



Economic and Social Council

Distr.: General
7 March 2017
English
Original: Russian

Economic Commission for Europe

Inland Transport Committee

Working Party on Customs Questions affecting Transport

Group of Experts on Legal Aspects of the Computerization of the TIR Procedure

Third session

Geneva, 12-13 December 2017

Item 4 of the provisional agenda

Identification of the holder and verification

of the integrity of electronic data interchange messages

Identification of the holder and verification of the integrity of electronic data interchange messages

Transmitted by the Government of the Russian Federation*

* The present document has been reproduced as received by the secretariat.

GE.17-03650 (E) 160317 160317



* 1 7 0 3 6 5 0 *

Please recycle 



I. Current threats to information security (automatic processing)

<i>Threat</i>	<i>Attack</i>	<i>Time of attack</i>	<i>Location of object attacked</i>	<i>Location of attacker</i>	<i>Threat code</i>	
Alteration of electronic documents	Software change	Outside of run-time	Any LAN station	Same LAN station	I1	
				Any LAN station → Server (through LOGIN SCRIPT)		
			Mail server	Mail server		
				Server	Any LAN station	
	Incorrect entry of electronic documents	During run-time		Any LAN station	Same LAN station	I2
					Any LAN station → Server (through LOGIN SCRIPT)	
	Malware	During run-time		Any LAN station	Same LAN station	I3
					Any LAN station → Server (through LOGIN SCRIPT)	
				Mail server	Mail server	
					Any LAN station	
Server				Any LAN station		
Interception of electronic documents	During run-time		Server	Any LAN station	I4	
	During data exchange		Network	Intermediate nodes	I5	
			Modem	Intermediate nodes		

<i>Threat</i>	<i>Attack</i>	<i>Time of attack</i>	<i>Location of object attacked</i>	<i>Location of attacker</i>	<i>Threat code</i>	
Entry of non-existent electronic document	Software change	Outside of run-time	Any LAN station	Same LAN station	I1	
				Any LAN station → Server (through LOGIN SCRIPT)		
			Mail server	Mail server		
					Any LAN station	
	Malware	During run-time	Server	Any LAN station	Any LAN station	I3
			Any LAN station	Same LAN station	Any LAN station → Server (through LOGIN SCRIPT)	
			Mail server	Mail server	Any LAN station	
				Server	Any LAN station	
	Manual entry	During run-time	Server	Server	Any LAN station	I6
			Mail server	Mail server	Any LAN station	
				Any LAN station		
LAN			Any LAN station			
		During data exchange	Network	Intermediate nodes	I7	
		Modem	Intermediate nodes			
Breach of confidentiality of electronic documents	Software change	Same as previous case				
	Malware					
	Monitoring of screen	During run-time	Any LAN station	Any LAN station	I8	
Mail server			Mail server			

<i>Threat</i>	<i>Attack</i>	<i>Time of attack</i>	<i>Location of object attacked</i>	<i>Location of attacker</i>	<i>Threat code</i>
	Interception of electronic documents	During run-time	LAN	Any LAN station	I4
		During data exchange	Network Modem	Intermediate nodes	I5
	Unauthorized copying	Outside of run-time	Server	Any LAN station	I9
Denial of reception of electronic document	Software change	During run-time	Any LAN station Mail server	Any LAN station Mail server	I3
		During data exchange	External customs body	External customs body	
Repudiation of electronic document	Same as previous case				I10
Duplication of electronic document	Software change Malware	Same as previous case			I16
	Iterative attack in network	Outside of run-time	Server LAN Network Modem	Any network station Any network station Intermediate nodes	I12
Loss or deletion of electronic document	Interception of electronic document	During run-time	Server LAN Network Modem	Any network station Any network station Intermediate nodes	I4
	Unauthorized copying	Outside of run-time	Server	Any LAN station	I9
	Software change				I11
	Malware	Same as previous case			

<i>Threat</i>	<i>Attack</i>	<i>Time of attack</i>	<i>Location of object attacked</i>	<i>Location of attacker</i>	<i>Threat code</i>
Unauthorized access to electronic document management system	Unauthorized access	Outside of run-time	Any LAN station	Same LAN station	I13
				Any LAN station → Server (through LOGIN SCRIPT)	
			Mail server	Mail server	
				Any LAN station	
Unauthorized access to data transfer channel	Unauthorized access to channel	During run-time	Server	Any LAN station	I14
			Any LAN station	From external network (Internet)	
		During data exchange	LAN	Any network station	I14
			Data transfer network	Intermediate node	I15
External network attack	External network attack	Outside of run-time	Modem		
			Server		I18
			Network station		
			Modem		
Malfunction of system	Software change, change to configuration of equipment, malware	Outside of run-time	Router		
			Anywhere	Anywhere	I17
Unauthorized router configuration	Unauthorized router configuration	Outside of run-time	Routers	Anywhere in network	I18

II. Protection from threats

Code	Security measures		
	Organizational	Physical	Technical
I1	<ol style="list-style-type: none"> 1. Instructions for changing software configuration 2. User instructions 3. Assign responsibility for contravening regulations 4. Instructions for changing user permissions 	<ol style="list-style-type: none"> 1. Restricted access to premises 2. Physical protection for premises 	<ol style="list-style-type: none"> 1. Ban on downloads to automated workstations from external discs 2. Protection against modification of executable files 3. Closed environment for program execution for each system user 4. Periodic check of integrity of executable files and software settings 5. Use of electronic signatures 6. Event logging
I2	<ol style="list-style-type: none"> 1. Data input validation 2. Check on document transmission 3. User instructions 4. Assign responsibility for contravening regulations 	None	<ol style="list-style-type: none"> 1. Data input validation (using software) 2. Check on document transmission (using software) 3. Event logging
I3	<ol style="list-style-type: none"> 1. Instructions for changing software configuration 2. User instructions 3. Assign responsibility for contravening regulations 	<ol style="list-style-type: none"> 1. Restricted access to premises 2. Physical protection of premises 	<ol style="list-style-type: none"> 1. Ban on downloads to automated workstations from external discs 2. Protection against modification of executable files 3. Closed environment for program execution for each system user 4. Periodic checking of system integrity 5. Event logging 6. Attack alerts
I4	<ol style="list-style-type: none"> 1. Instructions for changing software configuration 2. User instructions 3. Assign responsibility for contravening regulations 4. Instructions for changing user permissions 	<ol style="list-style-type: none"> 1. Restricted access to premises 2. Physical protection of premises 	<ol style="list-style-type: none"> 1. Restricted access to server by media access control address 2. Authorized access to server only from protected workstations 3. Ban on simultaneous access to server by users with the same name 4. Data conversion 5. Protection of server console 6. Event logging 7. Attack alerts

<i>Security measures</i>			
<i>Code</i>	<i>Organizational</i>	<i>Physical</i>	<i>Technical</i>
I5	1. Agreement with external organization	1. Restricted access to premises 2. Physical protection of premises	1. Data conversion 2. Use of electronic signatures 3. Time control (time-out)
I6	1. Instructions for changing user permissions 2. User instructions 3. Assign responsibility for contravening regulations	1. Isolation of protected system from other systems	1. Restricted access to personal computer (PC), server, etc. 2. Authorized access to server only from protected workstations 3. Restricted access to server by media access control (MAC) address 4. Ban on simultaneous access to server by users with the same name 5. Event logging 6. Attack alerts
I7	1. Agreement with external organization	1. Controlled access to premises 2. Physical protection of premises	1. Use of electronic signatures 2. Data conversion 3. Handshaking 4. Time control (time-out)
I8	1. User instructions 2. Assign responsibility for contravening regulations	1. Controlled access to premises 2. Physical protection of premises	1. Screen saver 2. Restricted access to PC 3. Controlled access to PC
I9	1. User instructions 2. Assign responsibility for contravening regulations	1. Controlled access to premises 2. Physical protection of premises	1. Restricted access to server by MAC address 2. Authorized access to server only from protected workstations 3. Ban on simultaneous access to server by users with the same name 4. Data conversion 5. Protection of server console 6. Event logging 7. Attack alerts
I10	1. Agreement with external organization 2. Archive electronic documents	1. Controlled access to premises 2. Physical protection of premises	1. Event logging 2. Use of electronic signatures

Security measures

<i>Code</i>	<i>Organizational</i>	<i>Physical</i>	<i>Technical</i>
I11	<ol style="list-style-type: none"> 1. User instructions 2. Assign responsibility for contravening regulations 	<ol style="list-style-type: none"> 1. Isolation of protected system from other systems 	<ol style="list-style-type: none"> 1. Restricted access to PC 2. Controlled access to PC 3. Event logging 4. Attack alerts
I12	<ol style="list-style-type: none"> 1. User instructions 2. Assign responsibility for contravening regulations 3. Archiving of electronic documents 	<ol style="list-style-type: none"> 1. Isolation of protected system from other systems 	<ol style="list-style-type: none"> 1. Handshaking 2. Electronic signatures 3. Time control (time-out) 4. Event logging
I13	<ol style="list-style-type: none"> 1. User instructions 2. Assign responsibility for contravening regulations 3. Instructions on using information security tools to prevent unauthorized access 4. Restrictions on persons with router configuration rights 	<ol style="list-style-type: none"> 1. Controlled access to premises 2. Physical protection of premises 3. Isolation of protected system from other systems 	<ol style="list-style-type: none"> 1. Restricted access to PC, server 2. Controlled user access to PC, server 3. Event logging 4. Screen saver 5. Change standard security system administrator name 6. Authorize work on network by only one security system administrator or network administrator 7. Owners of all executable files in system and critical setups must be security system administrators 8. Attack alerts 9. Firewalls; antivirus programs 10. Use of all built-in router security features
I14	<ol style="list-style-type: none"> 1. User instructions 2. Assign responsibility for contravening regulations 	<ol style="list-style-type: none"> 1. Protection of cable system 	<ol style="list-style-type: none"> 1. Encryption
I15	<ol style="list-style-type: none"> 1. User instructions 2. Assign responsibility for contravening regulations 	<ol style="list-style-type: none"> 1. Protection of cable system 	<ol style="list-style-type: none"> 1. Encryption

<i>Security measures</i>			
<i>Code</i>	<i>Organizational</i>	<i>Physical</i>	<i>Technical</i>
I16	<ol style="list-style-type: none"> 1. User instructions 2. Assign responsibility for contravening regulations 	<ol style="list-style-type: none"> 1. Controlled access to premises 2. Physical protection of premises 	<ol style="list-style-type: none"> 1. Restricted access to electronic document archives 2. Backups 3. Antivirus software
I17	All measures	All measures	All measures
I18	<ol style="list-style-type: none"> 1. Instructions on using data transmission channels 2. Agreement with external organization 3. User instructions 4. Assign responsibility for contravening regulations 		<ol style="list-style-type: none"> 1. Restrict the number of data transmission channels used 2. PCs with access to electronic document system physically isolated from Internet 3. Restricted access to PC with modem 4. Event logging 5. Attack alerts 6. Firewalls 7. Use of all built-in router security features

III. Informal model of an attacker

Attacker — a person who attempts to carry out prohibited operations or actions, either by mistake, through ignorance or knowingly, either with fraudulent intent (ulterior motives), or without (for fun or for pleasure, for self-affirmation, etc.), making use of various possibilities, methods and means.

The security system should be built taking account of the following assumptions concerning the possible types of persons who might break the security regulations:

(a) “*Inexperienced (careless) user*” — staff member of an organization who may attempt to carry out prohibited operations, access protected automated system resources not permitted to him/her, input incorrect data, etc., by mistake, through incompetence or negligence, without fraudulent intent and using only in-house (accessible to him/her) hardware and software.

(b) “*Amateur*” — staff member of an organization trying to bypass the security system without ulterior motives, for self-affirmation (“for fun”). To bypass the security system and carry out prohibited actions, he/she may make use of various methods to acquire additional permissions for access to resources (names, passwords, etc. of other users), exploit inadequacies in the construction of the security system and in-house (installed on the work station) programs (unauthorized actions going beyond his/her authorization level). He/she may also try to use additional non-in-house tools and technology (debuggers, service utilities), independently developed programs or standard additional hardware.

(c) “*External attacker (intruder)*” — third party individual or staff member of the organization acting directly with ulterior motives or out of curiosity or “for fun”, possibly in collusion with other persons. He/she may use a whole range of methods and means characteristic of general networks (X.25 network or IP-based networks) to crack security systems, including remote input of malware and the use of special hardware and software to exploit weaknesses in the automated system network node security system.

(d) “*Internal intruder*” — staff member of an organization acting intentionally from ulterior motives or revenge for offence caused, possibly in collusion with persons who are not staff members of the organization. He/she may use a whole range of methods and means to break through security systems, including secret methods for obtaining the necessary access, passive methods (interception hardware without modification of system components), active methods and means (modification of hardware, logging into data transmission channels, uploading malware and using special software development tools and throw-away programs), and combinations of them from both within and outside the organization, that is, from the public network.
