Cyber security flaws and deficiencies in the European Rail Traffic Management System towards cyber-attacks

Alexander Gabriel
TH Köln - University of Applied Sciences
alexander.gabriel@th-koeln.de

Florian Brauner
Kölner Verkehrs-Betriebe AG
florian.brauner@kvb-koeln.de

Andreas Lotter
University of Wuppertal, Germany
lotter@uni-wuppertal.de

Frank Fiedrich
University of Wuppertal, Germany
fiedrich@uni-wuppertal.de

Ompe A. Mudimu
TH Köln - University of Applied Sciences
ompe_aime.mudimu@th-koeln.de

ABSTRACT

Recent events have shown the vulnerability of IT systems of companies, organizations or even governments to hacker attacks. At the same time, information technologies are becoming increasingly established and important in various industries (digitalization). With a view to the modern development of terrorism, cyber-attacks can be used to physically damage critical infrastructures (CI). This leads to a new dimension of cyber-attacks, which are called terrorist cyber-attacks.

The following research contributes to the identification of weak information technology components of railway operating systems and thus improves the safety of public transportation in the context of the European railway traffic management system (ERTMS). The core of this paper is an extended literature research on security flaws in the ERTMS. The future introduction of a methodology for evaluating the criticality of information technology system components will build on this using cyber threats and public transportation as examples. Such a method may serve as a basis for further risk assessments and management measures.

Keywords

Cyber Attack, (Counter-) Terrorism, Vulnerability, European Rail Traffic Management System (ERMTS), Railway Transport

INTRODUCTION

The threat to railway companies or other CI from cyber-attacks is increasing in the course of the ongoing digitalization of society and industry (Settanni et al. 2017). In addition to the increasing complexity of attacks, companies are also becoming increasingly aware of the vulnerability towards cyber threats (German Federal Office for Information Security 2016). In the years from 2012 to 2017, the probability of becoming a victim of a cyber-attack - according to the companies surveyed - has risen by around 45 percent.

In the years 2007 to 2010, the Stuxnet attacks have already caused physical damage (Bambauer 2014). The basic principle of the Stuxnet code is also transferable to other sectors such as energy or transport, since similar protocols are often used due to industrial standardization (Karnouskos 2011; Lakshminarayana et al. 2016). Using the Black-Energy code, for example, it was possible in 2015 to successfully attack the Ukrainian

electricity grid and cause several hours of power outages (Khan et al. 2016). A similar vulnerability to the Stuxnet attacks has been exploited. However, not only these advanced and highly specific attacks pose a threat to CI. Large-scale damage to CI has also been caused by comparably unspecific attacks, such as WannaCry in the recent past. Worth mentioning here are the breakdowns of hospitals of the National Health System in Great Britain and in the rail traffic of the Deutsche Bahn, but also in many other companies (Volz und Auchard 2017).

The increasing threat posed by cyber-attacks is amplified by increasing digitization of industry and the associated transport sector (World Economic Forum 2016). With the introduction of the European Rail Traffic Management System (ERTMS) and its planned components Global System for Mobile Communications-Railway (GSM-R) and European Train Control System (ETCS), rail traffic systems are becoming even more digitally interconnected and thus potentially more susceptible to cyber-attacks.

Therefore, an indicator set is to be developed within the framework of the present work, which can be used to investigate which components of the ERTMS are particularly susceptible to cyber-attacks and on which factors this susceptibility is decisively dependent or via which vectors the ERTMS is vulnerable.

METHODOLOGY

Based on an extensive literature research, the threat of cyber-attacks to rail traffic respectively ERTMS is described in the following sections. For this purpose, potential attackers as well as the types of attacks and the corresponding threatened protection targets are identified and described. A comprehensive analysis of the ERTMS and its four essential components GSM-R, ETCS, ETML and INESS follows, which so far have only been examined individually and not in an integrated context.

The results of the literature research presented will serve as the future basis for adapting and extending the existing approach for assessing terrorist threats in urban transportation from the German research project "Risks and costs of terrorist threats to railbound public transportation" (RiKoV). In this context, the existing set of indicators for assessing the vulnerability of physical infrastructures is to be adapted and extended in order to be applicable to information technology environments as well. Experts from the public transportation sector are to be involved in this development process in order to develop a tool for information technology risk assessment and management that is as close-to-practice as possible.

CYBER THREAT AND INFORMATION SECURITY

Rail transport is an attractive and soft target for terrorist attacks (Strandberg 2013; Strandh 2017) due to its importance for the functioning of society and the economy (World Economic Forum 2016). The reason for this is, among other things, the comparatively simple availability of the necessary technical means of attack and the poor traceability to a specific attacker. This also makes cyber-attacks a potential tool for asymmetric warfare (Bens 2011). The following section therefore describes the threat to rail traffic from cyber-attacks by various attackers and the associated protection goals and risks.

Attacker types

The threats to rail transport posed by cyber-attacks can be manifold. Generally, cyber-attackers can be assigned to five categories:

a. Unsatisfied employees or other internal attacker (recruited for this purpose):
   - majority of cyber-attacks from the inside until 2001 (Diaz-Gomez et al. 2011; McLaughlin et al. 2016), since then increasing activity of external attackers (Nicholson et al. 2012)
   - threat can be much greater, since internal attackers have no barriers to pass/remain invisible, since they are legally present in the system
   - principle of perimeter protection is only partially applicable (Diaz-Gomez et al. 2011; Nicholson et al. 2012)

b. Governmental or state-affiliated organizations:
   - must overcome security barriers, which requires appropriate expertise, sufficient time, adequate financial/human resources
   - resources are available to an almost unlimited extent (Nicholson et al. 2012)
   - future conflicts may include cyber-war scenarios (Robinson et al. 2015), as cyber-attacks

allow to remain undetected/exploit ambiguities in international law (Bens 2011).

- usually have a political component

c. Cybercriminals:

- increasingly important factor (German Federal Office for Information Security 2016)
- typically based on enrichment intent (Robinson et al. 2015).
- scenarios typically include identity/data theft and selling of data as well as extortion - for example by data encryption.
- codes and exploits can either be self-developed with appropriate expertise or purchased
- development of dark web markets fosters the availability of tools for technically less skilled criminals (Persi Paoli et al. 2017)

d. Cyberterrorists:

- increased exchange between cybercriminals/cyberterrorists called Crime-Terror-Nexus (Makarenko 2012)
- favors the development/acquisition of expertise and secures the financing of terrorist groups
- European Police Office warns of growing threat from cyberterrorism, possibly accompanied by conventional terrorist attacks (European Police Office 2016)

e. Hacktivists and hobby hackers:

- no financial background/technical expertise for the acquisition/development of exploits
- fall back on freely available software/carry out largely automated attacks (Nicholson et al. 2012)
- can cause considerable damage (Baker 2008) if appropriate security measures are not in place

Protection goals

In order to ensure information security in computer systems, the three basic principles of confidentiality, integrity and availability must be guaranteed. These basic protection goals can be extended to include authenticity, accountability, non-repudiation and reliability of information. (Bedner and Ackermann 2010; Bless et al. 2005; Eckert 2014; DIN ISO/IEC 27000:2017)

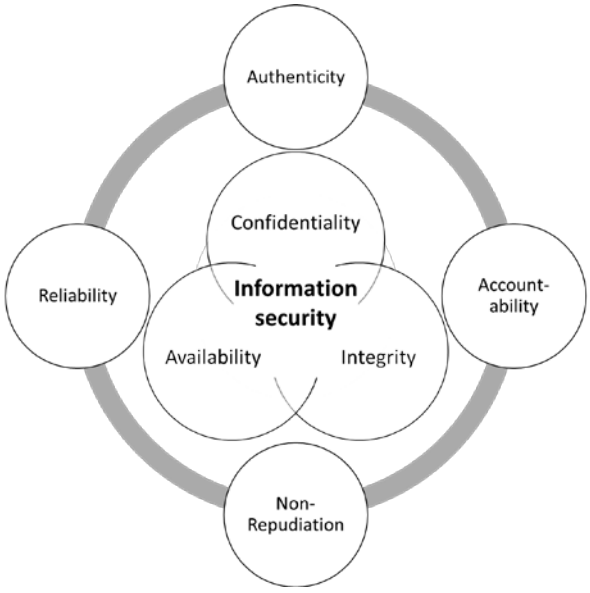


Figure 1. Basic and extended protection goals of information technology (Source: Author according to DIN ISO/IEC 27000:2017)

Table 1. Protection goals of information technology

Protection goal	Description
Confidentiality	making information accessible only to authorized and protecting it from unauthorized access
Integrity	assurance of authenticity/completeness of the particular values
Availability	usability of a subject/information by an authorized user at any time
Authenticity	ensuring that the information actually represents what it claims to be and the verifiability of it
Accountability	traceability of the responsibility for the origin and treatment of the information
Non-Repudiation	ability to prove events/trace them back to a place of origin without this being denied in retrospect
Reliability	ensuring that the intended behavior that triggers an information is consistent with the results

From a legal point of view, operators of CI in Germany are only obliged to take precautions to avoid disturbances of the availability, integrity, authenticity and confidentiality of their IT-systems to ensure the proper functioning of the CI (Section 8a (1). Law on the German Federal Office for Information Security). However, these precautionary measures are not specified; the concrete definition of protection goals is thus incumbent on the companies and is therefore part of each companies´ internal IT security policy. This gives companies the opportunity to define different levels of achievement and almost inevitably leads to different levels of security.

For application in the context of rail transport as CI, it can be assumed that compliance with the basic protection goals and the extended protection goals must always be demanded.

Threats and types of attacks

Information security is exposed to a variety of threats, each of which aims to compromise one or more of the aforementioned protection goals (Robinson et al. 2015). These threats to the protection goals can be divided into unintended threats from natural hazards, external influences or human error and intentional threats. The last form includes both active and passive cyber-attacks by the various attackers, as well as physical and combined forms of attacks that allow access to information technology.

This results in characteristic types of attacks with which the attacker's individual target is to be achieved through the impairment of one or more protection goals. In cyber-physical systems - such as rail traffic – the attack options can be divided into six different types according to Orojloo and Azgomi (2015):

a. Attacks against the truthfulness of the sensor data before it is read: e. g. manipulation of the sensor calibration or environmental parameters, so that the sensor delivers false data.

b. Attacks on the integrity of the measured or transmitted sensor data and control signals: e. g. manipulation of the communication between sensor and control unit or control unit and actuator, so that the transmitted data are modified.

c. Attacks on the availability of sensor data and control signals: e. g. flooding with requests, so that the sensor or control unit is overloaded.

d. Attacks on the control instructions: e. g. exchanging the instructions of the control unit so that it contains incorrect limit values.

e. Attack on the human-machine interface: e. g. manipulation of the operator display so that the operator makes a faulty decision.

f. Combined attacks: all the above-mentioned attack types can be combined and varied almost arbitrarily.

Further classification approaches differentiate between the attacked or affected domains in physical and cyber-side (Orojloo and Azgomi 2015). All types of attacks have in common that the attacker must have acquired a very detailed knowledge of the physical-technical and IT processes, protocols and interfaces in the attacking system to execute his attack successfully.

The threat of cyber-attacks poses various risks to a railway transport operator. Successful cyber-attacks can lead to considerable financial losses and damage to the companies´ image (German Federal Office for Information Security 2016; Nicholson et al. 2012). Most serious, however, are possible physical effects, which can be caused by a cyber-attack (Robinson et al. 2015).

INTRODUCTION TO THE ERTMS

One of the European Union's political objectives is the creation of trans-European rail networks which form the basis of the European Rail Traffic Management System (ERTMS). The ERTMS consists of four main components: the train communication system *Global-System for Mobile Communication-Railway* (GSM-R), the train control system *European Train Control System* (ETCS), the traffic management system *European Traffic Management Layer* (ETML) and the *Integrated European Signaling System* (INESS). However, the implementation of these sub-components has progressed to varying degrees so far (European Commission 2006).

GSM-R train communication system

GSM-R is largely based on the established mobile communications standard GSM. As the GSM network is only to be supported by network operators until 2030, efforts to develop a successor standard are currently being intensified (International Union of Railways 2016).

The GSM-R network is a cellular network, whereby the radio cells can have different geographical dimensions due to radio field attenuation and for capacity reasons. Usually they range from 7-15 km along the railway tracks (He et al. 2016) whereas in tunnels, they are usually reduced to 1-2 km (Kastell et al. 2006). The radio cells are uniquely identifiable. In addition to the features and specifications available in the public GSM network, the GSM-R network has a number of additional requirements, which take into account the special demands of rail traffic. The architecture of the GSM-R network is thus very similar to that of the GSM network and has only been extended by a few components (Winter 2009). General information regarding GSM architecture and functionality can be found in Eckert (2014) and Ruesche et al. (2008).

The GSM-R network and the network subscribers are protected by two essential security mechanisms: Network authentication and encryption of communication. A uniquely assigned subscriber identity module (SIM) is required for each handset in order to take part in the GSM-R network. Each handset is additionally uniquely identifiable via a device number. If a handset tries to establish a connection to the network, a personal identification number must be entered, and the device number must be registered as valid. The handset is then identified using a challenge-response procedure. (International Union of Railways 2015; Sorge et al. 2013; Winter 2009) This challenge-response procedure uses various keys, some of which are transmitted in plain text via the air interface. Once the connection is established, the communication is encrypted with a 64 bit key. (Eckert 2014)

Pre-computed tables allow the keys to be broken within a few minutes, especially since the keys are partially used for several days and 64-bit encryption is no longer a sufficient protection for the computing power available today (Barkan et al. 2008; Nohl und Paget 2009). This vulnerability also offers the possibility of "hijacking" the attacked handset, i. e. redirecting the data traffic destined for a handset (Barkan et al. 2008; Golde et al. 2013). Physical access to the SIM opens up numerous other possibilities for side-channel attacks, including cloning of the SIM (Brienco et al. 1998; Pagliusi 2002; Rao et al. 2002).

Since only one-way authentication of the handset takes place on the network, but not vice-versa, base stations can be imitated in an unauthorized manner (Eckert 2014; Sorge et al. 2013). The cryptographically unprotected backbone as well as the signaling channel and the update over the air (OTA) function lead to further shortcomings (International Union of Railways 2015; Sorge et al. 2013). Like all wireless networks, GSM-R is exposed to the threat of intentional jamming, parallel to the already existing frequency overlaps and bottlenecks in channel availability (He et al. 2016; Lindström 2012; Mili et al. 2013; Ruesche et al. 2008; Sniady and Soler 2012).

European Train control system (ETCS)

To improve the interoperability of trains, it is intended to replace the 20 different national train control systems throughout Europe with one ETCS. The ETCS also consists of several components, which can be differentiated into track-side and on-board infrastructure. Both components communicate with each other via air interfaces and will be implemented in three levels. The track-side infrastructure comprises the radio block centers (RBC) connected via GSM-R, which monitor the position of trains and form the interface to the interlockings issuing the movement authorities. These movement authorities are transmitted to the train´s ETCS on-board computer via beacons in the tracks or via GSM-R (Winter 2009).

Since security-relevant data, such as movement authorities, are transmitted via the ETCS, the integrity and authenticity of this data is especially sensitive. Therefore, this data is particularly protected by a cryptographic message authentication code. For this purpose, the triple data encryption standard is used in block cipher mode according to ISO 9797-1 MAC Algorithm 3 (ISO/IEC 9797-1). The keys required for this are generated in a key management center and brought to the handsets by couriers on physical storage devices (DB Netz AG 2014). In order to register a train, these keys must be exchanged between the handset and RBC using a challenge-response method with pseudo-random numbers. The connection is also encrypted after establishment, only emergency messages are excluded from this procedure. In order to make messages distinguishable in the ETCS, they receive a time stamp and sometimes require an acknowledgement of receipt. (Chothia et al. 2017; DB Netz AG 2014; European Railway Agency et al. 2016a; Ruiter et al. 2016; Union Industry of Signalling 2015a, 2015c; Winter 2009)

The transmission of messages from the beacons in the track can also be safety-relevant, so that these should be secured. Each beacon has an individual number and "knows" its successor beacon. This information is transmitted by induction when passing over the beacon. (European Railway Agency et al. 2016b; Union Industry of Signalling 2015b)

In addition to the security issues in the GSM-R network, shortcomings can also be found in the ETCS. Although the triple data encryption standard is still considered relatively secure, an attacker could search for collisions in the message authentication codes and thus deduce the key. Since the algorithm CBC-MAC is based on a 3DES encryption and this encryption uses three different keys KS1, KS2 and KS3, of which KS1 is used in each DES encryption round, in combination with the knowledge that two messages in EURORADIO with the same MAC have the same input for the last 3DES block, a conclusion can now be drawn for KS1. In a conceptual proof, it has already been shown that forged movement authorities can be sent to the train that it accepts. Since the emergency messages are not protected it is possible to use faked emergency messages to induce unintentional emergency braking (Chothia et al. 2017).

Furthermore, the pseudo-random numbers used to establish the connection are a possible starting point for attacks. If the random number generator is not cryptographically secure, the number generated by it can be calculated in advance if necessary, thus establishing an impermissible connection to the train, in which the attacker acts like an RBC, since the random numbers of train and RBC are transmitted at least once in plain text (Lopez and Aguado 2015).

The systematics of the key distribution by physical data carrier makes it particularly susceptible to social engineering. Since the keys are delivered manually on a physical data carrier, distributing the keys to the individual trains is correspondingly cumbersome and time-consuming. This can result in railway companies using few keys for large train fleets in order to reduce the effort. Furthermore, the use of a key over a longer period of time is favored by the complex procedure (DB Netz AG 2014; Lopez and Aguado 2015).

The introduction of the time stamp is intended to prevent a message from being sent multiple times, but the procedure is only used after the connection has been established, not during this process, so that it remains vulnerable to replay attacks. Furthermore, the recipient of a message must decrypt it first and check the MAC before the correctness of the attached time stamp can be checked. This could serve as a possible starting point for an attack with the aim of compromising availability. For this purpose, old messages can be resent that would be rejected by the system but increase workload, possibly resulting in system performance limitations. The messages do not have to be decrypted by the attacker, as their content is of no interest in this case, which is why EURORADIO does not offer a protective function. The only protection against this form of attack consists only of GSM-R encryption, which - as shown in the previous section - can be broken comparatively easily (Lopez and Aguado 2015).

Other forms of attack are physical replacement or modification of beacons or - since the ETCS depends on the GSM-R network - intentional jamming of the network (Mili et al. 2013).

European Train Management Layer ETML and signaling system INESS

The ETML aims to standardize the interfaces between railway companies so that the exchange of operational

data is possible, especially for cross-border train connections. The system will allow data to be shared between participating railway undertakings in terms of position, expected schedule, delay information and reasons, and estimated arrival times. These data are sent directly from the respective national operations centers to ETML headquarters in Vienna/Austria. The prepared data is available for all railway companies through a web interface via virtual private network access after registration (Winter 2009).

The aim of the INESS is to develop a uniform data format and a standard of requirements for interlocking systems. Since the interlocking transmits movement authorities via the RBC to the trains, controls the track switches or establishes direct communication with the drivers via GSM-R, the interlocking is highly security-relevant. The interlocking computer forms the interface between the dispatcher and the track-side ETCS equipment and RBC and consists of two independently operating computers (Deutsche Bahn AG 2016). They process the data entered by the dispatcher and pass their results on to a comparator, which checks whether the results match, after which the safety-relevant switching process is carried out. The display on the screens is also generated and calibrated by two computers. If there is no match, the display starts flashing and shows the lack of signal security. In addition, a second configuration with two computers or more computer is provided as hot standby (Fendrich and Fengler 2013; Maschek 2013).

Since INESS-compliant interlockings are still in development, it is only possible to draw general conclusions on security issues. In addition to the susceptibility to attacks by means of social engineering, attacks by introducing infected hardware - also by insiders - are conceivable. Attacks can also directly target the integrity and authenticity of the circuit diagrams displayed, the forwarding of switching commands and, last but not least, the availability of the entire interlocking system (Gordeychik und Timorin 2015).

CRITICALITY ASSESSMENT

The vulnerabilities described in the previous sections must be evaluated with regard to their criticality in a subsequent step using criteria. These criteria must be developed in close consultation with information technology experts and with the public transportation authorities. The intended methodology is based on a methodology developed as part of the RiKoV research project. Within the framework of RiKoV, a methodology for scenario-based vulnerability and risk assessment of terrorist threats was developed at the Cologne University of Applied Sciences in cooperation with the Karlsruhe Institute of Technology (Brauner 2017). This methodology will be briefly introduced in the following section.

INTRODUCTION OF THE RIKOV METHOD

Vulnerability in RiKoV is determined using a semi-quantitative approach, which evaluates the effect of preventive security measures according different scenarios and the hazard category of the target object. These two factors then determine the scenario-specific vulnerability of a target in a public transportation system.

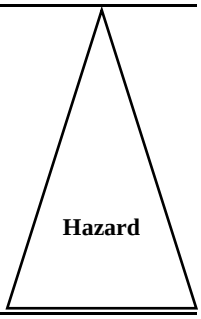
This approach has been designed in order to be applicable to different target objects, which makes it suitable for a transfer into this research. The system to be considered was defined with its direct environment as an observation space and evaluated for the four aspects of performance, structure, environment and time with a number of indicators.

These indicators can be rated with one to three points each and then add up to a risk score. This score is between the minimum of 11 and the maximum of 33 points (cf. Table 2) and will then be ranked in one of seven hazard categories using Table 3, whereby category 1 is the highest hazard category and category 7 the lowest. The numerical value of the hazard category is then used in a formula to calculate the vulnerability of the target object in combination with the qualitative effectiveness of selected preventive security measures in the environment (Brauner et al. 2014).

Table 2. Indicators for the determination of hazard categories (Brauner et al. 2014)

Aspect	Hazard indicator	Score		
		1	**2**	**3**
Performance	Number of travelers (per day)	Low	Medium	High
	Number of trains in service	Low	Medium	High
Composition	Number of floors	1 floor	2 floors	>2 floors
	Tunnels	Non-Existence	-	Existence
	Bridges	Non-Existence	-	Existence
	Geographic peculiarities (river, mountain, …)	None	-	Existence
	Supply facilities (electricity, consumables, …)	None	-	Existence
Environment	Special buildings with symbolic effect (cultural, political, religious)	None	-	Existence
	Direct airport connection (area proximity)	None	-	Existence
	Local attack relevance (official warnings, assessments by Federal Agencies)	None	Medium	High
Time	Major events (high fluctuation in the number of travelers)	None	Rare	Frequent
	Total score:	**Min./Max.: 11/33 points**		

Table 3. Hazard categories (Brauner et al. 2014)

Hazard category	Total score	Hazard
7	11 – 13	
6	14 – 16	
5	17 – 19	
4	20 – 22	
3	23 – 25	
2	26 – 29	
1	30 – 33	

Since the RiKoV approach presented above with its indicators only refers to physical infrastructures, it is necessary to develop a new set of indicators for assessing the vulnerability of information technology systems. This forthcoming work will be carried out in consultation with public transport operators and information security experts. The results of the literature research presented in this paper and the deficiencies found in ERTMS provide the necessary theoretical basis for such research.

CONCLUSION AND OUTLOOK

The authors demonstrate that, although numerous security measures have been implemented in the ERTMS, there are still some security problems and correspondingly vital threats to the protection targets. These have so far only been investigated separately and not yet described for the entire ERTMS. The extension and adaptation of the current RiKoV approach will therefore be a first step towards a comprehensive systemic vulnerability assessment for cyber-attacks on the ERTMS.

When developing a set of indicators, it should be noted that the selected criteria can provide a holistic picture of vulnerability and that the weighting takes into account the needs of end-users. In addition, the evaluation of the security flaws identified in this paper has to be carried out by experts in a real application-scenario and corresponding ambiguities need to be clarified in a panel discussion among experts. The practical application on the basis of a real example, taking into account the existing security measures, may be considered in cooperation with the Cologne Public Transportation Services.

REFERENCES

Baker, Graeme (2008): Schoolboy hacks into city's tram system. In: *The Telegraph*, 11.01.2008 (Online). Available online at: http://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html, checked on 08.08.2017.

Bambauer, Derek E. (2014): Ghost in the Network. In: *University of Pennsylvania Law Review* 162 (5), S. 1011–1091. Available online at: http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=9439&context=penn_law_review, checked on 03.08.2017.

Barkan, Elad; Biham, Eli; Keller, Nathan (2008): Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication. In: *J Cryptol* 21 (3), S. 392–429.

Bedner, Mark; Ackermann, Tobias (2010): Schutzziele der IT-Sicherheit. In: *Datenschutz und Datensicherheit - DuD* 34 (5), S. 323–328, checked on 14.08.2017.

Bens, Jonas (2011): Cyberwar und völkerrechtliches Selbstverteidigungsrecht. Überlegungen zum Begriff des bewaffneten Angriffs bei Attacken im Cyberspace. In: *Bonner Rechtsjournal* (2), S. 149–155. Available online at: http://bonner-rechtsjournal.de/fileadmin/pdf/Artikel/2011_02/BRJ_149_2011_Bens.pdf, checked on 07.08.2017.

Bless, Roland; Mink, Stefan; Blaß, Erik-Oliver; Conrad, Michael; Hof, Hans-Joachim; Kutzner, Kendy; Schöller, Marcus (2005): Sichere Netzwerkkommunikation. Grundlagen, Protokolle und Architekturen. Berlin, Heidelberg: Springer-Verlag Berlin Heidelberg (X.systems.press)). Available online at: http://site.ebrary.com/lib/alltitles/docDetail.action?docID=10182929.

Brauner, Florian (2017): Securing Public Transportation Systems. Wiesbaden: Springer Fachmedien Wiesbaden.

Brauner, Florian; Baumgarten, Christian; Bentler, Christian; Kornmayer, Tobias; Lotter, Andreas; Lechleuthner, Alexander M.; Mudimu, Ompe A. (2014): Methode zur Bestimmung der Vulnerabilität eines schienengebundenen ÖPV-Systems. Interner Projektbeitrag zum AP4.1. Fachhochschule Köln. Köln, checked on 15.01.2017.

Brienco, Marc; Goldberg, Ian; Wagner, Dave (1998): GSM Cloning. Smart Card Developers Association; University of California, Berkeley. Berkeley, Calif. Available online at: http://www.isaac.cs.berkeley.edu/isaac/gsm-faq.html, zuletzt aktualisiert am 01.09.1999, checked on 08.09.2017.

Chothia, Tom; Ordean, Mihai; Ruiter, Joeri de; Thomas, Richard J. (2017): An Attack Against Message Authentication in the ERTMS Train to Trackside Communication Protocols. In: Ramesh Karri, Ozgur Sinanoglu, Ahmad-Reza Sadeghi und Xun Yi (Hg.): Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security - ASIA CCS '17. the 2017 ACM. Abu Dhabi, United Arab Emirates, 02.04.2017 - 06.04.2017. New York, New York, USA: ACM Press, S. 743–756.

DB Netz AG (Hg.) (2014): European Train Control System (ETCS) bei der DB Netz AG. Die Basis der Zukunft. Frankfurt am Main, checked on 24.08.2017.

Deutsche Bahn AG (2016): Vom Stellhebel zum Mausklick: Wie die Bahn in ihrem Schienennetz täglich 40.000 Züge steuert. Frankfurt am Main. Available online at: http://www.deutschebahn.com/presse/duesseldorf/de/hintergrund/themenschwerpunkte/10177168/201507_Themendienst_Stellwerke.html, zuletzt aktualisiert am 10.02.2016, checked on 05.10.2017.

Diaz-Gomez, Pedro A.; ValleCarcamo, Gilberto; Jones, Douglas (2011): Internal Vs. External Penetrations: A Computer Security Dilemma. In: Hamid R. Arabnia, Michael R. Grimaila, George Markowsky und Selim Aissi (Hg.): Proceedings of the 2011 International Conference on Security & Management, SAM 2011. [affiliated with] WORLDCOMP'11; July 18 - 21, 2011, Las Vegas, Nevada, USA. Unter Mitarbeit von Leonidas Deligiannidis und Ashu M. G. Solo. S.l.: CSREA Press, S. 59–64, checked on 07.08.2017.

Eckert, Claudia (2014): IT-Sicherheit. Konzepte - Verfahren - Protokolle. 9., aktualisierte Aufl. Berlin: De Gruyter Oldenbourg. Available online at: http://www.degruyter.com/search?f_0=isbnissn&q_0=9783486859164&searchTitles=true.

European Commission (2006): ERTMS - delivering flexible and reliable rail traffic. A major industrial project for Europe. Luxembourg: Office for Official Publ. of the European Communities.

European Police Office (Europol) (2016): IOCTA 2016. The Internet Organised Crime Threat Assessment. Den Haag, checked on 08.08.2017.

European Railway Agency (ERA); Union Industry of Signalling (UNISIG); European Economic Interest Group ERTMS Users Group (EEIG ERTMS USERS GROUP) (2016a): System Requirements Specification. Chapter 3 Principles Subset-026-3 Issue 3.6.0. o.O.

European Railway Agency (ERA); Union Industry of Signalling (UNISIG); European Economic Interest Group ERTMS Users Group (EEIG ERTMS USERS GROUP) (2016b): System Requirements Specification. Chapter 8 Messages Subset-026-8 Issue 3.6.0. o.O.

Fendrich, Lothar; Fengler, Wolfgang (Hg.) (2013): Handbuch Eisenbahninfrastruktur. 2., neu bearbeitete Auflage. Berlin, Heidelberg: Springer Vieweg. Available online at: http://dx.doi.org/10.1007/978-3-642-30021-9.

German Federal Office for Information Security (BSI) (Hg.) (2016): The State of IT Security in Germany 2016. German Federal Office for Information Security (BSI). Bonn. Available online at: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2016.pdf?__blob=publicationFile&v=3, checked on 04.08.2017.

Golde, Nico; Redon, Kévin; Seifert, Jean-Pierre (2013): Let Me Answer That For You: Exploiting Broadcast Information in Cellular Networks. In: Sam King (Hg.): 22nd USENIX Security Symposium. August 14 - 16, 2013, Washington, D. C. 22nd USENIX Security Symposium. Washingtion D.C., 14.-16.08.2013. USENIX Association; USENIX Security Symposium. Berkeley, Calif.: USENIX Association, S. 33–48. Available online at: https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_golde.pdf, checked on https://www.usenix.org/system/files/conference/usenixsecurity13/sec13-paper_golde.pdf.

Gordeychik, Sergey; Timorin, Aleksandr (2015): The Great Train Cyber Robbery. SCADA StrangeLove. Chaos Computer Club e. V. Hamburg, 27.12.2015. Available online at: https://events.ccc.de/congress/2015/Fahrplan/events/7490.html, checked on 05.10.2017.

He, Ruisi; Ai, Bo; Wang, Gongpu; Guan, Ke; Zhong, Zhangdui; Molisch, Andreas F. et al. (2016): High-Speed Railway Communications. From GSM-R to LTE-R. In: *IEEE Veh. Technol. Mag.* 11 (3), S. 49–58.

ISO/IEC 9797-1, 01.03.2011: Information technology — Security techniques — Message Authentication Codes (MACs) — Part 1: Mechanisms using a block cipher.

DIN ISO/IEC 27000:2017, Oktober 2017: Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Überblick und Terminologie, checked on 25.01.2018.

International Union of Railways (UIC) (2015): EIRENE System Requirements Specification. Version 16.0.0. Unter Mitarbeit von GSM-R Functional Group. Paris, checked on 07.09.2017.

International Union of Railways (UIC) (2016): Future Railway Mobile Communication System. User Requirements Specification Version 2.0. Unter Mitarbeit von FRMCS Functional Working Group. Paris.

Karnouskos, Stamatis (2011): Stuxnet worm impact on industrial cyber-physical system security. In: IECON 2011 - 37th Annual Conference of the IEEE Industrial Electronics Society. IECON 2011 - 37th Annual Conference of IEEE Industrial Electronics. Melbourne, Vic, Australia, 07.11.2011 - 10.11.2011: IEEE, S. 4490–4494.

Kastell, K.; Bug, S.; Nazarov, A.; Jakoby, R. (2006): Improvments in Railway Communication via GSM-R. In: 2006 IEEE 63rd Vehicular Technology Conference. 2006 IEEE 63rd Vehicular Technology Conference. Melbourne, Australia, 07-10 May 2006: IEEE, S. 3026–3030.

Khan, Rafiullah; McLaughlin, Kieran; Laverty, David; Sezer, Sakir (2016): Threat Analysis of BlackEnergy Malware for Synchrophasor based Real-time Control and Monitoring in Smart Grid. In: 4th International Symposium for ICS & SCADA Cyber Security Research 2016. 4th International Symposium for ICS & SCADA Cyber Security Research 2016, 23-25 August 2016: BCS Learning & Development (Electronic Workshops in Computing).

Lakshminarayana, Subhash; Teo, Zhan-Teng; Tan, Rui; Yau, David K. Y.; Arboleya, Pablo (2016): On False Data Injection Attacks Against Railway Traction Power Systems. In: 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). 2016 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN). Toulouse, France, 28.06.2016 - 01.07.2016: IEEE, S. 383–394.

Lindström, Gustaf (2012): Is GSM-R the limiting factor for the ERTMS system capacity? Master thesis. KTH Royal Institute of Technology, Stockholm. School of Architecture and the Built Environment, checked on

15.09.2017.

Lopez, Igor; Aguado, Marina (2015): Cyber security analysis of the European train control system. In: *IEEE Commun. Mag.* 53 (10), S. 110–116.

Makarenko, Tamara (2012): Europe's crime-terror nexus. Links between terrorist and organised crime groups in the European Union : study. Luxembourg: EUR-OP (Study/EP, PE 462.503).

Maschek, Ulrich (2013): Sicherung des Schienenverkehrs. Grundlagen und Planung der Leit- und Sicherungstechnik. 2., überarb. u. erw. Aufl. 2013. Dordrecht: Springer. Available online at: http://gbv.eblib.com/patron/FullRecord.aspx?p=1317753.

McLaughlin, Stephen; Konstantinou, Charalambos; Wang, Xueyang; Davi, Lucas; Sadeghi, Ahmad-Reza; Maniatakos, Michail; Karri, Ramesh (2016): The Cybersecurity Landscape in Industrial Control Systems. In: *Proc. IEEE* 104 (5), S. 1039–1057.

Mili, S.; Sodoyer, D.; Deniau, V.; Heddebaut, M.; Philippe, H.; Canavero, F. (2013): Recognition Process of Jamming Signals Superimposed on GSM-R Radiocommunications. In: International Symposium on Electromagnetic Compatibility (EMC Europe), 2013. 2 - 6 Sept. 2013, Brugge, Belgium. Piscataway, NJ: IEEE, 45-50.

Nicholson, A.; Webber, S.; Dyer, S.; Patel, T.; Janicke, H. (2012): SCADA security in the light of Cyber-Warfare. In: *Computers & Security* 31 (4), S. 418–436, checked on 04.08.2017.

Nohl, Karsten; Paget, Chris (2009): GSM - SRSLY? 26th Chaos Communication Congress. Chaos Computer Club e. V. Berlin, 27.12.2009. Available online at: https://events.ccc.de/congress/2009/Fahrplan/events/3654.en.html, checked on 04.08.2017.

Orojloo, Hamed; Azgomi, Mohammad Abdollahi (2015): Evaluating the complexity and impacts of attacks on cyber-physical systems. In: 2015 CSI Symposium on Real-Time and Embedded Systems and Technologies (RTEST). 2015 CSI Symposium on Real-Time and Embedded Systems and Technologies (RTEST). Tehran, Iran, 07.10.2015 - 08.10.2015: IEEE, S. 1–8.

Pagliusi, Paulo S. (2002): A Contemporary Foreword on GSM Security. In: George Davida, Yair Frankel und Owen Rees (Hg.): Infrastructure Security. International Conference, InfraSec 2002 Bristol, UK, October 1-3, 2002 Proceedings. Berlin, Heidelberg: Springer (Lecture Notes in Computer Science, 2437), S. 129–144.

Persi Paoli, Giacomo; Aldridge, Judith; Ryan, Nathan; Warnes, Richard (2017): Behind the curtain: The illicit trade of firearms, explosives and ammunition on the dark web. RAND Corporation. Santa Monica, Calif., Cambridge, UK, checked on 08.08.2017.

Rao, J. R.; Rohatgi, P.; Scherzer, H.; Tinguely, S. (2002): Partitioning attacks. Or how to rapidly clone some GSM cards. In: Proceedings 2002 IEEE Symposium on Security and Privacy. 2002 IEEE Symposium on Security and Privacy. Berkeley, CA, USA, 12-15 May 2002: IEEE Comput. Soc, S. 31–41.

Robinson, Michael; Jones, Kevin; Janicke, Helge (2015): Cyber warfare. Issues and challenges. In: *Computers & Security* 49, S. 70–94.

Ruesche, S.; Steuer, J.; Jobmann, K. (2008): The European Switch. In: *IEEE Veh. Technol. Mag.* 3 (3), S. 37–46.

Ruiter, Joeri de; Thomas, Richard J.; Chotia, Tom (2016): A Formal Security Analysis of ERTMS Train to Trackside Protocols. In: Thierry Lecomte, Ralf Pinger und Alexander Romanovsky (Hg.): Reliability, Safety, and Security of Railway Systems. Modelling, Analysis, Verification, and Certification. First International Conference, RSSRail 2016, Paris, France, June 28-30, 2016, Proceedings. Cham, s.l.: Springer International Publishing (Lecture Notes in Computer Science, 9707).

Settanni, Giuseppe; Skopik, Florian; Shovgenya, Yegor; Fiedler, Roman; Carolan, Mark; Conroy, Damien et al. (2017): A collaborative cyber incident management system for European interconnected critical infrastructures. In: *Journal of Information Security and Applications* 34, S. 166–182.

Sniady, Aleksander; Soler, Jose (2012): An overview of GSM-R technology and its shortcomings. In: 2012 12th International Conference on ITS Telecommunications. 2012 12th International Conference on ITS Telecommunications (ITST). Taipei, Taiwan, 05.11.2012 - 08.11.2012: IEEE, S. 626–629.

Sorge, Christoph; Gruschka, Nils; Lo Iacono, Luigi (2013): Sicherheit in Kommunikationsnetzen. München: Oldenbourg. Available online at: http://www.degruyter.com/search?f_0=isbnissn&q_0=9783486720174&searchTitles=true.

Strandberg, Veronica (2013): Rail bound traffic—a prime target for contemporary terrorist attacks? In: *J Transp Secur* 6 (3), S. 271–286.

Strandh, Veronica (2017): Exploring vulnerabilities in preparedness – rail bound traffic and terrorist attacks. In: *J Transp Secur* 7 (3), S. 1–18.

Union Industry of Signalling (UNISIG) (2015a): EuroRadio FIS. Subset-037 Issue 3.2.0. o.O.

Union Industry of Signalling (UNISIG) (2015b): FFFIS for Eurobalise. Subset-036 Issue 3.1.0. o.O.

Union Industry of Signalling (UNISIG) (2015c): KMC-ETCS Entity Off-line KM FIS. Subset-114 Issue 1.1.0. o.O.

Volz, Dustin; Auchard, Eric (12.05.2017): More disruptions feared from cyber attack; Microsoft slams government secrecy. Washington D.C., Frankfurt am Main. Thomson Reuters. Available online at: http://www.reuters.com/article/us-britain-security-hospitals-idUSKBN18820S, checked on 03.08.2017.

Winter, Peter (Hg.) (2009): Compendium on ERTMS, European Rail Traffic Management System. International Union of Railways (UIC). 1. ed. Hamburg: DVV Media Group Eurailpress.

World Economic Forum (Hg.) (2016): Understanding Systemic Cyber Risk. World Economic Forum. Cologny/Geneva (White Paper). Available online at: http://www3.weforum.org/docs/White_Paper_GAC_Cyber_Resilience_VERSION_2.pdf, checked on 04.08.2017.