An Automated Graph Based Approach to Risk Assessment for Computer Networks with Mobile Components

Elena Doynikova[1,2] and Igor Kotenko[1,2(✉)]

[1] St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS), St. Petersburg, Russia
[2] St. Petersburg National Research University of Information Technologies, Mechanics and Optics, St. Petersburg, Russia
{doynikova,ivkote}@comsec.spb.ru

Abstract. The paper suggests an automated approach to risk assessment for computer networks with mobile components. The approach is based on the modeling of attacks against computer network as attack graphs and application of open databases of attack patterns and vulnerabilities. Distinctive features of the attacks against networks with mobile components are analyzed. On the base of this analysis we develop the technique of attack graph generation taking into account vulnerabilities of software and hardware for mobile access points as well as weaknesses of mobile devices and mobile connection channels. The technique for calculation of risk assessment metrics is suggested. Operation of the technique for the attack graph generation and calculation of risks is shown on a sample network with mobile components.

Keywords: Mobile networks · Mobile security · Risk analysis · Risk assessment Attack graphs · Security metrics

1 Introduction

Modern computer networks comprise various elements including mobile components. The distribution of mobile technologies leads to new risks for computer network security including risks from the attacks against wireless connections and wireless clients (that comprise mobile and fixed devices). Attacks of this type are becoming more attractive for the malefactors because of the confidential corporate data stored on wireless clients and new possibilities to penetrate enterprise computer networks.

The fact that the number of attacks against mobile devices in order to compromise the enterprise computer networks increases is confirmed, for example, by the report of Check Point Software Technologies Ltd. company [3]. Their list of top-10 attacks against computer networks contains Android malware HummingBad (a persistent mobile chain attack). There are also other serious malware for mobile devices: XcodeGhost, AndroRAT, BrainTest, etc. [3]. It is critical as soon as currently mobile devices can store confidential data and fulfill critical processes. Besides, mobile devices provide additional entry points to computer networks: if an attacker will be able to get privileges on a mobile device, he/she can further compromise all connected network. That is why

I. You et al. (Eds.): MobiSec 2016, CCIS 797, pp. 95–106, 2018.
https://doi.org/10.1007/978-981-10-7850-7_9

it is necessary to consider wireless clients in security awareness. Whereas fixed devices (desktops and workstations) can be controlled, it is more difficult to control mobile devices (laptops, smartphones). Owners of the mobile devices usually do not pay sufficient attention to the security: a lot of devices are not equipped with antivirus; users store not encrypted data, and connect to public Wi-Fi.

In this paper we consider possible attacks against networks with mobile components in the process of security assessment. For security assessment of mobile components we extend our approach suggested earlier for security assessment of fixed computer networks which is based on the analytical modeling and open standards [13, 14]. We review some features of mobile networks and analyze an opportunity of consideration of these features in case of application of the following open standards for security assessment: CAPEC [4] - for the attack pattern representation, CVE [6] - for the vulnerability representation, and CVSS [15] - for the vulnerability assessment. The technique for modeling of attacks against mobile networks and assessment of appropriate risks is suggested. It takes into account vulnerabilities of software and hardware of mobile access points (APs), weaknesses of mobile devices and mobile connection channels. The operation of the technique is demonstrated on an example. Thereby, the main contribution of the paper consists in the development and analysis of the risk assessment technique that considers mobile components.

This paper is an extended version of the paper presented on MobiSec 2016 [8]. Contrary to [8] the particularities of approach for security assessment of mobile components, and algorithms for models generation and assessment are provided.

The paper is organized as follows. Section 2 reviews related researches. Section 3 describes the suggested risk assessment technique for mobile components. In Sect. 4 the approach implementation is shown on an example. Conclusion analyzes the paper results and provides insight into the future research.

2 Related Work

There is a number of research works on the detection, analysis and defense against mobile attacks. Theoharidou et al. [20] consider a risk assessment technique for smartphones. It includes identification of assets, definition of assets criticalities, identification of possible threats, and definition of probabilities of threats considering required permissions. Risk for assets is defined on the basis of attack probabilities and assets criticalities using a risk matrix. Frei [9] reviews a tabular procedure of qualitative risk assessment and controls selection for mobile devices. It is based on existing solutions. The author provides some unique considerations connected with business requirements for the mobile risk assessment. He outlines possible threats for mobile devices and then defines their impacts to business, their likelihood of occurrence and possible controls, and considers risks before and after control implementation for a case study. But the techniques in [20] and [9] are not automated and do not consider in details risks of mobile devices compromise for the whole network.

There are automated techniques of risk assessment for mobile applications. In [22] the tool on the base of Natural Language Processing is suggested. It serves to define the

compliance of the application description and the required application permissions. Authors suppose that further on this basis the security risks of the application installation on mobile devices can be assessed. Jing et al. [19] describe a tool for the automated risk assessment of mobile applications on the base of machine-learned ranking. User should rank the permission groups according to their relevance to the applications of different type. The tool continuously assesses deviation of the required permissions from the expected baseline and defines risks of mobile applications according to the relevance of required permissions. Unfortunately, these works do not consider criticality of mobile devices security for the enterprise computer networks.

Security assessment of mobile networks is considered in [21]. Authors analyze typical components of mobile networks and possible threats. On the base of these data they assess the risk on a quantitative scale considering threat probability, network vulnerabilities and attack impact. Though [21] provides comprehensive analysis of mobile network components considering different protocols and architectures, it does not review automated risk analysis for corporative networks.

In this paper we suggest the technique for the automated risk assessment of the networks with mobile components on the base of analytical modeling and open standards. Main features of the approach are: (1) application of attack graphs to model possible steps of an attacker; (2) application of open standards to represent the input data, including CVE [6] - for vulnerabilities representation, CAPEC [4] - for attack patterns representation, CPE [18] - to represent software and hardware, CVSS [15] - to assess vulnerabilities; (3) application of open databases of vulnerabilities and attacks, including NVD [16] and CAPEC [4]; (4) application of quantitative metrics for security assessment. We suppose that this approach allows to outline weak places of computer networks introduced by unsecured mobile components, and further to increase common security level of networks.

3 Risk Assessment Technique

We suggested an approach to the automated security assessment of fixed computer networks earlier [13, 14]. The approach includes the stages: (1) data gathering (including links between network elements, software and hardware in the CPE format [18], vulnerabilities in the CVE format [6] and weaknesses in the CWE format [7], security events); (2) models generation; (3) calculation of the security metrics; (4) definition of the security level. We divide metrics on groups according to the models used for their calculation: metrics of the topological level are calculated on the base of the network model; metrics of the attack graph level – on the base of the attack model; metrics of the attacker level – on the base of the attacker model; metrics of the events level – on the base of the event model. For the security assessment the metrics of the topological level are mandatory and metrics of other levels are optional and can refine assessments.

In the previous research distinctive features of the wireless network components were not considered. In this paper we fill this gap. The modified processes of our approach and the appropriate data are: the input data gathering process and resulting input data (links between network elements, software and hardware, vulnerabilities and

weaknesses); the models generation process and generated models (network model, attack graph); the security metrics calculation process and generated metrics (attack probability, attack impact, security risk).

To describe particularities of the input data gathering we provide an example of the wireless network architecture in Fig. 1(a). In Fig. 1(b) the attack graph for the example network is provided (it will be described later). The network consists of the Wi-Fi APs (Wi-Fi router and Wi-Fi bridge) and the Wi-Fi clients (mobile devices). Wireless connections are represented with dashed lines. We get input data on the network components from networks scanning tools and administrators.

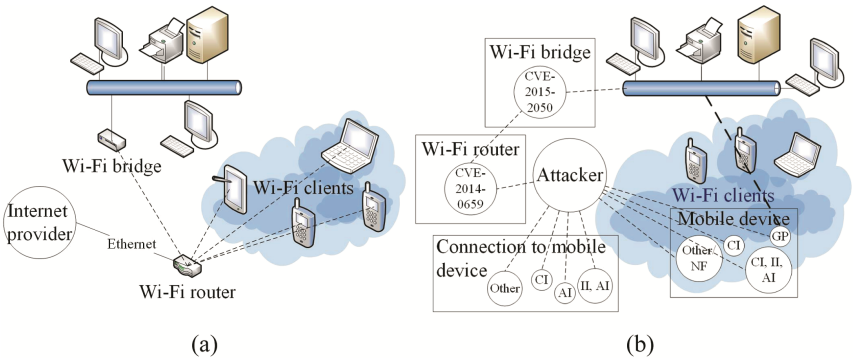

Fig. 1. Example of a wireless network (a) and the attack graph for the example network (b)

An important feature of our approach is the application of open standards and databases. We analyzed opportunity to use them for wireless clients and wireless APs.

Hardware and software of the wireless APs (wireless routers and other devices) can be represented in the CPE format, and its vulnerabilities in the CVE format can be found in the open databases.

For example: Dap-1350: D-Link Wireless Router/AP (in the CPE format: cpe: 2.3:o:d-link:dap-1350_firmware:1.10:*:*:*:*:*:*:*). The appropriate vulnerability instance from the NVD database [16]: CVE-2014-3872 (7.5 – HIGH) in the format: CVE_ID (BaseScore – BaseScore_Qual), where CVE_ID – id of the vulnerability; BaseScore – its quantitative CVSS score; BaseScore_Qual – its qualitative CVSS score. CVSS_Vector for this vulnerability incorporates CVSS indexes and their values [15]: AV:N/AC:L/Au:N/C:P/I:P/A:P, where AV defines access to the vulnerability (N – network, A – adjacent network, L – local), AC – access complexity for the vulnerability (L – low, M – medium, H – high), Au defines if additional authentication is required for the vulnerability exploitation (M – multiple, S – single, N – none), C, I, A – confidentiality, integrity and availability impact from the vulnerability exploitation accordingly (C – complete, P – partial, N – none).

Hardware and software of mobile devices can be also represented in the CPE format, and its vulnerabilities in the CVE format can be found in the open databases. But there is a challenge: new mobile devices can connect to the network and disconnect from it depending on the access policy. So mobile devices and connection channels stay

uncovered. To represent attacks against these objects we chose the CAPEC dictionary [4]. CAPEC database contains various attack patterns including attack patterns for mobile devices and mobile channels. Besides, the CAPEC database provides details on the attack patterns that can be used for security assessments: attack severity, required attacker skills, attack prerequisites and attack impact. CAPEC View that incorporates attacks on mobile devices is named "Mobile Device Patterns" (view id 553) [2]. This set can be complemented with attack patterns from CAPEC category "Communications" (id 512) [1]. In Table 1 these attack patterns are provided with fields of the CAPEC scheme that we will use for security assessment. We added field "Target" to separate attacks against mobile devices from the attacks against wireless channels. It can take values "channel" and "device". We fill this field manually, analyzing the attack pattern description. Field "Typical severity" defines an attack impact level. Field "Attacker skills" defines an attack complexity. These fields can take values: L (low), M (medium), H (high). Field "Attack prerequisites" provides a keyword that defines attack prerequisites ("none" – there is no prerequisites for this attack, "yes" – prerequisites exist). Field "Attack consequences" defines what security property is damaged. To determine it we map its values in the CAPEC database on the impact for the security properties: execute unauthorized code or commands – CI (confidentiality impact), II (Integrity impact), AI (availability impact); DoS: resource consumption – AI; modify application data – II; read application data – CI; other – other; bypass protection mechanism – GP (get privileges). We use this information to generate model of attacks against wireless devices and channels.

The particularities of the *models generation stage* are provided below. Initial network model is generated on the base of network hosts, their hardware and software, their vulnerabilities, and links between them. Model of the network with mobile components additionally contains nodes for the wireless devices, link type, and applicable CAPEC patterns for the wireless devices and channels. On the base of the network model the attack model in the form of an attack graph is generated. Nodes of the graph represent attack actions (exploitation of the vulnerabilities or attack patterns), edges – transitions from the attack action to the next one [12]. Attack actions against wireless APs are automatically included into the model. To model attack actions against other components of the network with wireless components (wireless devices and wireless channels) we generate nodes of the specific type for the attack graph. These nodes contain fields that we outlined in the previous section: "Target", "Typical severity", "Attacker skills", "Attack prerequisites", "Attack consequences". For the attack graph generation we use fields "Target" and "Attack consequences" of the CAPEC scheme. We divide the nodes on two groups: "Connection to mobile device" and "Mobile device". Each group is defined on the base of filed "Target": attack patterns with value "channel" are added to the "Connection to mobile device" group, attack patterns with value "device" are added to the "Mobile device" group. Further attack actions are grouped according to their consequences on the base of "Attack consequences" field: CI; II; AI; NF (not filled); GP; other. Group 1: GP; group 2: CI, II, AI; group 3: CI, II; group 4: CI, AI; group 5: II, AI; group 6: CI; group 7: II; group 8: AI; group 9: other/NF. Attack patterns of these groups are outlined with different colors in Table 1: from the darkest color for the group 1 to the lightest color for the group 9. Field "Attack consequences" is used to link the

Table 1. Mobile attack patterns from the CAPEC dictionary

Name	Target	Typical severity	Attacker skills	Attack prereq-uisites	Attack conse-quences
CAPEC-187: Malicious Automated Software Update	device	H	-	none	-
CAPEC-498: Probe iOS Screenshots	device	-	-	yes	-
CAPEC-499: Intent Intercept	device	-	-	yes	AI, II, CI
CAPEC-501: Activity Hijack	device	-	-	-	-
CAPEC-502: Intent Spoof	device	-	-	yes	-
CAPEC-604: Wi-Fi Jamming	channel	L	L	yes	AI
CAPEC-605: Cellular Jamming	channel	L	L	yes	AI
CAPEC-606: Weakening of Cellular Encryption	device	H	M	yes	other
CAPEC-608: Cryptanalysis of Cellular Encryp-tion	channel	H	M	none	other
CAPEC-609: Cellular Traffic Intercept	channel	L	M	none	CI
CAPEC-610: Cellular Data Injection	channel	H	H	none	AI, II
CAPEC-611: BitSquatting	device	L	L	none	CI, II, AI
CAPEC-612: WiFi MAC Address Tracking	channel	L	L	none	other
CAPEC-613: WiFi SSID Tracking	channel	L	L	none	other
CAPEC-614: Rooting SIM CardS	device	H	M	yes	AI, II, CI
CAPEC-615: Evil Twin Wi-Fi Attack	channel	L	-	none	CI
CAPEC-617: Cellular Rogue Base Station	device	L	L	none	CI
CAPEC-618: Cellular Broadcast Message Request	device	L	L	yes	other
CAPEC-619: Signal Strength Tracking	channel	L	L	-	other
CAPEC-621: Analysis of Packet Timing and Sizes	channel	L	H	yes	CI
CAPEC-622: Electromagnetic Side-Channel Attack	device	L	M	yes	CI
CAPEC-623: Compromising Emanations Attack	device	L	H	yes	CI
CAPEC-625: Mobile Device Fault Injection	device	-	H	-	CI
CAPEC-626: Smudge Attack	device	-	M	yes	GP
CAPEC-627: Counterfeit GPS Signals	device	-	H	none	other
CAPEC-628: Carry-Off GPS Attack	device	-	H	none	other
CAPEC-629: Unauthorized Use of Device Resources	device	-	H	-	other

nodes of attack graph. Attacks that lead to consequences "get privileges" allow to bypass authentication and to proceed attack on the graph nodes corresponding to the network hosts available to the mobile device user. Other groups correspond to the threats of different types.

The attack graph for the wireless network (Fig. 1(a)) is provided in Fig. 1(b). Wi-Fi router is equipped with Cisco WAP4410N wireless AP firmware 2.0.3.3, Wi-Fi bridge is equipped with Dap-1320 D-Link Wireless Repeater. Attack objects are represented with rectangles or appropriate icons. Attack actions (CAPEC attack patterns or CVE exploitation) are grouped according to their consequences and are represented with circles. Dashed lines link sequential attack actions. Attacks that lead to consequences "GP" (CAPEC-626) allow to proceed attack on the next nodes of the graph.

To *assess network security* it is necessary to define security risks for the network components. Risk is defined as product of the attack probability and the attack impact [11]. The attack probability for the graph nodes that represent attack actions against wireless APs is defined with the same equation as attack probability for the other attack graph nodes on the basis of CVSS indexes to show the complexity of the vulnerability exploitation and by using Bayesian equations for the conditional and unconditional probabilities [14].

But the graph nodes that represent attack actions against connection channels and mobile devices stay not covered. To define attack probabilities for these nodes we take into account several aspects: a probability that attacker will initialize an attack against a mobile device or a wireless channel, and the attack likelihood. To define the probability that attacker will initialize an attack we suggest to use the next scale: Low (L) – the limited number of the known devices (devices that are registered and stored in the organization, the owner and firmware are known) can connect to the wireless AP of the network (appropriate quantitative value – 0.3); Medium (M) – the limited number of the unknown devices (any employee can bring his/her own laptop or smartphone and connect to the network) can connect to the wireless AP of the network (appropriate quantitative value – 0.5); High (H) – unlimited number of the unknown devices can connect to the wireless AP of the network (appropriate quantitative value – 0.7). To define attack likelihood we use fields "Attacker skills" and "Attack prerequisites" of the CAPEC attack patterns [4]. To get quantitative values we define scales for these fields in analogy to CVSS [15]. Scale for the "Attacker skills": H – 0.35; M – 0.61; L – 0.71. If field is not filled then the value is L. Scale for the "Attack prerequisites": yes – 0.45; none – 0.704. If field is not filled, the value is "none". Attack likelihood for the graph node is calculated as multiplication of "Attacker skills" and "Attack prerequisites": $AttackLikelihood = AttackerSkills \times AttackPrerequisites$, where *AttackerSkills* – attack complexity according to the "Attacker skills" field; *AttackPrerequisites* – attack prerequisites according to the "Attack prerequisites" field. Final attack probability for the graph node is defined as: $Probability = AttackInit \times AttackLikelihood$, where *AttackInit* – probability that attacker will initialize an attack against the mobile device or channel; *AttackLikelihood* – likelihood that attacker can successfully implement an attack. Maximum value of the *Probability* is 0.35, minimum – 0.05.

We define attack impact as multiplication of the criticality of the targeted asset (*Criticality*) and the impact on the security properties of the asset (*PropImpact*): $Impact = Criticality \times PropImpact$.

Criticality and impact for the wireless AP is defined in the same way as for the other attack graph nodes [14] on the scale from 0 to 10: [criticality_of_confidentiality criticality_of_integrity criticality_of_availability]. Impact on the security properties of the wireless AP is defined on the base of the CVSS indexes C, I and A [15].

For attacks against mobile devices or channels an asset is data on the mobile device. Thus, the asset criticality is defined as criticality of confidentiality, integrity and availability of these data on the scale from 0 to 10 as vector. Impact on the security properties of the asset is defined on the base of the fields "Typical severity" (impact level) and "Attack consequences" (damaged security property). For the "Typical severity" we define the next scale: H – 0.66; M – 0.275; L – 0. If the field is not filled the maximum value is assigned (H). Impact on the security properties is defined as vector: [AI II CI] depending on the "Attack consequences" field. "Get privileges" value leads to impact on all three properties. If value of the "Attack consequences" field is "other" or not filled, it is defined as null impact.

Finally, the risk *Risk* for the attack graph node is defined as vector of three values – risk of confidentiality violation, risk of integrity violation, and risk of availability violation. Risk for each security property is defined as follows (if node contains few attack

patterns, the maximum risk value is selected): $Risk = Probability \times Impact$. Minimum risk value for the single security property is 0, maximum – 6.6. For the security assessment three values of risk are summed. Risk for the node is considered as low if it takes value from 0 to 2, medium – 2 to 5 and high if it is >5. Risk for the network component (host, wireless device, etc.) is defined by the maximum risk of the attack graph nodes of this network component for each security property.

4 Case Study and Discussion

In Fig. 2 a simple computer network that includes wireless subnet is represented. Network incorporates the assets: web application (*host* "Web server", *criticality* [10 10 10] in terms of confidentiality, integrity and availability on the scale from 0 to 10); windows server 2008 operation system (OS) (*host* "Web server", *criticality* [10 10 10]); ApacheStruts2 application (*host* "Web server", *criticality* [7 10 10]); Microsoft.NET Framework 4.6.1 (*host* "Application server", *criticality* [7 10 10]); Squid application (*host* "Proxy server", *criticality* [10 10 10]); authentication service (*host* "Authentication server", *criticality* [10 10 10]); slapd service (*host* "Authentication server", *criticality* [10 10 10]); linux OS (*host* "DB server", *criticality* [10 10 10]); mysql (*host* "DB server", *criticality* [10 10 10]); Citrix (*host* "Firewall", *criticality* [10 10 10]); Cisco WAP4410 N wireless AP firmware 2.0.3.3 (*host* "Access Point", *criticality* [10 10 10]); mobile devices (*criticality* [7 7 7]), etc. Attacker from the notebook attempts to attack mobile devices, channels and AP from the external network.

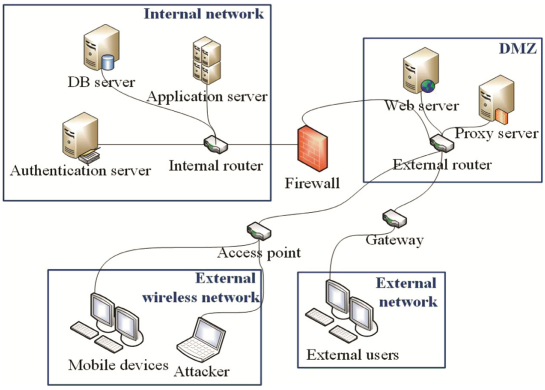

Fig. 2. Topology of the test network

The suggested technique was implemented by the modified tool for security assessment of computer networks [12–14]. The tool was extended to consider mobile components. Simplified version of the generated attack graph for the test network is outlined in Fig. 3. The graph contains possible attack sequences for the external attacker with mobile device. Darkened rectangles are used to represent attack actions. Attack actions for the same host are grouped in the colorless rectangles. Arrows link sequential attack

actions (consequences of the parent attack action allow to perform child attack action). C, I and A note confidentiality, integrity and availability, accordingly. Nodes of the attack graph in the user interface of the developed prototype are highlighted with green color for the low risk (light grey in Fig. 3), yellow color - for the medium risk (medium grey in Fig. 3) and red color - for the high risk (dark grey in Fig. 3).

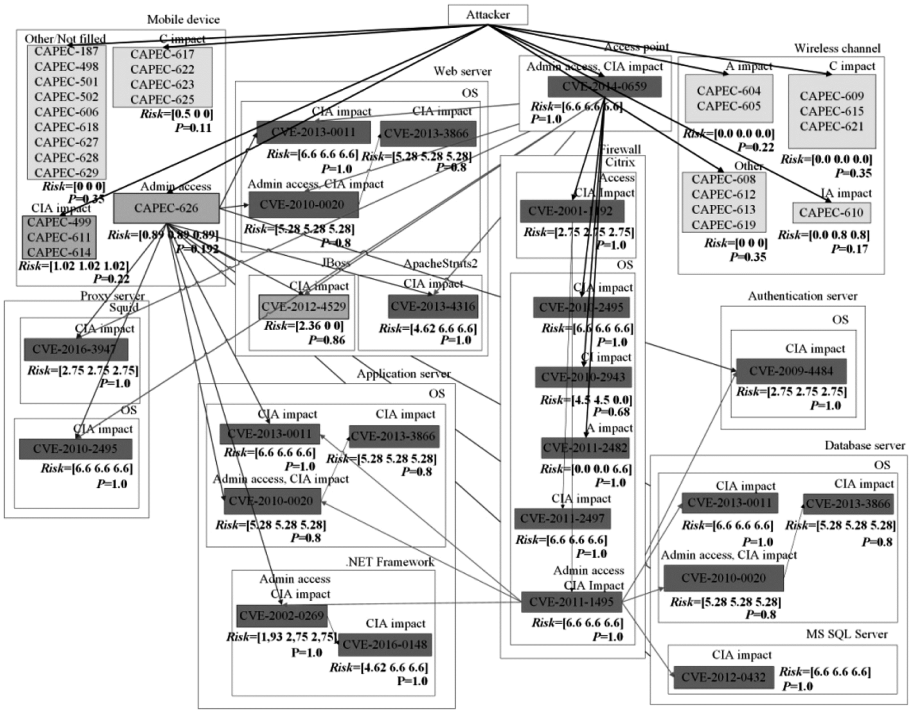

Fig. 3. Attack graph for the test network

Process of the risk calculation for the mobile device, wireless channel and wireless router (access point node in Fig. 3) on the base of the suggested technique is presented below. We consider that unlimited number of unknown devices can connect to the wireless AP of the test network, so $AttackInit = 0.7$.

We will show risk calculation process on the example of CAPEC-626 ("Admin access" group of the mobile device). "Attacker skills" value is Medium, so $AttackerSkills = 0.61$; "Attack prerequisites" exist, so $AttackPrerequisites = 0.45$. $Probability = AttackInit \times AttackLikelihood = 0.7 \times 0.61 \times 0.45 = 0.192$. "Typical severity" for the CAPEC-626 is not filled, so the maximum value (High) is assigned: $PropImpact = 0.66$. Considering asset criticality [7 7 7]: $Impact = Criticality \times PropImpact = 7 \times 0.66 = 4.62$ for all three security properties (because value of the "Attack consequences" field is "get privileges" that leads to impact on all security properties). *Risk* for this pattern is $[0.192 \times 4.620.192 \times 4.620.192 \times 4.62\ ]=[\ 0.890.890.89]$.. This group comprises only

one attack pattern, so *Risk* of this group is [0.890.890.89], total *Risk* is 2.67 (medium). For the wireless router the risk is defined on the base of the CVE-2014-0659. In this case attack probability is determined on the base of the CVSS Exploitability: *Probability* = 1; *PropImpact* is calculated on the base of CVSS impact: *PropImpact* = [0.66 0.66 0.66]. *Risk* = [6.6 6.6 6.6]. Risk for the other nodes that represent attack patterns or vulnerability exploitation is defined similarly. Risk level allows us to outline the most critical attack patterns and vulnerabilities and to select on this base security controls for them.

Output data of the suggested technique comprise the set of the security metrics for the network with mobile components. According to the obtained results vulnerabilities of the APs produce the most risk for the network security. It looks logical because multiple attack paths can go through them. At the same time according to the obtained results wireless channels are not under the risk. It can be explained by the fact that existing CAPEC attack patterns for the mobile channels require high attacker skills and impact only one security property. But this point needs additional research: in some cases the level of abstraction of the CAPEC attack patterns is not enough and specific attacks should be reviewed in individual cases. It relates to the attack impact and applied platforms, links to CWE [7] and CVE databases. For example, for CAPEC-608 impact is defined as "Other", it can be clarified from the "Summary" field that pattern allows to reveal traffic content (confidentiality impact). From the "Technical context" field we see that it is applied to the mobile paradigm (it is very broad), it can be clarified from the "Summary" field that it is applied to the A5/1 and A5/2 algorithms (specified for GSM use). Also, this pattern does not have links to any CVE instances, but has link to CWE-327. This weakness has links to multiple vulnerabilities, but they do not have links to the CWE-327. So this pattern cannot be connected to specific vulnerability instances. In future, in case of appearance of such links, it will give additional information on characteristics of possible attacks.

Suggested technique can be further developed: the list of possible attacks should be extended because CAPEC database contains not all possible attacks on the mobile devices; attack patterns should be processed more carefully; suggested metrics and their scales should be additionally tested. Nevertheless the approach allows to detect possible attack paths in the wireless network and to get quantitative risk values that allow to outline weak places of mobile networks and to select on this base the security controls for them. Compared to the other works in this area the suggested approach is automated, unified and it is more general and applicable to any networks with mobile components.

5 Conclusion

The paper suggests the extension of the approach to the automated risk assessment on the base of the attack graphs to the mobile networks. Distinctive features of the mobile networks are considered, including mobile software, mobility, and weaknesses of the connection channels. CAPEC, CVE and CVSS standards are analyzed if they are applicable to the mobile networks. CAPEC attack patterns for the mobile networks are reviewed. Their fields are analyzed and classified according to their possible values. The

technique for consideration of mobile subnets in the process of the attack graph generation is suggested. It is based on the CAPEC attack patterns and vulnerabilities of mobile devices. Also the technique of risk assessment for mobile subnets is suggested. It is based on the values of fields of CAPEC attack patterns and CVSS. The approach will be further extended. In the future work it is planned to review in details the attacks against different mobile devices and connection channels to expand the list of the considered attacks. It can be done on the base of the OWASP mobile checklist [17] and CWE list [7]. Nevertheless the approach allows to get quantitative risk values for the network objects considering attacks against mobile devices. This allow to outline the most critical attack patterns and vulnerabilities and further to select on this base security controls. Application of the suggested approach was shown on the example of calculations for the test network with a mobile subnet.

Acknowledgements. This research is being supported by the grants of the Russian Foundation of Basic Research (15-07-07451, 16-37-00338, 16-29-09482), partial support of budgetary subjects 0073-2015-0004 and 0073-2015-0007, and Grant 074-U01.

References

1. CAPEC-512: Communications. https://capec.mitre.org/data/definitions/512.html
2. CAPEC-553: Mobile Device Patterns. https://capec.mitre.org/data/definitions/553.html
3. Check Point Software Technologies Ltd.: Check Point – 2016 Security Report. https://www.checkpoint.com/resources/security-report/
4. Common Attack Pattern Enumeration and Classification (CAPEC). https://capec.mitre.org
5. Common Configuration Enumeration (CCE). http://cce.mitre.org/
6. Common Vulnerabilities and Exposures (CVE). http://cve.mitre.org/
7. Common Weakness Enumeration (CWE). https://cwe.mitre.org/data/index.html
8. Doynikova, E., Kotenko, I.: Security assessment based on attack graphs and open standards for computer networks with mobile components. Res. Brief. Inf. Commun. Technol. Evol. **2**, 5:1–5:11 (2016)
9. Frei, D.: Conducting a risk assessment for mobile devices. In: Central-VA-ISSA-May-2012-Meeting (2012)
10. Frigault, M., Wang, L., Singhal A., Jajodia, S.: Measuring network security using dynamic bayesian network. In: 2008 ACM Workshop on Quality of Protection (2008)
11. ISO/IEC 27005:2011: Information technology—Security techniques—Information security risk management, 2nd edn. (2011)
12. Kotenko, I., Chechulin, A.: A cyber attack modeling and impact assessment framework. In: 5th International Conference on Cyber Conflict 2013 (CyCon 2013), pp. 119–142. IEEE and NATO COE Publications, Tallinn (2013)
13. Kotenko, I., Doynikova, E.: Evaluation of computer network security based on attack graphs and security event processing. J. Wirel. Mob. Netw. Ubiquitous Comput. Dependable Appl. (JoWUA) **5**(3), 14–29 (2014)
14. Kotenko, I., Doynikova, E.: Security assessment of computer networks based on attack graphs and security events. In: Linawati, Mahendra, M.S., Neuhold, E.J., Tjoa, A.M., You, I. (eds.) ICT-EurAsia 2014. LNCS, vol. 8407, pp. 462–471. Springer, Heidelberg (2014). https://doi.org/10.1007/978-3-642-55032-4_47
15. Mell, P.: A Complete Guide to the Common Vulnerability Scoring System (2007)

16. NVD website. https://nvd.nist.gov/
17. OWASP Mobile Checklist Final 2016. https://drive.google.com/file/d/0BxOPagp1jPHWYmg3Y3BfLVhMcmc/view
18. Platform Enumeration (CPE). http://cpe.mitre.org/
19. Jing, Y., Ahn, G.-J., Zhao, Z., Hu, H.: RiskMon: continuous and automated risk assessment of mobile applications. In: The 4th ACM Conference on Data and Application Security and Privacy, pp. 99–110 (2014)
20. Theoharidou, M., Mylonas, A., Gritzalis, D.: A risk assessment method for smartphones. In: Gritzalis, D., Furnell, S., Theoharidou, M. (eds.) SEC 2012. IAICT, vol. 376, pp. 443–456. Springer, Heidelberg (2012). https://doi.org/10.1007/978-3-642-30436-1_36
21. Schneider, P. (ed.): Threat and Risk Analysis for Mobile Communication Networks and Mobile Terminals. Deliverable 5. Attack analysis and Security concepts for MObile Network infrastructures, supported by collaborative Information exchAnge project (2012)
22. Pandita, R., Xiao, X., Yang, W., Enck, W., Xie, T.: WHYPER: towards automating risk assessment of mobile applications. In: 22nd USENIX Conference on Security (SEC 2013), pp. 527–542 (2013)