QDoS} = 7.30$) vs ($Impact_{WD} = 2.10$) and ($LK_{QDoS} = 8.20$) vs ($LK_{WD} = 10.25$), resulting in ($NRR_{QDoS} = 1.64$) vs ($NRR_{WD} = 0.52$). This values ended up converted, using the conversion values of Table 2 in the levels and descriptions of Table 13.

Table 12. Selected attacks values.

Attack	$Impact_x$	LK_x	RR_x	NRR_x
War Driving	2.10	10.25	5.55	0.52
Queensland	7.30	8.20	17.60	1.64
PSK Cracking	8.30	3.05	5.40	0.41
Evil Twin	9.40	6.15	18.75	1.75

The table shows the selected attacks values of: Impact ($Impact_x$), Likelihood (LK_x), Risk Rank (RR_x) and Normalized Risk Rank (NRR_x) of the selected attacks. The full set of values are on the supplied additional material.

https://doi.org/10.1371/journal.pone.0188759.t012

Table 13. Examples levels.

Attack	NRR_x	Level	Description
War Driving	0.52	2	Minor
Queensland	1.64	5	Critical
PSK Cracking	0.41	2	Minor
Evil Twin	1.75	5	Critical

Correspondence of the Normalized Risk Rank (NRR_x) with the risk level and its corresponding description.

https://doi.org/10.1371/journal.pone.0188759.t013

Once the results were examined, it was apparent that unaccounted risk exists in the networks that employ VLC. According to our study, there were five, out of twenty evaluated attacks, that may present a critical risk for VLC networks. Therefore the implementation of VLC applications will need to add security measures. For example, assuming the existence of elements in the scenarios that leak light, such windows, allows attacks such as War Driving, Queensland alike DoS and Preshared Key Cracking to exist. Minimizing the light leakage, by blocking windows when possible, limits the likelihood of those attacks, and therefore increase the security of the system. However, if there is public access to the premises or the attacker fakes its identity, such in the case of the Evil Twin attack, this kind of protecting measure would have little to no impact in the attack associated risk and further security steps, such as the use of hard encryption, must be taken.

Conclusion

Even if the Risk Matrix methodology is a valid method to determine risk, and while it is not usually applied to the network security analysis, this works seems to demonstrate that this methodology presents itself as a valid process to determine the quantitative risk of different attacks. Therefore, Risk Matrix and Risk Maps approaches should be considered as a proper starting point in defining the risks that affect a network.

The adequate use of correction factors, based on the researchers and experts experience in the area, defines more accurately the impact and likelihood of the events and attacks studied. Therefore, several consensuated correction factors should be applied to reduce the uncertainty of such analysis while generating a proper distribution of the attacks levels.

By using weighted values, the uncertainty of risk from different attacks is diluted, and as a result, the real impact can be measured and be made more visible. This expected distribution is especially important for the researchers to select the riskier attacks, so the uncertainty of selecting the riskier attacks minimizing the resources is decreased. This optimization of resources is of prime importance in the security arena since, new and more sophisticated attacks appear continuously and may derail the researcher efforts.

The performed risk analysis highlight that even if *a priori* the VLC characteristics on the PHY and MAC layers seem to create a secure medium of communication, VLC implementation and unconsidered elements, such windows, open the possibility of a wide range of attacks that previously has been dismissed, and therefore present substantial risk in VLC use and implementation.

Finally, once all the attacks are positioned on a Risk Map, a clear picture of the relative quantitative risk of the attacks can be observed. This work demonstrated that, from the risk point, the QDoS and the Evil twin attack present the highest risk of all. Moreover, important attention should be paid to attacks such as War Driving since, even if they have a low risk due to their low impact, their likelihood and being the base for other insidious attacks warrant their occurrence.

Supporting information

S1 Table. Attacks weighs. The document includes all the attacks and the weights, factor, and indices used to generate the Risk Matrix according to the methodology utilized in this document. The document also includes statistics values obtained from the indices.
(ODS)

S1 Appendix. Attacks taxonomy. The document includes the taxonomy and the attacks classification used in this work.
(PDF)

S2 Appendix. List of parameters, symbols and variables. The document includes a full list of parameters, symbols, and variables used in this work as well as a short description of each one of them.
(PDF)

S3 Appendix. Glossary of terms. This appendix has been included to help non expert readers in the comprehension of the manuscript. The document includes a list of technical terms used in this work as well as a short description of each one of them.
(PDF)

Author Contributions

Conceptualization: Patricia Chavez-Burbano.

Data curation: Ignacio Marin-Garcia, Patricia Chavez-Burbano, Victor Guerra.

Formal analysis: Ignacio Marin-Garcia, Patricia Chavez-Burbano, Victor Guerra.

Investigation: Ignacio Marin-Garcia, Patricia Chavez-Burbano, Victor Guerra.

Methodology: Ignacio Marin-Garcia, Patricia Chavez-Burbano.

Project administration: Patricia Chavez-Burbano, Victor Guerra, Jose Rabadan, Rafael Perez-Jimenez.

Resources: Victor Guerra, Jose Rabadan, Rafael Perez-Jimenez.

Software: Ignacio Marin-Garcia, Patricia Chavez-Burbano, Victor Guerra.

Supervision: Victor Guerra, Jose Rabadan, Rafael Perez-Jimenez.

Validation: Ignacio Marin-Garcia, Victor Guerra, Jose Rabadan, Rafael Perez-Jimenez.

Visualization: Ignacio Marin-Garcia, Patricia Chavez-Burbano.

Writing – original draft: Ignacio Marin-Garcia.

Writing – review & editing: Ignacio Marin-Garcia, Patricia Chavez-Burbano, Victor Guerra, Jose Rabadan, Rafael Perez-Jimenez.

References

1. IEEE Standard for Local and Metropolitan Area Networks—Part 15.7: Short-Range Wireless Optical Communication Using Visible Light; 2011.
2. Haas H, Yin L, Wang Y, Chen C. What is LiFi? J Lightwave Technol. 2016; 34(6):1533–1544. https://doi.org/10.1109/JLT.2015.2510021

3. Burchardt H, Serafimovski N, Tsonev D, Videv S, Haas H. VLC: Beyond point-to-point communication. IEEE Communications Magazine. 2014; 52(7):98–105. https://doi.org/10.1109/MCOM.2014.6852089

4. Bazzi A, Masini BM, Zanella A, Calisti A. Visible Light Communications As a Complementary Technology for the Internet of Vehicles. Comput Commun. 2016; 93(C):39–51. https://doi.org/10.1016/j.comcom.2016.07.004

5. Feng L, Hu RQ, Wang J, Xu P, Qian Y. Applying VLC in 5G Networks: Architectures and Key Technologies. IEEE Network. 2016; 30(6):77–83. https://doi.org/10.1109/MNET.2016.1500236RP

6. Elgala H, Mesleh R, Haas H. Indoor optical wireless communication: potential and state-of-the-art. IEEE Communications Magazine. 2011; 49(9):56–62. https://doi.org/10.1109/MCOM.2011.6011734

7. Mahdy A, Deogun JS. Wireless optical communications: a survey. In: IEEE Wireless Communications and Networking Conference (WCNC). vol. 4 of Cat. No.04TH8733; 2004. p. 2399–2404.

8. Sewaiwar A, Tiwari SV, Chung YH. Smart LED allocation scheme for efficient multiuser visible light communication networks. Optics Express. 2015; 23(10):13015–13024. https://doi.org/10.1364/OE.23.013015 PMID: 26074554

9. Jung SY, Hann S, Park CS. TDOA-based optical wireless indoor localization using LED ceiling lamps. IEEE Transactions on Consumer Electronics. 2011; 57(4):1592–1597. https://doi.org/10.1109/TCE.2011.6131130

10. Wang TQ, Sekercioglu YA, Neild A, Armstrong J. Position Accuracy of Time-of-Arrival Based Ranging Using Visible Light With Application in Indoor Localization Systems. Journal of Lightwave Technology. 2013; 31(20):3302–3308. https://doi.org/10.1109/JLT.2013.2281592

11. Marin-Garcia I, Chavez-Burbano P, Muñoz-Arcentles A, Calero-Bravo V, Perez-Jimenez R. Indoor location technique based on visible light communications and ultrasound emitters. In: IEEE International Conference on Consumer Electronics (ICCE); 2015. p. 297–298.

12. Rabadan J, Guerra V, Rodríguez R, Rufo J, Luna-Rivera M, Perez-Jimenez R. Hybrid Visible Light and Ultrasound-Based Sensor for Distance Estimation. Sensors. 2017; 17(2):330. https://doi.org/10.3390/s17020330

13. Mostafa A, Lampe L. Physical-layer security for indoor visible light communications. In: IEEE International Conference on Communications (ICC); 2014. p. 3342–3347.

14. Mostafa A, Lampe L. Enhancing the security of VLC links: Physical-layer approaches. In: IEEE Summer Topicals Meeting Series (SUM); 2015. p. 39–40.

15. Blinowski G. Security issues in visible light communication systems. IFAC-PapersOnLine. 2015; 48(4): 234–239. https://doi.org/10.1016/j.ifacol.2015.07.039

16. Al-Kinani A, Wang CX, Haas H, Yang Y. Characterization and Modeling of Visible Light Communication Channels. In: IEEE 83rd Vehicular Technology Conference (VTC Spring); 2016. p. 1–5.

17. Classen J, Chen J, Steinmetzer D, Hollick M, Knightly E. The Spy Next Door: Eavesdropping on High Throughput Visible Light Communications. In: Proceedings of the 2Nd International Workshop on Visible Light Communications Systems. (VLCS). New York, NY, USA: ACM; 2015. p. 9–14.

18. Marin-Garcia I, Ramirez-Aguilera AM, Guerra V, Rabadan J, Perez-Jimenez R. Data sniffing over an open VLC channel. In: 10th International Symposium on Communication Systems, Networks and Digital Signal Processing (CSNDSP); 2016. p. 1–6.

19. Prasad R, Mihovska A, Cianca E, Mukherjee S. Comparative overview of UWB and VLC for data-intensive and security-sensitive applications. In: IEEE International Conference on Ultra-Wideband; 2012. p. 41–45.

20. Uysal M, Miramirkhani F, Narmanlioglu O, Baykas T, Panayirci E. IEEE 802.15.7r1 Reference Channel Models for Visible Light Communications. IEEE Communications Magazine. 2017; 55(1):212–217. https://doi.org/10.1109/MCOM.2017.1600872CM

21. Fu S, Zhou H, Xiao Y. The application of a risk matrix method on campus network system risk assessment. In: IEEE 3rd International Conference on Communication Software and Networks (ICCSN); 2011. p. 474–478.

22. Xiaosong L, Shushi L, Wenjun C, Songjiang F. The Application of Risk Matrix to Software Project Risk Management. In: International Forum on Information Technology and Applications (IFITA). vol. 2; 2009. p. 480–483.

23. Li ZP, Yee QMG, Tan PS, Lee SG. An extended risk matrix approach for supply chain risk assessment. In: IEEE International Conference on Industrial Engineering and Engineering Management; 2013. p. 1699–1704.

24. Cai X, Wang C, Chen S, Lu J. Model Development for Risk Assessment of Driving on Freeway under Rainy Weather Conditions. PLOS ONE. 2016; 11(2):1–16. https://doi.org/10.1371/journal.pone.0149442

25. Lu F, Bi H, Sun F, Yu C. Risk evaluation of IT outsourcing using Risk-matrix. In: 11th World Congress on Intelligent Control and Automation (WCICA); 2014. p. 599–601.

26. Theoharidou M, Mylonas A, Gritzalis D. In: Gritzalis D, Furnell S, Theoharidou M, editors. A Risk Assessment Method for Smartphones. Berlin, Heidelberg: Springer Berlin Heidelberg; 2012. p. 443–456.

27. Standard Practice for System Safety—MIL-STD-882D; 2000.

28. Brynjolfsson E, Hitt LM. Beyond Computation: Information Technology, Organizational Transformation and Business Performance. The Journal of Economic Perspectives. 2000; 14(4):23–48. https://doi.org/10.1257/jep.14.4.23

29. Obraczka K, Silva F. Network latency metrics for server proximity. In: Global Telecommunications Conference (GLOBECOM). vol. 1. Institute of Electrical and Electronics Engineers (IEEE); 2000. p. 421–427 vol.1.

30. Kurose J, Ross K. Computer Netwotking: A top-Down Approach. 6th ed. Hirsch M, editor. Pearson; 2013.

31. Hussein AT, Alresheedi MT, Elmirghani JMH. 20 Gb/s Mobile Indoor Visible Light Communication System Employing Beam Steering and Computer Generated Holograms. Journal of Lightwave Technology. 2015; 33(24):5242–5260. https://doi.org/10.1109/JLT.2015.2495165

32. Tanenbaum AS, Wetherall DJ. Computer Networks. 5th ed. Pearson; 2011.

33. Burbeck K, Andres SG, Nadjm-tehrani S. Time as a Metric for Defence in Survivable Networks. In: Proceedings of the Work in Progress session of 24th IEEE Real-Time Systems Symposium (RTSS); 2003.

34. Shang Y. Impact of self-healing capability on network robustness. Phys Rev E. 2015; 91:042804. https://doi.org/10.1103/PhysRevE.91.042804

35. Gao H, Hu J, Huang T, Wang J, Chen Y. Security Issues in Online Social Networks. IEEE Internet Computing. 2011; 15(4):56–63. https://doi.org/10.1109/MIC.2011.50

36. Ronen E, O'Flynn C, Shamir A, Weingarten AO. IoT Goes Nuclear: Creating a ZigBee Chain Reaction; 2016. Cryptology ePrint Archive, Report 2016/1047.

37. Goodspeed T. Extracting Keys from Second Generation Zigbee Chips. In: in Black Hat USA, Las Vegas. Citeseer; 2009.

38. Zillner T, Strobl S. ZigBee exploited: The good the bad and the ugly; 2015.

39. Stanton JM, Stam KR, Mastrangelo P, Jolton J. Analysis of end user security behaviors. Computers & Security. 2005; 24(2):124–133. https://doi.org/10.1016/j.cose.2004.07.001

40. Joshi JBD, Aref WG, Ghafoor A, Spafford EH. Security Models for Web-based Applications. Commun ACM. 2001; 44(2):38–44. https://doi.org/10.1145/359205.359224

41. Ni H, Chen A, Chen N. Some extensions on risk matrix approach. Safety Science. 2010; 48(10): 1269–1278. https://doi.org/10.1016/j.ssci.2010.04.005

42. Brand DVD. Risk analysis, a tool for decision—making. International Journal of Environment and Pollution. 1996; 6(4–6):388–397.

43. Ma L, Cheng L, Li M. Quantitative risk analysis of urban natural gas pipeline networks using geographical information systems. Journal of Loss Prevention in the Process Industries. 2013; 26(6):1183–1192. https://doi.org/10.1016/j.jlp.2013.05.001

44. Dao NN, Kim J, Park M, Cho S. Adaptive Suspicious Prevention for Defending DoS Attacks in SDN-Based Convergent Networks. PLOS ONE. 2016; 11(8):1–24. https://doi.org/10.1371/journal.pone.0160375

45. Gislason D. Zigbee Wireless Networking. Pap/onl ed. Newton, MA, USA: Newnes; 2008.

46. IEEE Standard for Low-Rate Wireless Networks—802.15.4-2015; 2015.