Security Assessment Based on Attack Graphs and Open Standards for Computer Networks with Mobile Components

Elena Doynikova[1] and Igor Kotenko[1,2*]
[1]St. Petersburg Institute for Informatics and Automation (SPIIRAS)
39, 14 Liniya, St. Petersburg, Russia
doynikova, ivkote@comsec.spb.ru
[2]St. Petersburg National Research University of Information Technologies, Mechanics and Optics
49, Kronverkskiy prospekt, Saint-Petersburg, Russia

Abstract

The paper suggests an automatized approach to risk assessment for wireless networks. The approach is based on attack graphs and open standards for security data representation, open databases of attack patterns and vulnerabilities. The suggested approach extends a technique to risk assessment of computer networks suggested by the authors earlier to consider mobile networks. The paper analyzes the features of attacks against mobile devices and wireless connection channels. On the base of this analysis an approach to attack feature consideration in the process of attack graph generation is developed. A technique of calculation of risk assessment metrics is suggested. Generation of an attack graph and calculation of risks is demonstrated on a sample network with mobile components.

Keywords: Mobile Networks, Mobile Security, Risk Analysis, Risk Assessment, Attack Graphs, Security Metrics

1 Introduction

Currently wireless networks are used everywhere. In spite of a number of advantages the distribution of mobile technologies leads to new risks for computer network security including risks from the attacks against wireless connections and wireless clients. Wireless clients comprise mobile and fixed devices. Whereas fixed devices (desktops and workstations) can be controlled, it is more difficult to control data stored on mobile devices (laptops, smartphones). It is critical because currently mobile devices can store confidential data. Besides, mobile devices provide additional entry points to networks. For example, if an attacker will be able to get privileges on a mobile device, he/she can further compromise all connected network.

Related works suggest the next approaches to security assessment for mobile devices. In [20] a risk assessment technique for smartphones is considered. 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 base of attack probabilities and assets criticalities. In [3] a tabular procedure of qualitative risk assessment and controls selection for mobile devices is suggested. There are automatized techniques of risk assessment for mobile devices: in [19] and [12] the tools are reviewed that define risks of mobile applications according to the relevance of required permissions. Security assessment of mobile networks is considered for example in [11]. Authors analyze

Research Briefs on Information & Communication Technology Evolution (ReBICTE), Vol. 2, Article No. 5 (August 31, 2016)
*Corresponding author: Laboratory of Computer Security Problems, St. Petersburg Institute for Informatics and Automation (SPIIRAS), 39, 14 Liniya, St. Petersburg, Russia

typical components of mobile networks and possible threats. On the base of these data they assess risk on a quantitative scale considering threat probability, network vulnerabilities and attack impact.

In this paper we consider possible attacks against mobile networks in process of security assessment. We extend on mobile networks the approach suggested earlier for security assessment of computer networks [15, 16]. Main features of the approach are as follows: (1) application of attack graphs to model possible steps of attacker; (2) application of open standards to represent the input data, including CVE [8] – for vulnerabilities representation, CPE [5] – to represent software and hardware, CCE [4] – to represent configurations, CRE [17] and ERI [13] – to represent controls, CVSS [18] – to assess vulnerabilities; (3) application of open databases of vulnerabilities and attacks, including NVD [10] and CAPEC [1]; (4) application of quantitative metrics for security assessment.

In the paper some features of mobile networks are reviewed. Opportunity of consideration of these features in case of application of CAPEC, CVE and CVSS for security assessment is analyzed. The technique of 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, weaknesses of mobile devices and mobile connection channels. Operation of the technique is shown on an example.

Thereby, main contribution of the paper consists in the development and analysis of the technique of risk assessment that considers mobile components. The paper is organized as follows. Section 2 describes the suggested risk assessment technique for mobile networks. Section **??** shows the approach implementation on an example. Conclusion analyzes the paper results and provides insight into the future research.

2 Risk Assessment Technique

2.1 Common Approach to Risk Assessment

The authors earlier suggested an approach to the automatized security assessment of computer networks [15, 16]. Common scheme of the approach is presented in Figure 1. The approach includes the next main stages: (1) data gathering; (2) models generation; (3) calculation of security metrics; (4) definition of the security level. Output data of each stage are used as input data on the next stage. Data transfer between layers is represented with arrows in Figure 1. Upper layer A in Figure 1 represents sources of the input data. Input data are represented on the layer B. Bold italic text is used for the names of standards that are applied for the input data representation. On the base of the input data, the models are generated (layer C) that are further applied for the metrics calculation. On the layer D and layer E output data of the metrics calculation process are represented. Metrics are divided according to the models used for their calculation. Dashed arrows are used for the optional data, as to define the security level the metrics of the topological level are necessary, and metrics of all other levels can refine this assessment. On the layer F output data of the security assessment are represented in the form of the network security level.

In the previous research distinctive features of the wireless networks were not considered. In this paper we extend the approach on the wireless networks.

2.2 Risk Assessment Technique Considering Mobile Networks

An example of the wireless network architecture is presented in Figure 2 (a). It consists of the Wi-Fi access points (Wi-Fi router and Wi-Fi bridge) and the Wi-Fi clients (mobile devices). Wireless connections are represented with dashed lines. From the security point of view its important features are mobile software, mobility, and weaknesses of the connection channels.

An important feature of the presented approach consists in application of the open standards for the input data representation and in application of the open databases of the software vulnerabilities. Though

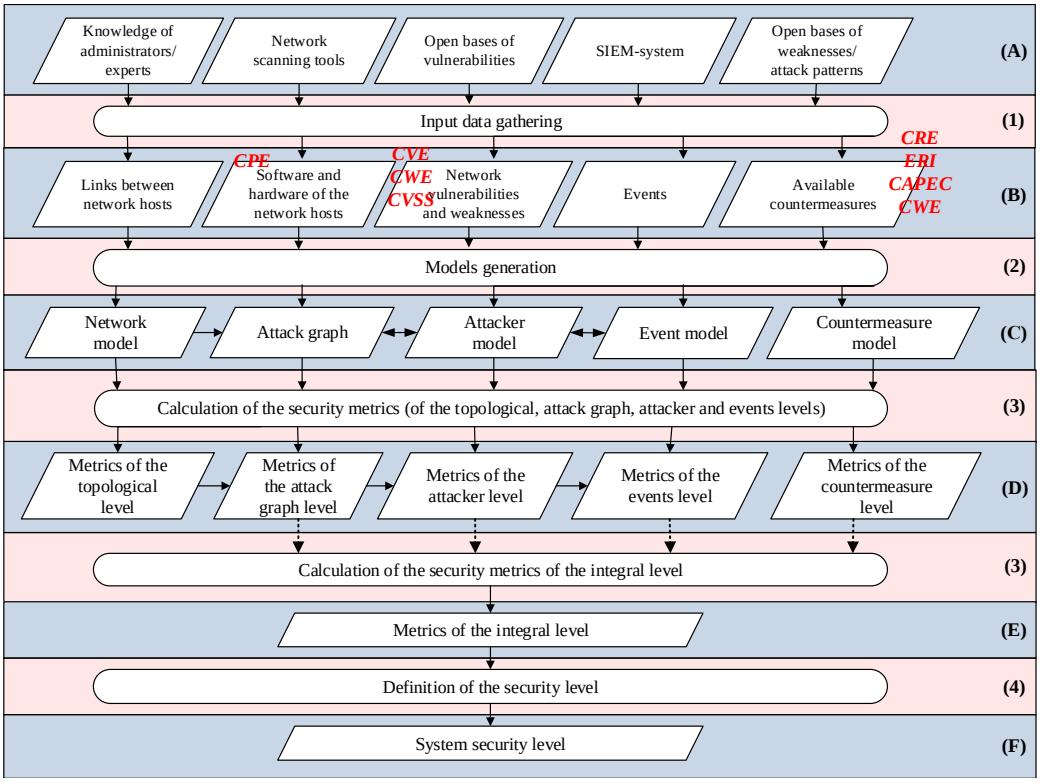

Figure 1: Common scheme of the security assessment approach [15, 16]

mobile software can be represented in the CPE format and its vulnerabilities in the CVE format can be found in the open databases, new mobile devices can connect to the network and disconnect from it. Thus, it is difficult to generate attack graph that will take into account all these devices.

On the other hand, vulnerabilities of the wireless access points (wireless routers and other devices) and appropriate attack paths can be easily modeled as attack graph. In Table 1 the examples of firmware for wireless access points in the CPE format are provided. For the firmware instances,

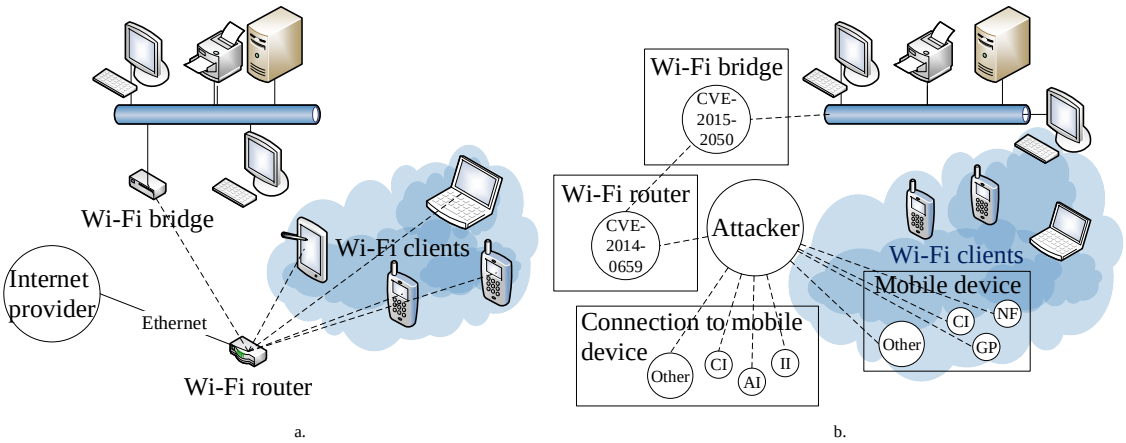

Figure 2: Example of the wireless network

the appropriate vulnerability instances from the NVD database [7] are presented in the form: CVE_ID

(CVSS_BaseScore – CVSS_BaseScore_Qual): CVSS_Vector, where CVE_ID – CVE id of the vulnerability; CVSS_BaseScore – quantitative CVSS score for the vulnerability; CVSS_BaseScore_Qual – qualitative CVSS score for the vulnerability; CVSS_Vector incorporates CVSS indexes and their values. The format of the CVSS_Vector: AV:N;A;L/AC:L;M;H/Au:N;S;M/C:C;P;N/I:C;P;N/A:C;P;N, where AV defines access to the vulnerability and can take values N (network), A (adjacent network), L (local); AC defines access complexity for the vulnerability and can take values L (low), M (medium), H (high); Au defines if additional authentication is required for the vulnerability exploitation and can take values M (multiple), S (single) and N (none); C, I and A stands for the confidentiality, integrity and availability impact from the vulnerability exploitation accordingly, and can take values C (complete), P (partial) and N (none) [18] .

But attack on the connection channels and the mobile devices stay not covered. Though mobile devices can be controlled via mobile access points (for example, number and configuration of the mobile clients can be limited), it is not always possible. So we suggest considering a probability of the fact that the mobile device is compromised. To define this probability we will take into account several aspects.

The first aspect is *a probability that attacker will initialize an attack against a mobile device or a wireless channel*. To define this probability we suggest to use the next scale: Low – 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 access point of the network (appropriate quantitative value – 0.3); Medium – 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 access point of the network (appropriate quantitative value – 0.5); High – unlimited number of the unknown devices can connect to the wireless access point of the network (appropriate quantitative value – 0.7). The next

Table 1: Examples of the firmware of the wireless access points and their vulnerabilities

Model	**Firmware**	**Vulnerabilities**
Dir-600L: D-Link Wireless Cloud Router	cpe:2.3:o:d-link:dir-600l_firmware:2.05:*:*:*:*:*:*:*	CVE-2014-8361 (10.0 – HIGH): AV:N/AC:L/Au:N/C:C/I:C/A:C
Dir-505L: D-Link Wireless Mobile Companion	cpe:2.3:h:d-link:dir-505l_shareport_mobile_companion: a1:*:*:*:*:*:*:*	CVE-2014-3936 (10.0 – HIGH): AV:N/AC:L/Au:N/C:C/I:C/A:C CVE-2013-4772 (9.3 – HIGH): AV:N/AC:M/Au:N/C:C/I:C/A:C
Dap-1320: D-Link Wireless Repeater	cpe:2.3:o:d-link:dap-1320_firmware:1.11:*:*:*:*:*:*:*	CVE-2015-2050 (10.0 – HIGH): AV:N/AC:L/Au:N/C:C/I:C/A:C
Dap-1350: D-Link Wireless Router/Access Point	cpe:2.3:o:d-link:dap-1350_firmware:1.10:*:*:*:*:*:*:*	CVE-2014-3872 (7.5 – HIGH): AV:N/AC:L/Au:N/C:P/I:P/A:P
Cisco WAP4410N wireless access point firmware 2.0.3.3	cpe:2.3:o:cisco:wap4410n_firmware: 2.0.3.3:*:*:*:*:*:*:*	CVE-2014-0659 (10.0 – HIGH): AV:N/AC:L/Au:N/C:C/I:C/A:C

aspect is connected with *the attack likelihood*. To define it we will use CAPEC attack patterns [13] for the mobile devices and mobile channels. CAPEC View that incorporates attacks on the mobile devices is named “Mobile Device Patterns” (view id 553) [7]. This set can be complemented with attack patterns from CAPEC category “Communications” (id 512) [6]. In Table 2 these attack patterns are provided with fields of the CAPEC scheme that we will use for the attack graph generation and risk assessment. Attack target can take values “channel” and “device” (field “Target”). 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. It can take values CI (confidentiality impact), II (Integrity impact), AI (availability impact) and their combinations, “get privileges” or “other”.

For the attack graph generation we use fields “Target” and “Attack consequences”. Depending on the field “Target”, an attack pattern is added to the device or channel node on the attack graph. Further we group attack patterns according to the values of the “Attack consequences” field and add appropriate nodes to the graph.

Attacks that lead to consequences “get privileges” (CAPEC-187, CAPEC-614, CAPEC-626, CAPEC-499) allow to bypass authentication and to proceed attack on the next nodes of the graph. The attack graph for the wireless network (Figure 2 (a)) is provided in Figure 2 (b). Wi-Fi router is equipped with Cisco WAP4410N wireless access point firmware 2.0.3.3, and Wi-Fi bridge is equipped with Dap-1320 D-Link Wireless Repeater. Attack objects are represented with rectangles or appropriate icons. Circles represent attack actions (CAPEC attack patterns or CVE exploitation). Attack actions are grouped according to their consequences: CI; II; AI; NF (not filled). Dashed lines link sequential attack actions.

Table 2: Attack patterns of the CAPEC View “Mobile Device Patterns”

Name	**Target**	**Typical severity**	**Attacker skills**	**Attack prerequisites**	**Attack consequences**
CAPEC-187: Malicious Automated Software Update	device	H	-	none	-
CAPEC-498: Probe iOS Screenshots	device	-	-	yes	-
CAPEC-499: Intent Intercept	device	-	-	yes	A, I and C
CAPEC-604: Wi-Fi Jamming	channel	L	L	yes	A
CAPEC-605: Cellular Jamming	channel	L	L	yes	A
CAPEC-606: Weakening of Cellular Encryption	device	H	M	yes	other
CAPEC-608: Cryptanalysis of Cellular Encryption	channel	H	M	none	C
CAPEC-609: Cellular Traffic Intercept	channel	L	M	none	C
CAPEC-610: Cellular Data Injection	channel	H	H	none	A, I
CAPEC-611: BitSquatting	device	L	L	none	C
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	A, I and C
CAPEC-615: Evil Twin Wi-Fi Attack	channel	L	-	none	C
CAPEC-617: Cellular Rogue Base Station	device	L	L	none	C
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	C
CAPEC-622: Electromagnetic Side-Channel Attack	device	L	M	yes	C
CAPEC-623: Compromising Emanations Attack	channel	L	H	yes	C
CAPEC-625: Mobile Device Fault Injection	device	-	H	-	C
CAPEC-626: Smudge Attack	device	-	M	yes	Get privileges
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

On the next step attack likelihood is calculated. We use fields “Attacker skills” and “Attack prerequisites”. To get quantitative values we define scales for these fields in analogy to CVSS [18]. Scale for the “Attacker skills”: H – 0.35; M – 0.61; L – 0.71. If field is not filled, then the maximum value is assigned (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”.

Final attack probability *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 wireless channel;
$AttackLikelihood = AttackerSkills \times AttackPrerequisites$,
where *AttackerSkills* – attack complexity according to the “Attacker skills” field; *AttackPrerequisites* – attack prerequisites according to the “Attack prerequisites” field. Maximum value of the *Probability* is: 0.35; minimum value – 0.05.

Risk is traditionally defined as product of the attack probability and attack impact.

We define attack impact as multiplication of the criticality of the targeted asset and impact on the security properties of the asset. For the attacks against mobile devices or mobile 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. It is defined on the scale from 0.0 to 10.0 as the following vector: [criticality_of_confidentiality criticality_of_integrity criticality_of_availability]. 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 – 0.660; M – 0.275; L – 0.0. 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. Thus, the attack impact *Impact* is defined as: $Impact = Criticality \times PropImpact$, where *Criticality* – criticality of the targeted asset; *PropImpact* – impact on the security properties of the asset.

Finally, the risk *Risk* for the attack graph node is defined as vector of three values – risk of confidentiality violation, risk of integrity violation, 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 0.0. Maximum – 6.6. For the security assessment three values of risk are summed. So risk for the node is considered as low if it takes value from 0.0 to 2.0, medium – 2.0 to 5.0 and high if it is >5.0.

3 Example

3.1 Input Data

In Figure 3 a simple computer network that includes wireless subnet is represented. In Table 3 network assets and their criticality values for this network are represented. Criticality values for the confidentiality, integrity and availability of assets are given as a vector on the scale from 0 to 10.0.

Attacker from the notebook attempts to attack mobile devices, mobile channels and mobile access point from the external network. Software for the mobile devices is not defined as we suppose that we do not know who will connect to the network.

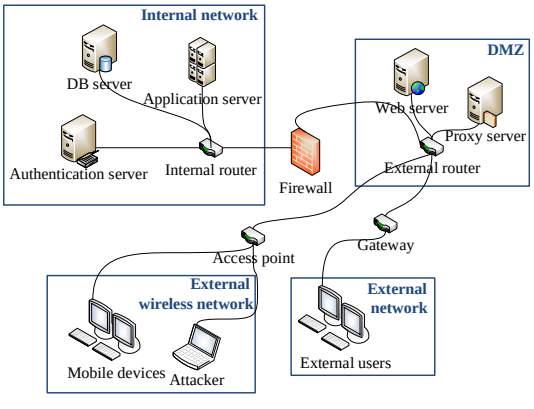

Figure 3: Topology of the test network

Table 3: Assets and criticality values for the test network

Service	Host	Criticality
Web application	Web server	[10.0 10.0 10.0]
Operation system (cpe:/o:microsoft:windows_server_2008::r2:x64)	Web server	[10.0 10.0 10.0]
ApacheStruts2 (cpe:/a:apache:struts:2.0.0)	Web server	[7.0 10.0 10.0]
JBossAS (cpe:/a:redhat:jboss_community_application_server:5.0.1)	Web server	[10.0 10.0 10.0]
Microsoft .NET Framework 4.6.1 (cpe:/a:microsoft:.net_framework:4.6.1)	Application server	[7.0 10.0 10.0]
Operation system (cpe:/o:microsoft:windows_server_2008::r2:x64)	Application server	[10.0 10.0 10.0]
Squid (cpe:/a:squid-cache:squid:4.0.6)	Proxy server	[10.0 10.0 10.0]
Operation system (cpe:/o:linux:linux_kernel:2.6.27.33)	Proxy server	[10.0 10.0 10.0]
Authentication service	Authentication server	[10.0 10.0 10.0]
Operation system (cpe:/o:suse:linux_enterprise_server:9)	Authentication server	[10.0 10.0 10.0]
LDAP (slapd service)	Authentication server	[10.0 10.0 10.0]
Operation system (cpe:/o:linux:linux_kernel:2.6.27.33)	DB server	[10.0 10.0 10.0]
SQL (cpe:/a:oracle:mysql:5.5.25)	DB server	[10.0 10.0 10.0]
Citrix (cpe:/a:citrix:ica_client:6.1)	Firewall	[10.0 10.0 10.0]
Operation system (cpe:/o:linux:linux_kernel:2.6.27.33)	Firewall	[10.0 10.0 10.0]
Cisco WAP4410N wireless access point firmware 2.0.3.3 (cpe:2.3:o:cisco:wap4410n_firmware:2.0.3.3:*:*:*:*:*:*:*)	Access Point	[10.0 10.0 10.0]
–	Mobile device	[7.0 7.0 7.0]

3.2 Risk Assessment

The suggested technique was implemented as the part of a tool for security assessment of computer networks developed earlier [14, 15, 16]. The tool was extended with new techniques of the attack graph generation and security assessment to consider mobile components. Generated attack graph for the test network is outlined in Figure 4. The graph contains possible attack sequences for the external attacker with mobile device. Darkened rectangles are used to represent attack actions (CAPEC attack patterns and CVE exploitation). 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 Figure 4), yellow color for the medium risk (medium grey in Figure 4) and red color for the high risk (dark grey in Figure 4).

Process of the risk calculation for the mobile device, wireless channel and wireless router on the base of the suggested technique is presented below. We consider that unlimited number of unknown devices can connect to the wireless access point of the test network. So, for all attacks on mobile network $AttackInit$=0.7.

We will show risk calculation process on the example of CAPEC-499 ("Admin access" group of the mobile device). "Attacker skills" value is not filled, so the worst case is selected: $AttackerSkills$=0.71; "Attack prerequisites" exist, so $AttackPrerequisites$=0.45. $Probability = AttackInit \times AttackLikelihood = 0.7 \times 0.71 \times 0.45 = 0.22$. $PropImpact$ for the CAPEC-499 is High, so it is equal to 0.660. Considering asset criticality [7.0 7.0 7.0]: $Impact = Criticality \times PropImpact = 7.0 \times 0.66 = 4.62$ for all three security properties. So, *Risk* for this pattern is $[0.22 \times 4.62\ 0.22 \times 4.62\ 0.22 \times 4.62]$=[1.02 1.02 1.02]. It is maximum *Risk* in this group.

Calculations for the patterns of the other groups (due to the paper size limitations only patterns with

maximum risk value are selected) are presented in Table **??**, where *AI – AttackInit*, *AS – AttackerSkills*, *AP – AttackPrerequisites*, *AL – AttackLikelihood*, *P – Probability*, *PI – PropImpact*, *C – Criticality*, *R – Risk*; L – Low, M – Medium, H – High, nf – not filled.

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*=1.0; *PropImpact* is calculated on the base of CVSS impact: *PropImpact*=[0.660 0.660 0.660]. *Risk*=[6.6 6.6 6.6]. Risk for the other nodes that represent 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.

Table 4: Risk calculations for the selected nodes of the attack graph

Node	Group	CAPEC	AI	AS	AP	AL	P	PI	C	R
Mobile device	Other	CAPEC-628	0.7	H 0.35	none 0.704	0.25	0.17	other [0.0 0.0 0.0]	[7.0 7.0 7.0]	[0.0 0.0 0.0]
Mobile device	Not filled	CAPEC-498	0.7	- 0.71	- 0.45	0.32	0.22	- [0.0 0.0 0.0]	[7.0 7.0 7.0]	[0.0 0.0 0.0]
Mobile device	C Impact	CAPEC-625	0.7	H 0.35	- 0.45	0.16	0.11	[nf - -] [0.66 0.0 0.0]	[7.0 7.0 7.0]	[0.5 0.0 0.0]
Mobile device	Admin access	CAPEC-499	0.7	- 0.71	yes 0.45	0.32	0.22	[nf nf nf] [0.66 0.66 0.66]	[7.0 7.0 7.0]	[1.02 1.02 1.02]
Wireless channel	Other	CAPEC-612	0.7	L 0.71	none 0.704	0.49	0.35	other [0.0 0.0 0.0]	[7.0 7.0 7.0]	[0.0 0.0 0.0]
Wireless channel	C Impact	CAPEC-608	0.7	M 0.61	none 0.704	0.43	0.3	[H - -] [0.66 0.0 0.0]	[7.0 7.0 7.0]	[1.39 0.0 0.0]
Wireless channel	A Impact	CAPEC-605	0.7	L 0.71	yes 0.45	0.32	0.22	[- - L] [0.0 0.0 0.275]	[7.0 7.0 7.0]	[0.0 0.0 0.79]
Wireless channel	I Impact	CAPEC-610	0.7	H 0.35	none 0.704	0.25	0.17	[- H -] [0.0 0.66 0.0]	[7.0 7.0 7.0]	[0.0 0.79 0.0]

3.3 Discussion

According to the obtained results vulnerabilities of the access points are the most critical for the network security. It looks logical because multiple attack paths can go through them. At the same time according to the existing CAPEC attack patterns wireless channels are not under the risk. It can be explained by the fact that existing patterns of attacks on 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 [6] and CVE databases. For example, for CAPEC-608 impact is defined as “Other”. From the “Summary” field we can see 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). From the “Summary” field we can see that it is applied to the A5/1 and A5/2 algorithms (specified for GSM use). Also, this pattern doesn’t have links to any CVE instances, but has link to CWE-327. In turn, this weakness has links to multiple vulnerabilities. But these vulnerabilities do not have links to the CWE-327. So this pattern can’t 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 is the first step of the development of the approach to the security assessment

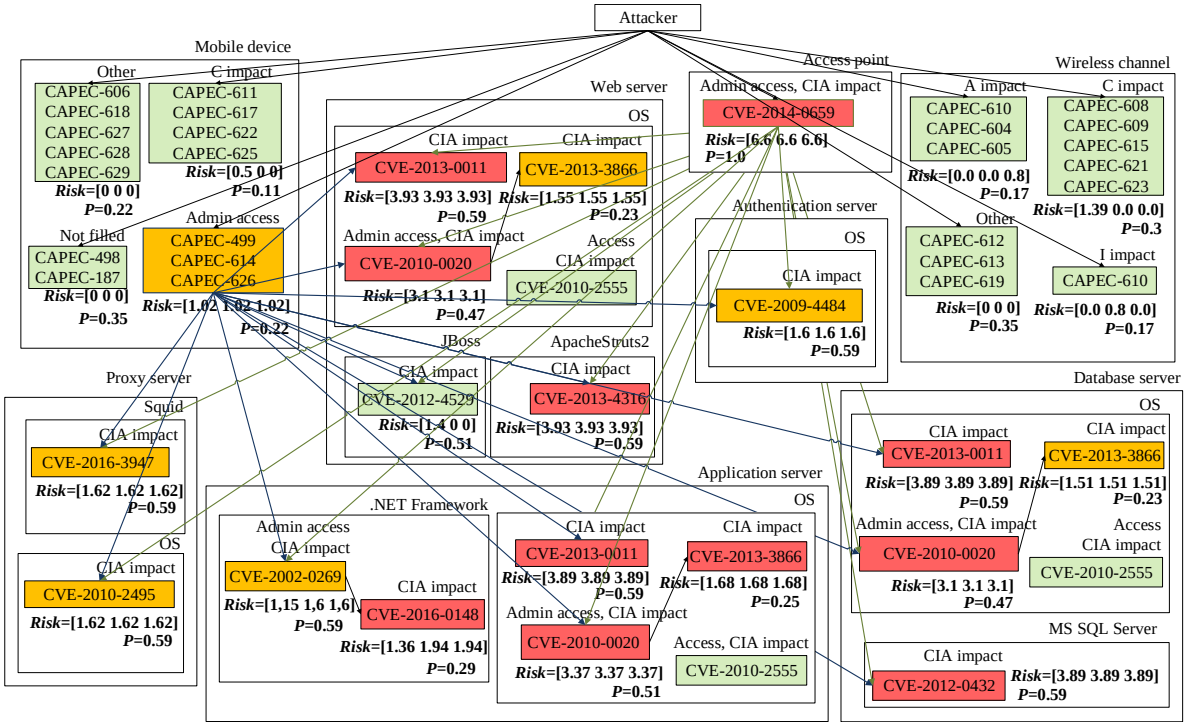

Figure 4: Attack graph for the test network

of wireless networks. It will be further extended. First of all CAPEC database contains not all possible attacks on the mobile devices. Attack patterns should be processed more carefully (from the previous paragraph we see that a lot of information can be taken from the text fields, so they should be parsed accurately). Suggested metrics and their scales should be additionally tested (namely, probability of attacks on the devices and channels).

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 unified (it is based on the open standards) and it is more general and applicable to any networks with mobile components. Another advantage of the suggested technique that it is automatized and requires minimum manual work.

4 Conclusion

The paper suggests the extension of the approach to the automatized risk assessment on the base of the attack graphs on 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. Technique of the consideration of mobile subnets in the process of an attack graph generation is suggested. It is based on the CAPEC attack patterns and vulnerabilities of the mobile devices. Also technique of the risk assessment for the mobile subnets is suggested. It is based on the values of the fields of CAPEC attack patterns and CVSS.

It is the first step of the development of the approach to the security assessment of the wireless

networks. It 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 [9] and CWE list [2].

Nevertheless approach allows to get quantitative risk values for the network objects considering attacks against the mobile devices. This allow to outline the most critical attack patterns and vulnerabilities and further to select on this base security controls for them. Application of the suggested approach was shown on the example of calculations for the test network with mobile subnet.

Acknowledgments

The work is performed by the grant of RSF #15-11-30029 in St. Petersburg Institute for Informatics and Automation of the Russian Academy of Sciences (SPIIRAS).

References

[1] Common Attack Pattern Enumeration and Classification (CAPEC). https://capec.mitre.org.

[2] Common Weakness Enumeration (CWE). https://cwe.mitre.org/data/index.html.

[3] Conducting a risk assessment for mobile devices, May 2012. http://centva.issa.org/wp-content/uploads/2012/05/Risk-Assessment-Mobile-Devices.pdf.

[4] Common Configuration Enumeration(CCE), November 2014. http://cce.mitre.org/.

[5] Platform Enumeration (CPE), November 2014. http://cpe.mitre.org.

[6] Communications (capec-512), November 2015. https://capec.mitre.org/data/definitions/512.html.

[7] Mobile device patterns (capec-553), November 2015. https://capec.mitre.org/data/definitions/553.html.

[8] Common Vulnerabilities and Exposures (CWE), MAY 2016. http://cce.mitre.org/.

[9] Mobile checklist final 2016 (owasp), August 2016. https://drive.google.com/file/d/0BxOPagp1jPHWYmg3Y3BfLVhMcmc/view.

[10] National vulnerability database, June 2016. https://nvd.nist.gov.

[11] A. Egners, E. Rey, H. Schmidt, P. Schneider, and S. Wessel. Threat and risk analysis for mobile communication networks and mobile terminals. Technical Report D5.1(II)-1.0, RWTH Aachen University etc., 2012.

[12] Y. Jing, G.-J. Ahn, Z. Zhao, and H. Hu. Riskmon: continuous and automated risk assessment of mobile applications. In *Proc. of the 4th ACM conference on Data and application security and privacy (CODASPY'14), San Antonio, Texas, USA*, pages 99–110. ACM Press, March 2014.

[13] C. Johnson. Enterprise remediation automation. In *Proc. of the 6th Annual IT Security Automation Conference (ITSAC'10), Baltimore, Maryland, USA*, pages 1–36. IEEE, September 2010.

[14] I. Kotenko and A. Chechulin. A cyber attack modeling and impact assessment framework. In *Proc. of the 5th International Conference on Cyber Conflict (CyCon 13), Tallinn, Estonia*, pages 1–24. IEEE, June 2013.

[15] I. Kotenko and E. Doynikova. Security metrics for risk assessment of distributed information systems. In *Proc. of the 7th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS'13), Berlin, Germany*, pages 646–650. IEEE, September 2013.

[16] I. Kotenko and E. Doynikova. Security assessment of computer networks based on attack graphs and security events. In *Proc. of the 2nd IFIP TC 5/8 International Conference on Information and Communication Technology (ICT-EURASIA'14), Bali, Indonesia, LNCS*, volume 8407, pages 462–471. Springer-Verlag, April 2014.

[17] G. McGuire, D. Waltermire, and J. Baker. Cre - common remediation enumeration. CRE Specification 1.0 (DRAFT), December 2011. https://scap.nist.gov/specifications/cre/.

[18] P. Mell, K. Scarfone, and S. Romanosky. A complete guide to the common vulnerability scoring system version 2.0. CVSS v2 Complete Documentation, June 2007. https://www.first.org/cvss/v2/guide.

[19] R. Pandita, X. Xiao, W. Yang, W. Enck, and T. Xie. Whyper: Towards automating risk assessment of mobile applications. In *Proc. of the 22nd USENIX conference on Security (SEC'13), Washington, D.C., USA*, pages 527–542. IEEE, August 2013.

[20] M. Theoharidou, A. Mylonas, and D. Gritzalis. A risk assessment method for smartphones. In *Proc. of the 27th IFIP TC 11 Information Security and Privacy Conference (SEC'12), Crete, Greece, LNCS*, volume 376, pages 443–456. Springer-Verlag, June 2012.

Author Biography

Elena Doynikova graduated with honors from St. Petersburg Electrotechnical University "LETI". She is researcher of the Laboratory of Computer Security Problems of St. Petersburg Institute for Informatics and Automation. She is the author of more than 50 publications and participate in several Russian and international research projects. Her main research interests are risk analysis and security assessment in the computer networks.

Igor Kotenko graduated with honors from St.Petersburg Academy of Space Engineering and St. Petersburg Signal Academy. He obtained the Ph.D. degree in 1990 and the National degree of Doctor of Engineering Science in 1999. He is Professor of computer science and Head of the Laboratory of Computer Security Problems of St. Petersburg Institute for Informatics and Automation. He is the author of more than 200 refereed publications, including 12 textbooks and monographs. Igor Kotenko has a high experience in the research on computer network security and participated in several projects on developing new security technologies. For example, he was a project leader in the research projects from the US Air Force research department, via its EOARD (European Office of Aerospace Research and Development) branch, EU FP7 and FP6 Projects, HP, Intel, F-Secure, etc. The research results of Igor Kotenko were tested and implemented in more than fifty Russian research and development projects.