Andrzej Gapiński

Strategies for Computer Networks Security

The computer and network security should be viewed in a more general context of the information assurance or information security. As such it represents theory and practice of assuring information.

Here, we use Merriam-Webster's[17] online dictionary for information definition: *Knowledge obtained from investigation, study, or instruction, intelligence, news, facts, data, a signal or character (as communication system or computer) representing data, something (as message, experimental data, or a picture) which justifies change in a construct (as a plan or theory) that represents physical or mental experience or another construct*.

An "assurance", according to the Oxford American Dictionary[18], given our context, means: *a formal declaration or promise given to inspire confidence*, *while the security, using the same source* is: *the safety, against espionage or theft or other danger*.

To define an information security we adopt definition after NIAG[7]: *The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability*.

So information security encompasses all measures undertaken to assure information's safety. Here, the definition is not limited to an information data. It pertains also to knowledge or/and capabilities. The information security encompasses policies and implementations mechanisms, which may include preventive measures undertaken to guard information and capabilities against threats.

Computer security can be defined, after Palmer[16] as: *The protection of the computer resources against accidental or intentional disclosure of confidential data, unlawful modification of data or programs, the destruction of data, software or hardware, and the denial of one's own computer facilities irrespective of the method together with such criminal activities including computer related fraud and blackmail*.

The computer security involves the elimination of weaknesses or vulnerabilities that might be exploited to cause loss or harm.

Historical background

Initially, the information assurance arose in several ways: methodologies and proofs of information correctness, validation of policy to requirements, acquisition of data and/or software from trusted sources, etc., to name a few root motivational causes or needs. Information secrecy and limited access were always part of information assurance as long as human civilization goes back in time. Certainly, for origin of concealment of meaning and/or obfuscation of information one has to go back hundreds if not thousands of years back in human history, to see first attempts of cryptography or encryption. The carved cipher-text on stone in Egypt (ca 1900 BCE), ancient Greek

scytale, Caesar cipher, cript-analysis of Al-Kindi (9th century), poly-alphabetic cipher of Leon Battista Alberti (*ca* 1467), security of the key and Kerckhoff principle of encryption (1883) mark some of the milestones of the historic developments until twenty century. The twenty century brought a modern understanding of information security with mathematics based elaborate encryption schemes. The foundations of theoretical cryptography were laid out by inventor of information theory Claude Shannon[14].

Mathematics, information and computer science, game theory are some of the areas involved nowadays in devising theoretical understanding and development of secure schemes to provide information security. The area of information assurance or security has been greatly enriched in the last two decades due, in a not small part, to birth and expansion of the Internet and its needs. The wireless communications introduced new level of threats, which have to be mitigated to ensure security of data/information[3]. Since level of achieved information security follows the assumed overall security strategy and/or policy, in next segment we will review the concepts of threat, vulnerability, and risk as factors that affect the security strategies.

Threat, vulnerability, and risk

Risk is the potential for a loss[12]. The risk can be quantified based on risk analysis. The issue is well understood by the insurance industry, which has to assess the cost of the repairs (vulnerability) versus the likelihood of the accident all the time.

Two components of risk then are threats and vulnerabilities.

- Threat: action or event that has a potential to cause loss or harm.
- Vulnerability: weakness in security that might be explored to cause a loss or harm.

Clearly threat and vulnerability affect the risk (Threat + Vulnerability → Risk), but to determine quantitative dependence is usually rather difficult to assess. Naturally, the higher vulnerability the higher risk, but even with small vulnerability and high threat the risk can be not low.

Computer security rests on confidentiality or secrecy, integrity, and availability of the assets. Here we are using the following descriptions of these terms[9]:

- Confidentiality, or secrecy – the concealment of information.
- Integrity – trustworthiness of information or data/resources; ensuring that data can be modified only through an authorized mechanism.
- Availability – allowing authorized entities access to assets. This includes authentication as well.

In the case of wireless networks Balakrishnan[3] extends these concepts by including additionally a non-repudiation feature. Confidentiality involves limiting the access to assets through means such as cryptography, biometrics, etc. Integrity requires an articulation of who can modify the assets: information, data, hardware, etc. Availability refers to the ability to use the information and/or resource desired. Computer and network security were subjects of risk assessment and management analysis and modeling.

Trust

Here, we will follow the trust definition after[17]: *assured reliance on the character, ability, strength, or truth of someone or something*.

Naturally, the trust concept is an integral part of any information security strategy, as an interwoven element of articulated policy regarding addressing risks. Here, the trust relationship will be viewed with respect to factors described above and extended by the concept of affinity among entities.

Level of the trust required for safe data access and transfer varies with types of networks. In standard routing protocols vulnerability arises from the fact that nodes trustworthiness is not taken into account while routes are being established[15]. Mobile networks which are often ad hoc self-configuring networks where nodes rely on other nodes for communications, trustworthiness of other nodes must be determined dynamically on the fly and not lend themselves to centralized imposed trust relationships[3].

Computer and Networks Security Models and Resulting Strategies

The computer and network security of any organization follows the assumed overall strategy or policy regarding information security. Therefore the core factors which will determine computer and network security are implied by specific strategic decisions, regarding overall information security policy or strategy put forth by decision makers in any organizations.

A security policy is a statement of what is, and what is not, allowed. After RFC 2196[13]: *security policy is a formal statement of the rules by which people who are given access to an organization's technology and information assets must abide*.

Standards for Security under Risk Management

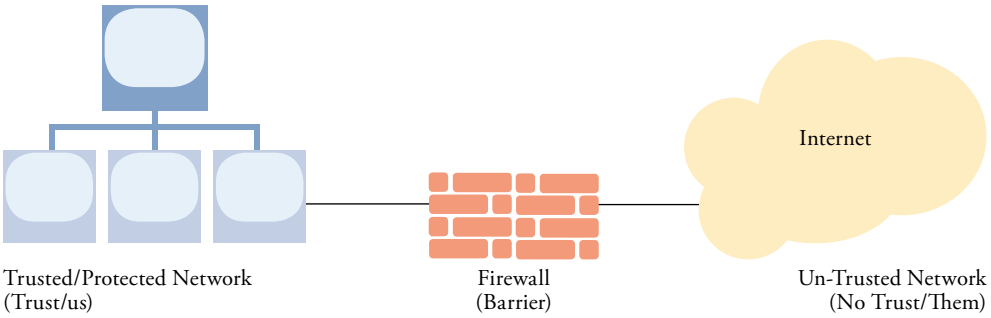
There were attempts to set standards for risk assessment and to quantify risk with regard to information security. In 1979, the National Bureau of Standards published its Federal Information Processing Standards (FIPS) 65, Guideline for Automatic Data Processing Risk which many considered, de facto, as a standard in risk-management modeling[11]. Its Annual Loss Expectancy (ALE) model proposed a metric to quantify computer-related risks. The shortcomings, such as indifference to events of various frequency of appearance, rendered the document not adequate to address current security concerns. In the mid-1980s, the National Bureau of Standards (now a part of the National Institute of Standards and Technology, or NIST) and National Computer Security Center (NCSC), initiated research in the area of computer security risk-management modeling. The developed framework had seven basic elements: requirements, assets, security concerns, threats, safeguards, vulnerabilities, and outcomes expressed in a quantified manner. In retrospect, the excessive complexity, massive computational needs of the model, unavailability of data, and most importantly binary concept of the risk rendered the scheme impractical. The 1990s brought Integrated Business Risk Management models in which security was treated as a part of business processes.

Decision modeling introduced statistical decision theory to management area that includes risk management, which addressed the shortcomings of deterministic models. As such it was the decision-driven modeling, which by quantifying uncertainty was able to encapsulate knowledge of an organization.

Soo Hoo[10] formulated the comprehensive computer security risk model, which addressed shortcomings of previous modeling schemes. While it combined deterministic and probabilistic approaches of past models, and thus eliminated major inadequacies of its predecessors, due to its extensive complexity the model offered little help especially for small and medium size companies.

From historic perspective, computer security was considered either as a risk management issue, part of decision making process, or a pure technological issue to be addressed by technical gurus. Business, science, technology areas formulated and developed various models for computer security looking at the issue from different, and thus lacking uniformity perspective. While on one hand, the disci-

Figure 1 **Bastion Host Topology. Domains: Trusted vs. Not-Trusted**[8)]



pline specific oriented models were easier to implement and thus were more practical, on the other hand general multidisciplinary models were much more comprehensive, much harder to implement. This dilemma of whether to implement a narrowly defined model or a more general one, have led and caused shortcoming of all past and present models for computer and network security.

Topology: Security Models of Computer Networks Architecture

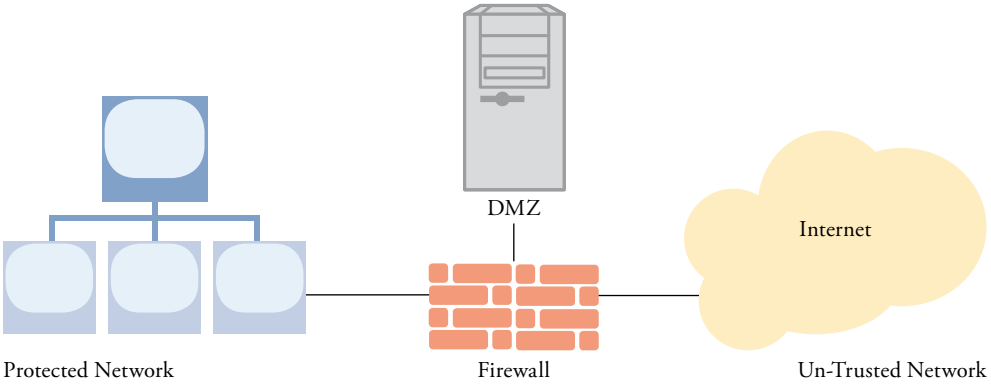
From the beginning of computer networks existence the network topology established two zones with respect to security of computer operations and data transfer: internal zone to protect assets and external to the organization zone – not to be trusted. Thus it was assumed from the beginning of computer systems and networks that the whole cyber universe was divided into two zones: trustworthy (us) and not trustworthy (them) domains. Consequently it was assumed that to ensure information security it was enough to build barrier, such as firewall between two domains. The firewalls in their functionalities add to routers' capabilities in packet filtering. See Figure 1 – Bastion Host Topology[9)]. The firewalls performed packet filtering and could provide additional performance enhancing functionalities besides perimeter security.

With computer network development the demilitarized zone (DMZ) was added to host vital servers with data bases, etc., which provided increased information security. See Figure 2.

DMZ may exist within two-firewall scenario. In some literature the world of networks is segmented into three categories: trusted, un-trusted, and unknown as neither trusted nor un-trusted[8)]. Here two-zone approach will be used without loss of generality.

The current firewall technology went beyond packet filtering and added "stateful inspection" capabilities to monitor active or open data connection routes. In this process high-numbered ports, proxy

Figure 2 **Firewall with DMZ configuration**[8)]



sockets, are allowed to be used between client and server for the duration of the connection, which is monitored and teardown upon completion[9].

The past models assumed protected network as being trusted thus secured, which is not entirely true. More and more internal breaches were reported by industry. The recent report with analysis and statistical data, known to author, performed by Verizon with collaboration of U.S. Secret Service and Dutch High Tech Crime Unit (2011)[19], provides the following classification of security breaches with respect to origin (internal vs. external) relative to past year:

Who is behind data breaches?
92% stemmed from external agents (+22%)
17% implicated insiders (-31%)
<1% resulted from business partners (-10%)
9% involved multiple parties (-18%)".

The drop reported for internal breaches on percent basis may be misleading, as explained by the report due to a significant increase of external attacks in absolute numbers rather than decrease in internal or inside breaches.

As a consequence of the reality of internal threats to organizations, the assumed above model which de facto was and still is an opus operandi for all computer networks has to be changed to one which assumes no trusted domains. See Figure 3.

Thus the computer and network security strategies and/or policies have to be changed to reflect the current reality of security threats and risks.

Since security policy is determined to large extend by the "mind set", the changes to security models follow changes or/and reevaluation at organizational leadership level. Appropriate technology solutions should only follow assumed security model and articulated strategies.

Software and hardware interplay may cause security risk

So far we considered computer security from networks perspective. The similar types of trust based relationships should be considered at computer level, where one faces multivendor interoperability and consequently possible threats from assumed implicit trust among software and/or devices.

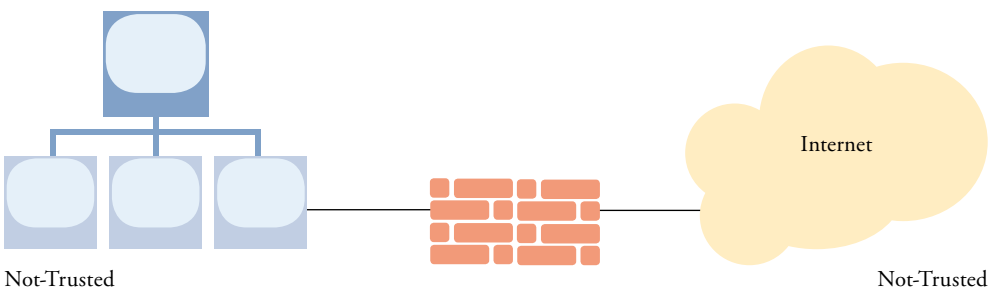
As an example it is implicitly assumed that operating systems trusts computer components, both hardware & software related for lack of malicious intent from devices in interoperation, which may present a security threat [6].

Cyber-security should rely more on "active data structures", where self-protecting data would be capable to preserve its integrity by using inherited genetic footprint[6].

Trust, Affinity, Affinitive Trustor and Trustee

In our model we consider the concept of trust defined in[1] as follows: *Trust is the firm belief in the competence of an entity to act as expected such that this firm belief is*

Figure 3 **Needed Trust Model**



not a fixed value associated with the entity but rather subject to its behavior and applies only within the context and at a given time.

Accordingly we assume that communicating entities assess trust relationship dynamically as the need for re-assessment arises. We will use the term of subjective logic after Josang[5] in assessing trust in terms of trust variables.

Extending the model of Balakrishnan[2] the following model of Trust, Ti, trust for entity *i* is represented by the following structure:

Ti : {Ni,Ri}, where *Ni* represents set of all trust entities, *Ri* represents the set of trust relationships between "i" entity and all others (or needed for trust relationship). While Balakrishnan model applies to nodes in the context of wireless networks, here the entities may represent objects that are software or hardware based.

Here trust (T) is defined as a subjective logic function in terms of mapped trust variables: entity affinity (EA), availability (A), confidentiality (C), integrity (I), and a composite factor (O), which is entity and/or application dependent, such as for example non-repudiation factor, association time, etc. All trust variables will be updated by evidence-to-value mapping operator similarly as in Balakrishnan model[2].

Here it is proposed to define Entity Affinity (EA*ij*) between entities i & j as a quantity given by an affinity function, which specifies affinity or mutual similarity with respect to shared security policy. Motivation behind "entity affinity" term is to introduce factor, which would describe commonality between two entities with respect to shared trust relationship in the context of security.

Entity Affinity

EA*ij* – quantifies relationship between two entities with respect to functional and/or administrative dependence, shared security policy/strategy, etc.

Entity Affinity may play deciding factor in establishing trustworthiness between two entities.

Entities space E, $ej \in E$, where j=1,…, n.

Elements of E space, which comprises all entities, may be viewed as a set containing objects of software or hardware in nature. The affinitive trusts relationships would necessitate formulation of its security strategy as a subset of overall security strategy.

Thus it follows that protected network as in figures 1 & 2 in actuality should become network with strong entity affinity relationship. Next the concepts of Trustor and Trustee for any two entities in trust relationship are defined:

- Entity *ej* is a Trustor if it grants trust attributes to any entity.
- Entity *ek* is a Trustee of *ej* if it receives trust attributes from Trustor *ej*.

It is possible then to describe trust relationship quantitatively among any entities.

The algebraic framework of the proposed security model is the subject of the manuscript in progress[4].

Conclusions

The purpose of the article was to review the current status of computer and networks security from the perspective of practiced strategies and implemented topologies. Computer and network security should be considered in a broader context of information security. Basic strategy and topological models assumed in the past were based on binomial division of trusted and not-trusted domains, that is no longer sufficient to provide an adequate model for ensuring security. The implicit trust relationships presumed often in the past among elements of the same network or domain are no longer practically sufficient for secure operations and/or data or information transfers. The same concerns apply to multivendor, non-uniform

systems of software and hardware devices, which have to operate within the same systems or networks.

Thus the trust relationship must be assessed by all communicating entities, irrespective of whether or not they belong to trusted or not-trusted operating domains. Trust relationship is defined as a subjective logic function. Framework for assessing trust in the terms of standard determining factors such as availability, integrity, confidentiality, and other application dependent factors is described. The proposed trust framework includes entity affinity value, which determines the trustworthiness between two entities. New proposed trust framework enables one to define trust that may be used for variety of objects, which may represent software, network, or hardware related components.

References:

1. Azzedin F., Maheswaran M., *Evolving and Managing Trust in Grid Computing Systems*, "Proceedings of IEEE Canadian Conference on Electrical & Computer Engineering", 2002, pp. 1424-1429.
2. Balakrishnan V. *et al.*, *Subjective Logic Based Trust Model for mobile Ad Hoc Networks*,"Securecomm", 2008, Sept. 22-25, Istanbul, Turkey. ISBN 978-1-60558-241-1.
3. Balakrishnan V. *et al.*, "Securecomm", 2008,, *Trust Enhanced Security Framework For Mobile Ad Hoc Wireless Networks,* Ph.D. Thesis, Dept. of Computing, Macquarie University, Sydney 2010.
4. Gapinski A., *Algebraic Framework for Computer Network Security*. In preparation.
5. Josang A., *A Logic for Uncertain Probabilities*, "International Journal of Uncertainty. Fuzziness and Knowledge-Based Systems", 2001, No. 9(3), pp. 279-311.
6. Kenyon H.S., *Changing Strategy for Computer Network Defense*, 2000, http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=1872&zoneid=254.
7. *National Information Assurance Glossary*, CNSS Instruction, No 4009, 2010, http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf.
8. Schou C., Shoemaker D., *Information Assurance for the Enterprise. A Roadmap to Information Security*." McGraw-Hill, New York 2007.
9. Solomon M.G., Chapple M., *Information Security Illuminated*, Jones &Bartlett Publishers, Sudbary, Massachusetts 2005.
10. Soo Hoo K.J., *How Much Is Enough? A Risk-Management Approach to Computer Security*, Consortium for Research on Information Security and Policy (CRISP), Stanford University 2000.

Internet sources:

11. http://csrc.nist.gov/publications/PubsFIPS.html.
12. http://en.wikipedia.org/wiki/Risk.
13. http://tools.ietf.org/html/rfc2196.
14. www.britannica.com/EBchecked/topic/538577/Claude-Shannon.
15. www.cisco.com/en/US/docs/ios/11_0/router/configuration/gde/ciproute.htm.
16. www.ibm.com/federal/security.
17. www.merriam-webster.com/dictionary/trust.
18. www.oxforddictionaries.com.
19. www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-201_en_xg.pdf.

Andrzej Gapinski, Ph.D., Associate Professor of Engineering, Penn State University – Fayette.