# Security Analysis in RE-TRUST. Preliminary Security Analysis of the Entrusting Protocol

Igor Kotenko (SPIIRAS)

## 1. Short Review of Related Work, Trust and Security Analysis Notions

Current level of the open and distributed systems deployment and development implies the need of both security and trust analysis, in particular for Remote Entrusting approach developed in RE-TRUST Project.

Research in this field is reflected in a large list of papers. And in various papers there are different understandings of such notions like «security analysis» and «trust analysis», related, as a rule, with the security of some system or its particular components and with the security of trust mechanisms correspondingly.

In particular, there are at least the following ***understandings of the «security analysis» notion***:

1. Analysis of the system protection grade while the credentials regarding the system setup are delegated to a set of different participants.
2. General analysis of the system security accompanied by the evaluation of possible vulnerabilities regarding multifarious attacks.
3. Analysis of the protection grade for the system whose nodes contain known local vulnerabilities.
4. High-level security risks analysis where security is understood in broad sense.

***Approach to the analysis of the system protection grade while some credentials regarding system setup are delegated to a set of different participants*** is described, for example, in [Li&Winsborough 2005] и [Li&Tripunitara 2006]. In compliance with this approach the security properties of the system (for example, simple safety, bounded safety, containment, etc.) as well as the current state of the system from the participants' permissions standpoint are defined precisely. Then it is suggested to prove required properties using the logical reasoning rules.

***General analysis of the system security accompanied by the evaluation of possible vulnerabilities regarding multifarious attacks*** is represented, for example, in [Jefferson, et al 2004] и [Security Evaluation Report 2007]. The results of such analysis can be represented, for instance, in the form of a *table whose columns describe possible threats, requirements for the attacker to exploit them, possible consequences, countermeasures*, etc. Examples of the threats are «man-in-the-middle» attacks, DoS attacks, «trojan horses», etc.

***Analysis of the protection grade for the system whose nodes contain known local vulnerabilities*** can be found in [Pamula&Jajodia 2006]. In this case the following precise *metric* is defined for system robustness: *weakest attacker able to violate the defined properties*. [Pamula&Jajodia 2006] suggested the precise algorithm to define such attacker based on the descriptions of the system (network) nodes.

***High-level security risks analysis where security is understood in broad sense*** deals with common and particular evaluations of security analysis, including the *estimation of possible losses* from threats realization, *loss expectancy*, *return on investment*, etc.

**In general, security analysis of a protection mechanism includes the following activities:**

- Defining security properties and their metrics;
- Search for possible attacks on the protection mechanism and the protected program (attack discovery);
- Analysis of possibilities for prevention of these attacks (attack prevention);
- Estimation of attack fulfillment complexity (attack assessment).

«Trust analysis» concept is used in several senses too. In particular it may mean:

- security analysis of trust mechanisms which are components of the protection mechanisms as a whole;
- security analysis for the system in which the trust mechanisms play key role (in this case the «trust analysis» concept is tightly connected with the «security analysis» concept).

The first option is described, for example, in [Shmatikov&Talcott 2005], where a formal model for reputation based trust mechanism based on term rewriting is introduced.

The second option is specified in [Presti, et al 2005], where «trust analysis» notion is used instead of the «security analysis» notion.

So, in the case, when the protection mechanism is based on trust passing from one subject (component, process, etc.) to another one, *the trust analysis procedure supposes analyzing in what extent one can rely on subject's dependability to whom specific actions were delegated and a certain trust level was given*.

In RE-TRUST conditions, the trusted server, which is provided a priori with all trust from the protection mechanism designers, gives the part of the trust to the mobile module and possibly secure tamper resistant HW devices on the client side as well, which also fulfill some part of server's functions. In fact, the trust being passed in such a way is delegated to the mobile module and smart card not since the trusted server really trusts them, but because it has to do it (there is no other ways to monitor the program's state in a rather exact manner).

Thus, the trust analysis is in the defining how much the trusted server can trust these elements, which in its turn completely leads to the security analysis of these elements and overall protection mechanism.

## 2. General Procedure of Security Analysis

**The general methodology of security analysis**, as a rule, includes the following main stages [Shmatikov Lectures, etc.]:

1. Modeling the whole system and its components.
2. Modeling the adversary (attacks).
3. Identifying the security properties.
4. Checking if the properties preserved under attacks.

**As the result of this analysis**, by means of formal apparatus, simulation or some qualitative reasoning, it is defined (proved) that under given assumptions about system, no attacks of a certain form will destroy specified properties (figure 1). If it is determined that a successful attack exists, and security properties are violated, i.e. an error in the protection mechanism (system) is discovered, then the necessity of improving the protection mechanism (system), if possible, is concluded.

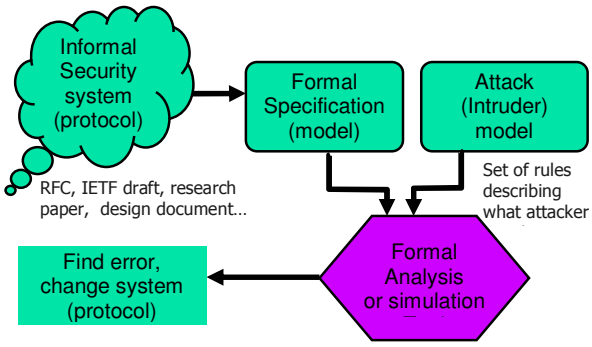


Figure 1. Explicit intruder method

Analyzing the security, it is inevitable, that the researchers use some assumptions about the properties and possibilities of intruders. Thus, as a rule, this analysis is fulfilled under a fundamental tradeoff [Shmatikov Lectures, etc.] which can be expressed as follows:

- Formal models are abstract and greatly simplified (as components are modeled as finite-state machines, security functions are modeled as abstract data types, security properties are stated as unreachability of "bad" states);
- Formal models are tractable (lots of verification methods are used, many are automated), but are not necessarily sound (proofs in the abstract model are subject to simplifying assumptions which ignore some of attacker's capabilities);
- Attack in the formal model implies actual attack.

According to the Trust model, the protection mechanism consists of specific elements – TR (tamper resistance techniques) techniques, replacement technique and entrusting protocol.

**The general of security analysis of the protection mechanism is characterized by the following steps.**

1. At first, **we consider the general attack model**, which includes the specifications of different possible attack classes, and project each of possible attack classes to every protection mechanism's element. In other words, for each such an attack it is needed to determine, which mechanism's elements an attacker have to maliciously tamper with to accomplish it successfully.

2. Then, **each attack is exposed (specified) and concretized in terms of each such an element/technique**. Otherwise the attack (its aim and activities) is described in terms of each protection mechanism element; it is determined which structural parts of the protection mechanism and protected program are subjects of influences; how and by which tricks and tools it is realized.

3. After that, the **security properties and protection mechanisms, which each protection element should provide, are determined**. If it is possible, three classes of protection mechanisms are distinguished: attack prevention, detection and reaction. **Different metrics for each security property are selected**.

4. **It is analyzed, how these security properties are preserved under attack realization**. For each protection element/technique it is investigated how the protection mechanisms (determined in steps 2 and 3), including the mechanisms of attack prevention, detection and reaction, can resist against these attacks. One should determine:

- How persistent the attack prevention mechanisms are.
- Whether the attacks can be found.

- How effective the reaction mechanisms are.
- In what situations and in what conditions these mechanisms/elements do provide the security properties and in what do not.
- What can be added or changed in these mechanisms/elements to heighten the protection against these attacks.
- What to undertake to prevent from attack successful fulfillment and neutralize their consequences.

If it is possible to accomplish, one should evaluate the assessments characterizing attack fulfillment complexity.

5. **For each protective element/technique one should draw a conclusion** on the fact which attacks and by which conditions can be successfully realized by an attacker and which attacks can be successful in spite of all protective techniques applied.

If necessary attack model can be refined and corrected attacks (i.e. the feedback to attack model is defined).

## 3. Security analysis of the entrusting protocol

Let us carry out the *preliminary security analysis of the entrusting protocol* according to the scheme produced in the previous section.

**1.** In compliance with attack model, the possible attacks connected with the entrusting protocol are **interception** and **replacement** of network messages upon any communication act between the client and server (man-in-the-middle case) and **tampering with the protocol functioning within the client program** (man-in-the-end case).

**2.** *Man-in-the-middle attack* represents either

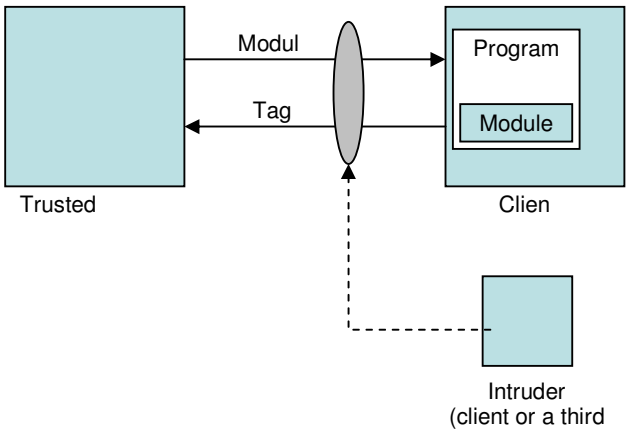


Figure 2

(1) *an investigation of network traffic* between the client program and trusted server with the goal to *intercept* some data (without traffic modification) to realize different types of attacks or

(2) *a replacement (of a part of or entire) network traffic* with the purpose to both *mislead the trusted server about client program state* (in case of modification of the traffic from the client to the server) and *modify the traffic* driven to the client when it is combined with any malicious tampering within the client itself, i.e. it means the case for an attacker it is more

profitable for any reasons to carry out a part of malicious actions not on the client directly, but between the client and server (e.g. it could be more difficult to detect these or easier to implement).

To accomplish attacks of (1) and (2) types, it will be demanded to overcome a property of *confidentiality* of the messages being transmitted on communication channel to view passing data. Subject to entrusting protocol implementations (specific realizations will be presented in respective protocol related deliverables), the given attack can have its own peculiarities. However, in general case such attacks suppose particularly receiving/interception of secret keys shared between the corresponding client's SW component (in charge for the client side of the protocol) and the trusted server, which are exploited to encrypt/decrypt the traffic, etc. The situation is also possible, when such a key receipt is realized by means of crypto analysis, if it can be carried out within the bounds of reasonable time.

For the attack of type (2) besides confidentiality property, an *authentication* of passing messages will be needed. In particular, if protective technique based on MAC (Message Authentication Code) codes is applied, then the complexity of this attack fulfillment will depend on the complexity of corresponding hash function collision matching.

In case of *man-at-the-end attack* on the protocol the attacker is expected to tamper with a specific program component which is located within the mobile module and is in charge of a client side of the protocol.

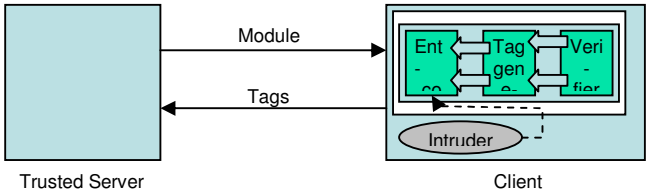


Figure 3

Malicious change of the state of this component (or its program code) occurs by the attacker to modify entrusting protocol functioning rules, including, the rules of outgoing client traffic forming. In case the entrusting protocol is resistant enough, any similar modifications could be discovered by the trusted server indirectly (as reveal of some non-coordination in the protocol or discovery of received data value deviation from specific value bundle expected). *We should take into consideration that the vulnerabilities of similar kinds could arise not only from the insufficient resistance of peculiarly entrusting protocol, but also some flaws of corresponding lower-layer protocols*, which serve as a basis of the protocol in question. In other words such attack can lie in a search of respective network layer protocol vulnerabilities to make the entrusting protocol less resistant.

As a whole any malicious actions against the protocol for an attacker it's better to fulfill within man-in-the-middle attacks, since these would be less disclosed by the trusted server (as the actions on the middle can't be revealed by the program's verifier directly).

**3.** In general case, the attack (1) disclosure is quite complicated, since the attack itself manifestly does not affect on the protection mechanism and program. At the same time the attack (2) can be discovered by means of *revealing any deviations of data* delivered to the trusted server, although the revelation of such type of deviations does not demonstrate obligatory the fact that exactly this type attack, but not any other type attack on the client side, has been accomplished.

The attack (2) could be discovered as well in situation when the total time spent for an attacker to intercept, analyze and modify messages coming in the server is so significant that it can not be explained by overheads of data transmission in physical channels.

Thus, to heighten the detection degree of attack (2), besides control over passing data integrity provision, it is reasonable to apply algorithms and protective schemes being able to raise the time spent by an attacker for the analysis and modifications.

Discovery of man-in-the-end attacks on the protocol is carried out both within the verification process, conducted in the mobile module, and immediately on the trusted server as the detection of any deviations in the protocol work.

**4.** A discovery of type (2) attack itself means an attempt to tamper with the protection mechanism work, and as a result the client stops to be considered as authenticated one and breaks all communications. At that, it is reasonable to complicate attack fulfillment to increase maximum allowable value of replacement period. Therefore from this point of view the rise of time spending is quite sound as well.

For the protocol protection against man-in-the-end attacks, the general client verification techniques are applied (such as client code obfuscation, assertions and so forth).

**5.** Conclusions. In general case, the discovery of attach (1) does not seem to be possible; nevertheless it is reasonable to apply a variety of protective means complicating the process of its realization. For the attach (2) prevention, one should also provide the integrity of data passing on communication channel as much as possible.

The degree of resistance and detection of the man-in-the-end attacks mainly comes to the quality of the corresponding verification techniques of the client's mobile module. More detailed security analysis of the entrusting protocol will be carried out taking into account specific network and cryptographic protocols at the stage of SW prototypes constructions in the subsequent documents.

## References


[Shmatikov Lectures] V.Shmatikov. Design and Analysis of Security Protocols. Lectures.

[Jefferson, et al 2004] D. Jefferson, A.D. Rubin, B. Simons, D. Wagner. A Security Analysis of the Secure Electronic Regisration and Voting Experiment (SERVE). http://servesecurityreport.org/

[Li&Winsborough 2005] N. Li, J.C. Mitchell, W.H. Winsborough. Beyond Proof-of-compliance: Security analysis in Trust management. Journal of the ACM (JACM) Volume 52, Issue 3, May, 2005. P.474-514.

[Li&Tripunitara 2006] N.Li, M.V. Tripunitara. Security Analysis in Role-Based Access Control. ACM Transactions on Information and System Security (TISSEC), Volume 9, Issue 4, November, 2006. P.391-420.

[Presti, et al 2005] S.L.Presti, M.Butler, M.Leushel, C. Booth. A Trust Analysis Methodology for Pervasive Computing systems. Trusting Agents for Trusting Electronic Societies, Springer Berlin / Heidelberg, 2005. P.129-143.

[Pamula&Jajodia 2006] J. Pamula, S. Jajodia. A weakest-adversary security metric for network configuration security analysis. Proceedings of the 2nd ACM workshop on Quality of protection, Alexandria, Virginia, USA, P.31-38, 2006.

[Security Evaluation Report 2007] Security Evaluation of the Sequoia Voting System. Public Report. Computer Security Group. Department of Computer Science. University of

California, Santa Barbara. 2007. http://www.sos.ca.gov/elections/voting_systems/ttbr/red_sequoia.pdf

[Shmatikov&Talcott 2005] V. Shmatikov, C. Talcott. Reputation based trust management. Journal of Computer Security, Volume 13, Issue 1, January, 2005. P.167-190.