

NATIONAL UNIVERSITY OF PUBLIC SERVICES

PÉTER VARGA

Official and author's review of PhD thesis titled

***Protecting Wireless Networks
of the Critical Information Infrastructures***

Scientific advisor:

Prof. Dr. Zsolt HAIG

Budapest
2012

The scientific problem

Wireless networks provide new type attack target for the elements of information systems of critical infrastructures namely the critical information infrastructures. Interdependencies – from the vantage point of wireless networks– between critical information infrastructures and its wireless network components are not or just partially known. In addition, the relationship between the wireless infrastructures of critical and other non-critical infrastructures, and between infocommunications technology endpoints which use wireless technology, and the relations between other portable devices. It also necessary to study possible attack vectors why (?) have not been identified.

It is essential from the from the critical information infrastructures perspective to identify attack or target for medium models to the wireless network. It is also possible to design effective defence only if attack models and attack methods are known, attack and defence models of wireless network to be identified and matched. The efficiency, effectiveness considerations of defence, however, should be supplemented with new standpoints to make it rational for cost-sensitive business actors to implement adequate defence.

Up to now defence and attack were studied, evaluated and analysed domains. Several standards and methodologies can be found on these questions. However, each of them focuses only the aspects of defence or attack. The relevant published references did not connect attack and defence methods in an itemised way. The second problem with the open methodologies is that they are imposing economic, technological and competence requirements to which medium size organisations cannot fully meet. The large number of wireless endpoints, however, involves threats not only to their operators. These endpoints may serve indirectly as a starting point for anonymous attacks, which increases the threat to critical information infrastructures. It is necessary to clarify which technical, administrative, or possibly legislative means could increase the defense potential of wireless networks without creating a disproportionate burden for lay operators.

Aims of research

During my research in the field of wireless networks security used in critical information infrastructures the following objectives were determined:

1. Examine internal and external dependencies of the critical information infrastructures. Create a structured model of assessing and analysing the essential attributes of the inter- and intradependencies connections of the critical information infrastructures.
2. Analyze and classify technologies and technical requirements of wireless networks used in critical information infrastructures, and based on this survey discover the possible attack routes.
3. Develop a structured and integrated approach of attack and defence theory and practice of the wireless networks of critical information infrastructures, and based on this correlate attack methods and defense controls.
4. Recommend a method for securing the endpoints of the wireless networks, including the general measures and criteria in the light of the attack and defence taxonomies.
5. Develop a wireless network penetration test method, based merely on cell phones. This method –combined with similar computer based tests– by itself allows for critical information infrastructure IT operators 24/7 wireless network testing.

Applied research methods

During my research I performed a wide range literature exploration, studying both national and international literature. I performed applied research to discover the special features of the domestic installations of wireless networks. I created models to explore the characteristics of inter- and intradependencies of the critical infrastructures. I continuously tested the acquired knowledge in my practice as an IT engineer. I attended regularly –as a member of the audience or a speaker– the related national and international scientific conferences and other proceedings. I presented the results of my research in a number of scientific conferences at

home and abroad, both in Hungarian and in English. I published my findings not only in conferences but also in peer-reviewed journals.

Structure of the thesis

I split my thesis into three chapters:

Chapter 1: In this chapter I present an overview of the concepts of infrastructure, critical infrastructure and critical information infrastructure and wireless networking. I analyse internal and external relationships of the critical information infrastructures, and I also define their inter- and intradependency model.

Chapter 2: In this chapter –based on my measurements– I analyse and investigate the wireless networking technologies used in critical information infrastructures, identifying the associated technical requirements, and based on these studies I show the possible attack routes.

Chapter 3: In this chapter I analyse the attack methods and defence measures of the critical information infrastructure. I also take into consideration the attacker's identity, objective and motivation. In my lab environment I test and confirm the attack methods and steps described in professional references. Based on these details I matched attack methods and defence controls. Based on defence methodologies I developed an integrated method for the wireless networks of the critical information infrastructures. I developed a wireless network penetration test method, based merely on cell phones. This method is a fundamental element of network security sustainability.

Conclusions

IT devices and connecting networks play increasing role in our ordinary life. It is very difficult to find an area where networked IT devices were not used as a tool to enhance or control works. In the domain of critical information infrastructures the adequate computer network connections are essential providing sound operation. Based on my measurements I proved that besides traditional wired network connections the wireless network solutions – notably devices categorised under IEEE 802.11 standard– play an important role in critical information infrastructure. By integrating wireless network segments into critical information infrastructure, operators opened a new attack surface. Because of this, I felt it necessary to

study the impact of possible malfunctions of wireless networks to critical information infrastructures, and as a spreading result through to other critical information infrastructures. Therefore, I created a complex model which enables to assess and analyse inter-and intradependencies of critical information infrastructures, and also makes it possible to analyse the content of relationships on both micro and macro level. Based on this model, I demonstrated that wireless network infrastructure can be interpreted as a special sub-infrastructure, and it is also possible analyse it as such in every critical information infrastructure. This model opens new way for further research that could improve understanding and analysis of inter-and intradependencies of critical infrastructure and critical information infrastructure.

I study wireless network segments since 2004, examining the applied technology, devices and the proliferation of such wireless technology. My latest comprehensive study mainly focused on critical information infrastructures. From the test results I highlighted three critical information infrastructure, and found that they use heterogeneous network and security solutions. This heterogeneity makes these infrastructures vulnerable, and therefore I explored the possible attack paths which either directly or indirectly –via the wireless network– threaten the security of critical information infrastructure.

The current professional references consider protection and attack of wireless networks as independent and not directly connected problems. Of course there are responses to individual (single) attacks, but they are not currently not establishing a coherent system. Therefore, I considered it important to build a unified taxonomy, which focuses not only on wireless network attack or defence standpoints but maps all significant attacks to the counteracting controls that reducing probability and/or effect of such strikes with appropriate measures. In a test environment I examined the most commonly used attacks methods. I came to the conclusion that –in case of poorly protected networks– a large percentage of attacks are feasible with little expertise and low cost, so they are potential hazard for wireless network of critical information infrastructure. My studies also proved that both Enterprise and SOHO wireless network devices are used in critical information infrastructures. Enterprise network security devices are armoured with a lot more security functions than a networks built from traditional SOHO devices. The method I developed can be used in both environments, on the stipulation that the steps of protective actions used in best possible way, relative to the capabilities of the defended network. I recommend the implementation of this method to all critical information infrastructure operator or security manager as a kind of minimum security requirements applicable to wireless networks.

Based on my research and relevant sections of the professional references I developed a complex method to describe attacks and defence theory and practice of wireless networks of critical information infrastructures, mapping wireless networks attack techniques to security controls. This method provides guidance to infrastructure operators how to apply a series of measures mapped to attacks to enhance wireless network security.

With the development of information and communication technology the computing power, storage capacity, and greatly expanded functionalities of mobile phones also improved. Capabilities of recent smartphones challenging the capabilities of desktop/laptop computers. In my dissertation, I developed merely smartphones based method for wireless penetration testing, which is methodological summary of current Android applications.

The development has a dual objective: In one hand, to prove mobile threats reality against wireless networks, and to show how much information can be collected about wireless networks using only a cell phone and free applications. On the other hand, the objective of such method development is to provide a practical, simple to use guideline. This guideline could be used by IT staff responsible for managing and/or monitoring critical information infrastructures to assess wireless network vulnerability. The method what I developed based on open source and freely available software, and therefore target systems can be checked at any time and anywhere cost effectively.

New scientific achievements of the thesis

The research work and studies of new scientific results, consider the following:

1) I created a structured model of assessing and analysing the essential attributes of the inter- and intradependencies connections of the critical information infrastructures. This model is suitable for demonstrating in an integrated way the internal dependencies within a critical information infrastructure, and the external dependencies between two or more critical information infrastructures. This model also appropriate for inter- and intradependency risk assessment.

2) Based on theoretical requirements and test results I defined all attack routes that incorporating wireless networks against critical information infrastructures.

3) I developed a structured and integrated approach of attack and defence theory and practice of the wireless networks of critical information infrastructures, and based on this I correlated attack methods and defence controls.

4) Based on the attack and defence taxonomies I recommended a method for securing the endpoints of the wireless networks of critical information infrastructures.

5) I developed a wireless network penetration test method, based merely on cell phones. This method –combined with the similar computer based tests– by itself allows for critical information infrastructure IT operators 24/7 wireless network testing.

Practical usability of thesis

During my research I made an effort to in thorough way to investigate the relationship between wireless networks and critical information infrastructures. I propose to use my dissertation in higher education within subjects associated with computer network and critical information infrastructures.

The interconnected attack methods and defensive controls, covered by my dissertation, could be used as complementary curriculum in professional periodic trainings.

I propose to use the entire dissertation as a fundamental reference for critical information infrastructure operators.

Publications

Reviewed publications in Hungarian

1. Varga Péter: A kritikus információs infrastruktúrák értelmezése. Hadmérnök, III. évf. 2. sz., 2008. június 149-156.p. ISSN 1788-1919
Honlap: http://www.hadmernok.hu/archivum/2008/2/2008_2_varga.pdf
2. Varga Péter; Illési Zsolt: Kritikus infrastruktúrák hatás alapú modellezése. Hadmérnök, IV. évf. 4. sz., 2009. december 390-399.p. ISSN 1788-1919
Honlap: http://www.hadmernok.hu/2009_4_vargap_illesi.pdf
3. Varga Péter: A polgári műsorszórás, mint kritikus információs infrastruktúra elemzése V. Évfolyam 3. szám - 2010. szeptember 201-211.p. ISSN 1788-1919
Honlap: http://www.hadmernok.hu/2010_3_illesi_varga.pdf
4. Varga Péter; Illési Zsolt: Wardriving és a térinformatika V. Évfolyam 3. szám - 2010. szeptember 80-86.p. ISSN 1788-1919
Honlap: http://www.hadmernok.hu/2010_3_varga.pdf

Publication in English

5. Varga Péter: Wi-Fi enumeration 8th Students' Science Conference
Lengyelország, Szklarska Poręba 2010. augusztus 288-293.p. ISSN 1732-0240

Publication in Conference Proceedings

6. Varga Péter: International and Domestic Regulations of Wireless Network Defense
XXVI. Nemzetközi Kandó Konferencia 2010. november 4-5.
Honlap: <http://regi.kvk.uni-obuda.hu/konf2010/> ISBN 978-963-7158-04-9
7. Varga Péter: Defence taxonomy of wireless networks
XXVII. Nemzetközi Kandó Konferencia
2011. november 17-18. Honlap: <http://kvk.uni-obuda.hu/konf2011/>
ISBN 978-615-5018-20-6
8. Varga Péter: Kritikus információs infrastruktúrák informatikai támadás elleni védelme
Veszélyhelyzeti kommunikáció konferencia,
2007.szeptember 11., Budapest
Honlap: http://emcom2007.kando.hu/prezentacio/varga_peter.pps
9. Varga Péter; Illési Zsolt: Kritikus infrastruktúrák hatásalapú modellezésének kérdései
XXIV. Nemzetközi Kandó Konferencia, 2008.november 7., Budapest
Honlap: <http://regi.kvk.uni-obuda.hu/konf2008/doc/eloadasok/32.ppt>
10. Varga Péter; Illési Zsolt: Kritikus infrastruktúrák hatásalapú vizsgálata
Robothadviselés 8. konferencia, 2008. november 27., Budapest
Honlap:http://www.zmne.hu/tanszekek/ehc/konferencia/prezrw8/Varga_Illési.pdf
11. Varga Péter: A kritikus infrastruktúrák és a vezeték nélküli hálózat kapcsolata
EMCOM 2009 konferencia, 2009. november 13., Hévíz
Honlap: http://regi.kvk.uni-obuda.hu/emcom2009/doc/varga_peter.ppt
12. Varga Péter; Illési Zsolt: GNU Radio a mérésfejlesztésben
XXV. Kandó Konferencia, 2009. november 23.,
Budapest ISBN 978-963-7154-92-8 Honlap: <http://kvk.bmf.hu/konf2009/>
13. Illési Zsolt; Varga Péter: Rádiós hálózatok krimináltechnikai vizsgálata
XXV. Kandó Konferencia, 2009. november 23.,
Budapest ISBN 978-963-7154-92-8 Honlap: <http://kvk.bmf.hu/konf2009/>
14. Dr. Lukács György; Varga Péter: EMC/EMI probléma
EMC 2010., 2010. március 9., Budapest
Honlap: http://kvk.bmf.hu/emc2010/doc/emc2010_lukacs_gyorgy.ppt
15. Varga Péter: Rádiós hálózatok elleni támadások rendszertana
Robothadviselés 10. 2010. november 24. Budapest
Honlap: http://robothadviseles.hu/pres/Varga_Peter10.pdf
16. Varga Péter: Okostelefon a vezeték nélküli hálózatok zártságának vizsgálatában
Emcom 2011 2011. május 3-4. Eger
Honlap: http://regi.hte.hu/uploads/File/varga_peter.ppt

Curriculum Vitae

Name: Péter János VARGA

Date of Birth: 17.19.1974.

Education:

- 2007 – (2013) PhD Institute in Military Technology of National University OF Public Services (prior: Miklós Zrínyi National Defense University): PhD studies
- 2002 – 2007 University of Miskolc, Faculty of Mechanical Engineering and Informatics, information engineering studies
- 2000 – 2001 Budapest Tech, Keleti Faculty of Business and Management, manager studies
- 1993 – 1999 Kandó Kálmán Faculty of Electrical Engineering, technical teaching studies
- 1993 – 1999 Kandó Kálmán Faculty of Electrical Engineering, electrical engineering studies

Work experience:

- 2012– Óbuda University, assistant lecturer (egyetemi tanársegéd)
- 2009 –2012 Óbuda University, council administrator – expert
- 2008 – 2009 LEWA Kft, engineer of informatics and relationship manager
- 2000 – 2008 Budapest Tech Kandó Kálmán Faculty of Electrical Engineering Institute OF Communication Engineering, assistant lecturer (tanársegéd), lab training
- 2000 – 2008 Szabóky Adolf Vocational Training School, provisional teacher of informatics in adult education
- 2001 – 2004 MATRIX Kft. auditor in telecommunication companies audits
- 1994 – 1996 Mikrotrend Kft, software tester

Language skills: Russian B2 complex
English B1 complex

Professional activities:

1. **Education:** Electrical engineering, Telecommunication, Telecommunication technologies, Telecommunication networks

2. **Research and development, consulting:**

- Pannon GSM accounting precision audit (Matrix Kft);
- Emitel accounting precision audit (Matrix Kft);
- New opportunities and design guidelines of long distance analogous optical connections establishment (Magyar Telekom)

3. **Involvement in Professional Organisations:**

- Scientific Association for Infocommunications, member since 2010
- Kandó College for Advanced Studies, member since 2012
- Hungarian Association of Military Science, member since 2009

Specialities:

- wireless network security
- wireless network attack detection
- optical and wireless network interconnections
- smartphone based wireless network