An Analysis of Ethics as Foundation of Information Security in Distributed Systems

Jussipekka Leiwo
Monash University, PSCIT
McMahons Road, Frankston, Vic 3199, Australia
skylark@fcit.monash.edu.au

Seppo Heikkuri
Nokia Telecommunications, Switching Systems
PO Box 111, Fin-0038, Helsinki, Finland
Seppo.Heikkuri@ntc.nokia.com

Abstract

Security of distributed systems requires both technical and administrative foundations. Technical foundation is based on cryptographic measures and access control models, and is considerable well understood. Administrative foundation is based on several non-technical layers added on top of technical communication protocols. Several models for secure interconnection of information systems suggest common ethics to be the uppermost layer and base for legal, managerial and operational procedures. In this paper, ethics as a foundation of secure interconnection of systems is critically analysed and several problems of ethical layer shall be identified. Considering this analysis, a new group and social contract layer shall be suggested on top of ethical layer. The new approach can be enforced within current technology, supports social behaviour of human beings, and is iterative allowing forming of larger secure communities by interconnecting existing secure groups.

1. Introduction

Ethics is an important facet of comprehensive security of information systems. Research in ethics and information systems have been also carried outside the information security community. Anyhow, we see that the relationship of hackers and information security personnel has not yet been properly analysed. Within this report, a philosophical point of view shall be taken, and problems of establishing ethical protection measures against violations of information security shall be studied. Our major argument is that hacking ethics is significantly different from information security ethics, and therefore major difficulties must be solved to establish widely accepted standards for ethical usage on information systems and communication networks. This argument is supported by an extensive analysis and comparison of philosophical and ethical theories. This analysis leads to quite opposite results of the main stream arguments that support the need of common ethical foundation for the security of information systems. A new group and social contract based security layer shall be added on top of ethical layer. This addition provides with a framework that is feasible within the current technology, supports natural social behaviour of human beings, and is iterative enabling forming of larger communities from smaller units.

Typically, the hacking community has been arguing for the freedom of information. Security community has been opposing by arguing that system intrusion and hacking, even if no actual harm is caused, is unethical and criminal activity that one should not commit to, even if technically possible. The question rising from this conflict is how can these two groups claim they have a right to tell each other what is ethical and what is not. Recently, the trend appears to be that the ethics approved by the security community is having the law enforcement. Several attempts around the world are made to enforce proper behaviour in the information society by juridical methods. From a stereotypic information security point of view hackers are seen as criminals, unaware of the results of their immoral activities making fun out of serious problems. Hacker community, on the other hand, sees information security staff as militants that respecting the freedom of individual and information.

These conflicts lead to the fundamental research questions within this paper: Is the ethics based foundation adequate, and how can it be made more feasible. The scope of this report is limited on philosophical aspects. Comprehensive protection requires several types of technical and non-technical protection measures but technical measures are only considered regarding the feasibility of the proposed approach. Feasibility within current technology is a major requirement for a group based security model, and as will be shown, our proposal can be enforced by current secure group communication mechanisms.

Authors attempt to remain neutral, not arguing for or against any of the ethical systems or opinions analysed in this report. We also try to keep our personal interpretations of different results neutral and analyse issues objectively. We are combining results of two areas that typically provoke strong emotions: hacking and ethics. Therefore, extensive effort is made to remain objective. Opinions presented in this report do not necessarily represent opinions of authors or organisations they represent but due to objectivity and significance to

1060-3425/98 $10.00 (c) 1998 IEEE

the topic, they are included and studied. Instead of judging opinions, we are working for an establishment of a framework that could both be flexible and effective. In this paper, the concept “hacker” refers to a person breaking into computer systems or committing into other such activities. This is how this concept is commonly used instead of the original term “cracker”. Those responsible for protecting systems shall be called as “security personnel” or “information security personnel”. This concept appears to be more neutral than concept related to misusers, but there is no - as far as authors are aware - general concept that is commonly used like “hacker”.

The analysis shall begin by briefly introducing the need for security by analysing the origins of threats in open public networks in section 2. Characteristics of hackers, and the relationship of computer crime and hacking shall be studied in section 3. The relationship of ethics and information security shall be studied in section 4. Different theories and models highlighting the importance of ethical operations as a fundamental requirement of information security are surveyed and compared to fundamental concepts of ethical theories. Major section within this paper is section 5 where problems on establishing information security on ethical operations in public networks are identified and studied in detail. Strong evidence against ethics based approach shall be presented. A new foundation for the security of information systems, based on group communication, shall be established in section 6. Proposed model shall be evaluated, conclusions drawn and areas of future research identified in section 7.

2. The need for security in open public communication networks

The expansion of Internet brings together different cultures and societies where norms of ethical and acceptable behaviour, and the role of computing and communication networks within the society, vary a lot. On the other hand, this expansion and evolution has been proven to offer significant business opportunities to corporations and is therefore well justified, the business impact of open networks should not be underestimated [15]. Especially small business benefit from open networks, but larger corporations need more governmental involvement to gain such benefits [37]. Open public networks support adaptivity of organisations, that is a fundamental requirement for the success of organisations at 1990's [2,24,29]. Global, open public networks, such as the Internet, can provide with flexibility enabling organisations to quickly adapt to the rapidly changing business environment. Information security is a major business requirement and a critical success factor of information systems. Heterogenicity of open networks forces organisations using Internet for transferring of confidential or other security critical information to seriously consider countermeasures against different information security threats. Security of business in adaptive and virtual organisations is not of only theoretical and scientific interest, but experiences of real life also highlight the importance and complexity of the issue [6]. A common approach has been to specify and enforce policies for ethical use of Internet, but - as will be studied within this report - this may not be practically possible.

An interesting approach to the information technology has been taken by [34]. The major argument is, that fundamental risks of information technology are not in the technical implementations but in the ideologies behind them. Therefore, information technology should be used only in strictly controlled circumstances. This approach becomes interesting in open, distributed systems, where the major objective is to provide common mechanisms that enable wide application of underlying communication infrastructure. In public networks the fundamental ideology is openness. Once organisations employ the Internet on the transmission of security sensitive information, the underlying ideology is violated. Also, this ideology has, until recently, reduced the interest on strong security measures built in communication protocols. As security measures are reasonable weak, attempts to establish the foundation of secure networking based on ethics have been made. This raises the major concern within this paper. Is the ethical foundation for information security feasible?

3. Aspects on hackers

The section is dedicated on studying the question whether hackers, as specified within this paper, are criminals or not. As this issue is not clear, a reasonable significant amount of analysis is dedicated on the topic. Section 3.1. shall start the analysis by studying characteristics of computer criminals. The relationship of computer crime and hacking shall be summarised from different points of view in section 3.2. When studying the nature of computer crime and hacking, it should be kept in mind that not only hackers commit into immoral activities. Methods organisations use to monitor their employees should as well be analysed regarding ethical application of information technology. According to the MacWorld Poll [30], 21.6% of corporations search employee files on the authority of executive managers, and only 34.6% of management finds this unacceptable. In 66.2% of the cases where files were searched, employees were not warned. Files that were searched included electronic work files (73.8%), electronic mail (41.5%), network messages (27.7%), and voice mail (15.4%). Major reasons for this were work flow

monitoring, investigation of theft or espionage and performance review.

Further, the question of ethical coordination of information services can be applied to questionnaire the ethics of different governmental organisations. Several cryptopolicies and governmental initiatives have been set to restrict application of security enforcement mechanisms to enable monitoring of network traffic to prevent money laundry, drug dealing and other forms of organised crime. Discussion of the topic is, anyhow, not within the scope of this paper. See, for example, [2,11,12] for details.

3.1 Characteristics of computer criminals

Several studies have been conducted to characterise a potential computer criminal. For example, findings of [8] suggest that a typical computer criminal is 18-46 year old, highly motivated, acts to seek for challenges and publicity, and is energetic, bright, and smiling. This is not necessary too satisfactory listing of characteristics. For example, how does smiling indicate the potentiality into computer crime? Also, the age limit 18-46 years indicates that almost anyone involved in computer business is a potential candidate. Findings of Forester and Morrison [14] are very different. Computer criminal is summarised as a loyal, trusted employee, not necessarily possessing great computer expertise, but been tempted by the discovery of flaws in computer systems or loopholes in controls and monitoring procedures. Computer criminals also appeared to be motivated by greed, pressing financial problems, or other personal problems such as alcohol or drugs. 80% of investigated cases were caused by insiders of a company, 25% were carried out by managers or supervisors, 24% by technical staff, and 31% by lowly clerks and cashiers

These facts are in conflict with the common view of computer criminal as a whiz-kid with computer skills much more highly developed than social and ethical skills. The question then rises, what makes a person to commit a computer related crime. Four major factors can be identified, called MOMM model [9]. The acronym stands for Motive, Opportunity, Means, and Method. Four major motivations were listed: money, ideology, compromise, and egotism. For hackers, the major motivation is told to be either fun or money, or egotism. Most of the hackers and virus writers are said to be motivated by egotism, the will to show the superiority of one when compared to others by breaking into systems and sabotaging them. This appears, anyhow, to be in conflict with the hacker ethics of a hacker known as Knightmare [13] who suggests that hackers should never harm any system or gain financial benefit from the hacking. The MOMM model is in align with the motivation factors of computer crime by Forester and Morrison [14]. According to them, computer crime can be seen as an intellectual game, as a “Land of opportunity” for easy crime, as a “Cookie jar” that will easily solve financial or personal problems, as a “soap box” for political expression, as a “fairyland” of unreality, as a “toolbox” for modernising old crime or creating new, or as a “magic wand” that can be programmed to do anything, or even as a 'battle zone' between managers and employees.

Yet another classification is provided by [19] who first classifies offenders into Crackers (hackers within the terminology of this paper), Criminals and Vandals according to the motivation of crime. For crackers the motivation is access to system or data, no matter what is the reason behind that approach. Criminals are motivated by personal gaining of the offence, and vandals have pure intention to cause damage. These, partly overlapping, categories are further divided into different categories, and four types of characteristics: organisational, operational, behavioural and resource characteristics. Considering these, the computer crime adversarial matrix has been developed by FBI. Details can be found in [19, pp.65-69].

3.2. Computer crime and hacking

The relationship of hackers and computer criminals is not clear at all. For example, Angerfelt [3] lists eight forms of computer crime, from which Hacking and Cracking is one. Young [38] divides hackers into utopians and cyberpunks. Utopians believe they help the society by identifying vulnerabilities and cyberpunks intentionally cause harm to institutions and bureaucracies such as teleoperators they see as deserving harm. Denning [10] suggests a more practical point of view by dividing hacking into traditional hacking and malicious hacking.

Hackers can be seen as criminals, or they can be seen as independent computer enthusiasts with a strict moral code preventing activities they concern criminal. Criminal activities are mostly concerned with causing harm to the property or information. The code of ethics of Knightmare includes as a first statement [13]: “Never harm, alter or damage any computer, software, system, or a person in any way”. Also, if the damage is done, the hacker should do what is necessary to correct the damage and prevent it from occurring in the future. Knightmare also states that no hacker should unfairly profit from a hack, and computer managers should be informed about security vulnerabilities. It is interesting to see, that former Greek philosophers see themselves in quite a similar light than hackers see themselves. According to Plato [33, pp.136]:

> *A philosopher is a lover of wisdom. But this is not the same thing as a lover of knowledge, in the sense in which an inquisitive man may be said to love*

knowledge; vulgar curiosity does not make a philosopher. … Consider a man who loves beautiful things, who makes a point of being present at new tragedies, seeing new pictures, and hearing new music. Such a man is not a philosopher, because he loves only beautiful things, whereas the philosopher loves beauty in itself. The man who only loves beautiful things is dreaming, whereas the man who knows absolute beauty is wide awake. The former has only opinion; the latter has knowledge.

The similar arguments can easily be made to define a hacker attempting to achieve something beyond the skills on applying information systems, a deeper understanding of systems. They tend to see themselves as searchers of something more than knowledge, the general and detailed understanding of the reasons that make systems work. This is very romantic way of thinking, like is the above definition of a philosopher, and leads to the fundamental problem of hacking and ethics, to be analysed in detail in section 5. If there is information that hackers think should be free, but the owner of that information wants to restrict, is it ethical and right to obtain unauthorised access to that information. The first answer seems obvious, it should not be done. Anyhow, a more detailed and thoroughfull analysis shows, that the answer is not that simple and obvious. According to Hobbes (1588-1679) [33, pp.534-535] the natural state of men is freedom. Before any government is at place, every individual desires to preserve his liberty, not to acquire dominion over others. Conflicts arisen from this are escaped by forming different communities in the means of a social contract. An obvious interpretation of social contract on hackers would be, that hackers are those that have not agreed the social contract of the community providing information services to users who share their social values.

The view of a hacker as a protector of the freedom of information and liberty of human beings may be difficult to fit into the characteristics of a typical computer criminal. The law enforcement currently appears to criminalise system intrusion. This leads to several problems in understanding the behaviour of computer criminals. If it is assumed that systems are adequately protected, and still intentional violations occur, the assumptions as computer criminals as ordinary employees getting the opportunity can be forgotten. Denning [10] suggests that, as the hackers are very different from criminals finding computers as a new tool. Instead of criminalising their activities, it would be of best interest of all if co-operation could be established and new approaches developed. This co-operation leads to the analysis of questions like should hackers be employed to identify potential secure breaches of systems. This question typically provokes controversy but shall not be further studied within this paper.

4. Ethics and information security

Within this paper, a wide approach shall be taken towards information security. It refers to the protection of information assets against violations of confidentiality, integrity, and availability against different threats. There is no generally agreed definition of the security of information systems, and some critics has targeted on this division (see for example [4] or [7] for details), but for the purposes of this paper, it is satisfactory. More important than the exact definition of information security are the types of protection measures required to provide comprehensive protection of information. Technical protection measures are not alone enough, but a more comprehensive approach is required, as will be seen later in this section. Operational, administrative, ethical, sociological, legal, and other such non-technical protection measures are required on top of technical protection measures to develop and maintain good information security. Typically, ethical aspects and information security awareness are some key factors when end users are doing tasks using information technology securely. Hartmann [16] lists examination levels for comprehensive information technology security to include technical and technological elements, organisational elements, legal and economical elements, and social and ecological elements. Along with these, information security should be studied from the ethical dimensions. According to Hartmann, ethics in information technology is such a large question that system designers, developers, and users are not alone enough to give answers. Instead, entire society should be involved in the discussion concerning responsibilities of different groups involved.

Kowalski [21] has identified four major reasons for ethical issues to appear in the computer security research. First, there is the widening control gap in commercial information systems. Control gap can be further divided into three categories: Technological gap, socio-technical gap, and social gap. Technological gap is between what the reality and expectations of the capabilities of security enforcing functions. Socio-technical gap is the inconsistency between socially expected norms and computer security policies, and the social gap refers to individuals not acting according to expected social norms. Second, ethics may be the common language for specialists of different areas, and can be understood also by groups outside the computing community. Third, current systems are so large that there are no implicit technological control structures to manage them. Instead, most systems are managed by individuals' implicit control structures that are built on the framework of ethical principles. Fourth, there is the need for top-down approach, like to ISSI (Information Systems Secure Interconnection) -model. According to ISSI, five non-technical layers are added on top of OSI protocols. The

uppermost of these is ethical layer, that is a good starting point to reach agreements between users and systems.

Ethics in information system has been widely studied also outside the information security community. Four major topics that ethics should address in information technology are [25]:

Privacy What information about one's self or one's associations must a person reveal to others, under what conditions and with what safeguards? What things can people keep to themselves and not be forced to reveal to others?

Accuracy Who is responsible for authenticity, fidelity, and accuracy of information? Similarly, who is to be held accountable for errors in information and how is the injured party to be made whole?

Property Who owns information? What are the just and fair prices for its exchange? Who owns channels, especially the airways, through which information is transmitted? How should access to this scare resource be allocated?

Accessibility What information does a person or an organisation have a right or a privilege to obtain, under which conditions and within what safeguards?

These four questions are the major concerns in the discussion of ethical dimensions of information security and hacking. The personal responsibility of individuals to respect these facets enters an essential role. If the approach towards society and networks is very different, groups can not trust on the respect of other groups towards the facets. The situation becomes even more difficult when one group intentionally takes violations of the protection established to clarify these questions as a challenge and merit within their society.

Still we have not given a specification for the fundamental concept within this paper, ethics. A definition or ethics regarding information systems can be given, for example, as by James Moor [27]. Ethics is seen as an analysis of the nature of social impact of computer technology and the corresponding formulation and justification of policies for the ethical use of technology. If this is linked to information security and ethics, as presented in earlier paragraphs, the common computer ethics appears to be the base for the entire information security development. Questions related to the ethics in information security should be expanded to cover entire ethical use of information and information systems.

The need for ethics in general can be, for example, justified by the greed of people. According to the utilitarian school [33, pp.745], ethics is necessary because man desires conflict. Conflict is caused by egotism, most of people are interested in their welfare than that of others. Therefore, ethics have two purposes: to find criteria to distinguish between good and bad, and to promote good desires and discourage bad ones. To make this difference, two basic approaches can be taken: deontological (rule-based) ethics and consequential ethics. Deontological ethics states that there are things that should be done and things that should not be done. Virtue is seen as an end of ethical activities. According to consequential ethics, what is done is not essential but the value of activities is determined by the outcome. Virtue is seen as a means to achieve the desired good outcome.

Information security specialists tend to deontologically specify what is ethical behaviour and what is not. On the other hand, typical approach among hackers is that their activity provides good outcome for the information security community by identifying vulnerabilities in systems. These approaches unfortunately are in a strong conflict. Further depth into the conflict can be found by introducing another dimension to the classification of ethical theories into two categories: Phenomenologist vs. Positivist and individualist vs. collectivist ethics:

Phenomenologism vs. Positivism According to the phenomenological school, what is good is given in the situation, derived from the logic and language of the situation or from dialogue and debate about “goodness” per se. Positivism encourages us to observe the real world and derive ethical principles inductively.

Individualism vs. Collectivism According to the individualistic school, the moral authority is located in the individual, whereas collectivism says that a larger collectivity must care the moral authority.

Major schools, based on these concepts, can be listed to be Collective Rule-Based Ethics, Individual Rule-Based Ethics, Collective Consecuentialists, and Individual Consecuentialists. A more detailed analysis of these concepts is not required for the purposes of this paper. A detailed analysis of these schools is provided by Laudon [22]. A more comprehensive analysis on ethics from the information technology point of view is given, for example, by [35].

5. Problems with ethical foundation

Different views of information systems can be roughly considered as different social contracts. The purpose of a social contract is to voluntarily escape the potential conflict caused by ultimate freedom of each individual by forming groups and delegating authority to some instance. Hackers can be considered as individuals, who have agreed upon a very different social contracts than information security personnel. They tend to maintain their freedom and individuality in the controlled world. For example, according to Knightmare [13]:

> *What I'm about to do is give my own version of the Hacker's Ethic. This is a set of beliefs that I have about the world of computers. It may not be what you believe, but that's all right. Hacking has to do with independence.*

This may lead into severe difficulties in bridging the cap between hackers and information security personnel. Even if the importance of common ethics in comprehensive security of information systems is recognised, there are problems. For example, according to Kowalski [21]:

> *Computer security administrators are realizing that ethics can function as the common language for all the different groups within the computer community.*

The conflict is clear. Hackers tend to maintain their individualism and independence by their approach towards ethics and computing, while on the other hand ethics should be commonly agreed upon by different groups related to information systems. In the networking community, where different cultural and technical information security problems increase, the adoption of common ethics becomes even more difficult [28]. The important concept becomes cultural relativism [17]. In cultural relativism, it is assumed that each judgment is based on personal values, and personal values are based on the culture the individual is associated with. Therefore, it becomes obvious that ethical values may vary significantly between different cultures. According to cultural relativism, hacking and information security are different cultures, and therefore they are not capable of judging each others values.

Ethical protection measures intend to provide a common high moral code for the usage of communication networks. As shall be studied within this paper, it is very difficult to find common values between hackers and information security personnel. As these values can not be identified, there is no need for common moral code to protect these values. Plato searched for a common foundation for moral considerations, but after Hegel cultural relativism has had more important impact. The truth values of ethical value statements are subjective and can therefore not be transferred from one moral system to another. Universality is a fatal requirement for ethical and moral systems, especially when the relationship of culture and moral is agreed upon.

As suggested by the ISSI model, ethical measures should be on top legal protection measures. Anyhow, law enforcement easily becomes the uppermost of the types of protection measures. According to John Locke (1632-1704) [33, pp.606-610] every human being has the right to punish attacks on himself or his property. Anyhow, typically societies require this right to be transformed into law enforcement authorities. Russell states [33, pp.608], that “The beginning of a politic society depends upon the consent of the individuals to join into and make one society”. In the terms of information security, this refers to the agreement of common rules for adequate behaviour within information systems. If the agreement of a social contract is based on volunteering, the essential question arises on how to expect that those, who disagree with it would follow it?

Jean Jacques Rousseau (1712-78) [33, pp.660-674] stated that in the development from the state of nature, there comes a time when individuals can no longer maintain themselves in primitive independence. It then becomes necessary to self-preservation that they should unite and form a society. The essential question then becomes on how to pledge liberty without harming others. The fundamental question, to which social contract is to provide an answer, is to find a form of association which will defend and protect with the whole common force the person and goods of each associate, and in which each, while uniting himself with all, may still obey himself alone, and remain as free as before. Rousseau indicated clearly, that each individual should obey the common direction, and those not obeying the general will should be forced to do so. The social contract of Rousseau has several implications that lead to the society too far from our society to be acceptable.

An opposite view was taken by Immanuel Kant (1724-1804) [33, pp.675-690]. He stated that each man is to be regarded as an end in himself. His doctrine of the Rights of a Man and his love of freedom is shown in his saying “There can be nothing as dreadful than that actions of a man should be subject to the will of another”. This, anyhow, leads to the impossibility of agreeing when two people's interests conflict and to the democratic assumption, that each opinion should be counted equally when making decisions that affect many.

These examples do not cover all the discussion about social contracts and ethics in history. They do, anyhow, highlight the different approaches taken towards the rights of an individual with respect to the law enforcement. As the current trend appears to criminalise hacking, introduction of these views may be necessary. Alignment of the law enforcement against hacking with the democratic rules of modern society may not be simple. For example, The democracy principle of OECD [1] requires that the security of information systems should be compatible with the legitimate use and flow of data and information in a democratic society. The important question is whether criminalisation improves the situation or makes it worse. According to general theory of deterrence, the threat of punishment, along with the probability of being caught if some illegal action is taken, acts in preventing misuse of different resources. It has been shown that severity of punishment, when controls are established to improve the probability of detection, has a significant impact on reducing computer misuse [23,36]. On the other hand, the criminalisation of hacking may lead into the growth of computer underground. In fact, there is little evidence that punishment will in the long run reduce the number of offences, but may even have an opposite impact [10,26]

From the philosophical point of view, the important concept in legislation becomes utilitarianism [33, pp.740-747]. An important character is Jeremy Bentham who stated that good is happiness in general, but also each individual pursues what he believes to pursue his own happiness. The justification of criminal law is its capacity to make the interests of the individual coincide with those of the community. Crime is punished not for revenge or hate but for the prevention of crime. Therefore, the punishment should rather be certain than severe. Properties of good legislation were subsistence, abundance, security and equality. Liberty was not mentioned. Bentham's ethics has some obvious logical conflicts, like how to expect that law enforcement authorities are capable of working for common good, since humans are driven by a seek of personal good. Anyhow, these conflicts shall not be studied within this paper. This is a commonly agreed problem in information security. Investigation and prosecution require detailed understanding from both law and information technology. As there is a lack of qualified law enforcement personnel, the justification of juridical measures as enforcement of ethics can be questionned.

6. Extended ISSI model

To establish a new foundation for the security of distributed systems, three fundamental requirements shall be set for the proposed framework: First, the framework must support the natural behaviour of human beings with establishment of social contracts. Second, the framework must be iterative in the sense that large systems can be composed from smaller sub systems. Third, the Framework must be feasible within current technologies.

First requirement is crucial to guarantee that no conflicts exist with behaviour of human beings within society in general and in the context of public distributed systems. This requirement is satisfied by the group establishment procedure. As has been shown, it is a natural tendency of human beings is to form informal groups that can be formalised. Humans within a group can be expected to follow the acceptable code of conduct within that group. Similarly, different groups can form larger groups, that is essential to satisfy the second requirement. The model must support forming of groups first of human beings, and then by combining groups and establishing communication links between different groups. This is supported by the nature of group behaviour. As groups expand, it is not only that groups get new members, but different groups with common interests act in co-operation to achieve their goals. As that goal is common for each participant, agreement of social contract can be expected over original group boundaries.

Third objective is obvious. Any solution that can not be enforced by technological measures can not be considered adequate. As security of information systems requires both technical and non-technical measures, special effort must be paid on the assurance that all methods support each other and do not set contradictory or infeasible requirements for each other. Security protocols have been established for secure group communications (see, for example [18,31,32]), and therefore the uppermost level in the extended ISSI (eISSI) model can be enforced using existing technology. Additionally, a concept called threshold cryptography can be used to justify the feasibility of group behaviour. In traditional cryptography, participants in communications either share a secret key for encryption and decryption of messages or posses a secret key of their own and a private key of other communicating party. Additionally, these keys and different cryptographic algorithms are used for digitally signing documents in order to provide assurance from the identity of a person and to prevent non-repudiation of participation. In threshold cryptography, secrets are divided and distributed to several members of the organisation and commitment into communication requires acceptance of a specified sub group of secret holders. This reduces the possibility of misuse of secrets when some participants are dishonest and reduces the need for sharing full secrets among several parties.

To motivate the new layer, let us briefly summarise the ISSI-model [21]. Technical protection measures are studied regarding the OSI protocol stack. Even though not widely implemented and commonly replaced by TCP/IP protocol suite, OSI provides with a well-established framework for layered communication protocols. It is widely used as reference for education and research of data communication networks. As the focus of this paper is not on actual communication protocols, there is no need to replace this part of the model. On top of technical protection measures is a layer of secure operation of systems. This is well justified since there is a great need to operate systems in a secure manner to make sure security enforcement technologies are properly applied. Further, the ISSI model assumes managerial and administrative layers on top of operational layer. This is on align with commonly agreed view that comprehensive information security requires participation of several administrative layers and strongly depends on the managerial commitment. Inclusion of legal and ethical measures is also justified. As has been shown within this paper, there is a need for legal and ethical measures to provide with comprehensive security of information systems.

Ethics being the top layer has anyhow a significant draw back. As has been shown within this paper, an assumption of ethics being the foundation for security is far too optimistic and can not be enforced due to the heterogenicity of public networks. Therefore, ethics can only be enforced within groups that agree upon common

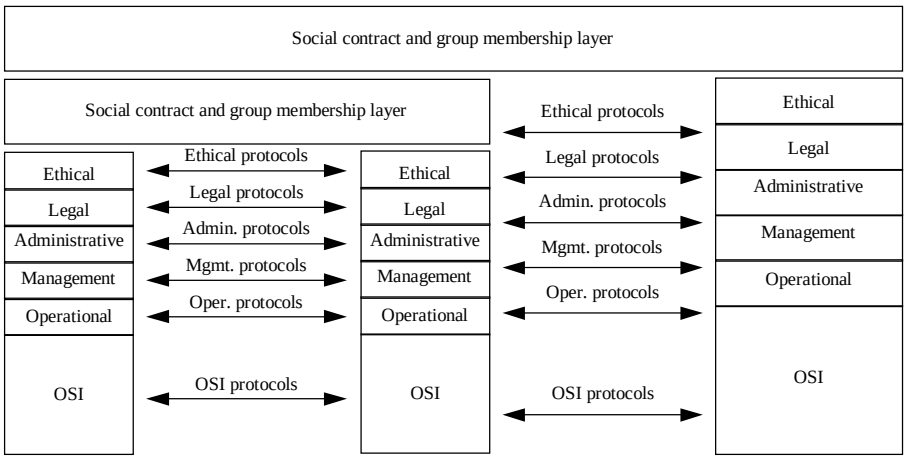

Figure 1. Extended ISSI model

ethical norms and terms of acceptable usage of information systems. This commitment can originate from various factors. Motivating factor towards agreement of common norms for operation of systems at the organisational level could be common business interests. On the individual level, terms of employment or codes of conduct within the peer group can be the driving factor. These assumptions are, anyhow, not valid outside of the groups involved. Therefore, there is a need to extend the ISSI-model by adding a group and social contract layer on top of ethical layer. Each group can be separated from other groups by technical and procedural measures, and ethics and other requirements can be expected to be enforced only within groups. Enforcement of ethical measures among different groups may not necessarily be feasible. In the case of different groups willing to act together to satisfy common objectives, the eISSI framework supports generation of larger groups by combining different potentially hierarchical systems that agree same ethical norms. Construction of a larger group from one independent group and a joint group of two other groups is illustrated in figure 1. The major difference to other layers is that group layer must cover entire system, and no agreements can be trusted over group boundaries.

Protocols for external communication have to be carried out via ethical layer. Especially in the case of potential group inclusion it is important to communicate starting from ethical layer and in the case of positive result, enforce the enhanced ethics within both peer groups. As each member in both groups has agreed the common ethical principles, enforcement of measure group wise is a feasible task. Since the group communication can be carried out in a secure fashion, as provided by secure group communication technologies, the group establishment should be the major concern of non-technical aspects. The two phases are ethics negotiation and ethics enforcement:

Ethics negotiation phase is where organisations or individuals representing themselves negotiate the content of ethical communication agreement over specific communication channels.

Ethics enforcement phase is where each organisation enforces changes in the ethical code of conduct by specifying administrative and managerial routines, operational guide lines, monitoring procedures, and sanctions for unacceptable behaviour.

Organisations or individuals involved in negotiation should code desired ethical norms in terms of acceptable behaviour within the information processing. Agreement should be searched and once reached, contract made and agreed norms enforced throughout the organisation. In the optimal case, ethics has the law enforcement and juridical actions against violations can be prosecuted in court. This may not be the case in most rules, and therefore layers below legal layer are required. First comes the commitment of top management (administrative layer). Top management has a duty of ensuring secure processing of information and authority to set organisation-wide policies, such as norms of acceptable processing of information agreed upon in the ethics negotiation phase. This authority is then delegated to lower management layers (management layer) where the operational procedures are adapted to the changing norms regarding processing of information. Management is in charge of specifying and enforcing (with the support of technical personnel) secure operation (operational layer) of systems in order to satisfy upper level requirements and to make sure that technical protection measures (OSI layers) are adequate and cost-effective. Furthermore, various feed

back mechanisms are implemented to monitor changes in the processing environment and changing requirements. Depending on the severity of required alterations, reflections reach different layers and alterations need to be propagated throughout the organisation to lower layers.

7. Evaluation, conclusions and future work

In the protection of global distributed systems that employ open public networks, there is a great demand to clearly specify what are individuals' rights and responsibilities regarding to those networks. The distributed global nature of networks makes this a significantly difficult task. The lack of centralised authority, and differences in moral codes between different groups, such as original developers of networks, business users, private users and governmental organisations easily lead to significant inconsistencies between operational policies and methods how these policies are enforced. All these groups have significantly different objectives and requirements for the use of networks, and balancing different needs and wishes may be a difficult task.

The obvious question of this arises is that is it possible to have a common communication network to adapt all different needs and requirements. Can network protocols and systems be designed such that all environments and usages are expected to adapt into same fundamental features. Protocol stack design has focused on hiding technical details of lower layers from upper layers, but can fundamental transmission protocols be duplicated under same higher layer protocols to provide varying levels of security without losing the interoperability. Several extensions have been designed to common TCP/IP protocol suite to provide security at IP layer, though fundamental issues of protocol operations may lead to severe security problems. The balance between interoperability, low cost and security is not easy to find.

The issue becomes even more complicated when studying non-technical issues related to security processing of information. Establishment of a common ethics to provide comprehensive protection of information resources in global communication networks is extensively complicated task. Bridging the cap between hackers and information security personnel is difficult, whereas extreme necessary, task. From the ethical point of view, the two approaches towards ethics, consequential presented by hacker community, and deontological presented by the information security community, are the source of conflict. Current trend appears to bridge this cap by law enforcement, that is suggested to be efficient measure against intentional misuse of computing resource, but may on the other hand lead to the increase in the computing underground community.

Several models suggest, that social and ethical measures should be on top of the protection measures to provide with an adequate protection of information in global systems. These measures would establish a base for adequate legislation, where organisations could base their security work on. Currently, it appears that the situation is not as suggested by theories. As there is no consensus on the ethical aspects of information security, the law enforcement is taking the role of providing guide lines on ethical behaviour. This problem has been approached by establishing an extension to the ISSI model for security interconnection of information systems. Extended ISSI-model (eISSI) adds a group establishment and social contract layer on top of ethical measures to provide an approach that is to align with the human behaviour, supports iterative interconnection of different groups, and is feasible within the current technology.

As the focus of this paper has been on the analysis of the need for an extended approach, the two components of the application of group layer at eISSI model, ethics negotiation phase and ethics enforcement phase, have not been studied in detail. The major need for future research is the identification of factors having impact on a successful ethics negotiation phase, and analysing the boundaries of acceptable refinements within organisations. If these issues shall not be addressed, unexpected conflicts may occur and cause severe threats to the security of information systems.

The major question here is, that whether the ethical contract is transitive, and are the changes required in the group expansion acceptable. Therefore, expansion requires broadcasting of new issues throughout organisations to identify possible conflicts with previous rules. Iterative negotiations are required to find a solution that satisfies all parties. Conflicts in requirements may lead to violations of code of conduct, and therefore increase the risk of becoming susceptible to an attack. To support these negotiations, the question arouses on suitable mechanisms for coding ethical norms. Without a generally accepted coding mechanism, group negotiation phase can not be fully utilised. The major area of future research lies in specifying mechanisms for formulating thee norm bases and reason about them.

Normative positions and deontic logic has been applied on the specification of technical security requirements [20] and the most desirable approach should be expansion of these theories to cover entire spectrum of security requirements from technical to ethical and social contract level.

References

[1] *OECD Recommendation, guidelines and explanatory memorandum for the security of information systems*, November 1992.

[2] R.J. Anderson. Crypto in Europe - markets, law and policy. In *Conference on Cryptographic Policy and Algorithms*. Queensland, Australia, 1995.

[3] B. Angerfelt. Computer crimes. a study of different types of offences and offenders. In *IFIP TC11 International Conference on Information Systems Security*, 1992.

[4] D.Bailey. "A philosophy of security management". In M.D. Abrams, S.Jajodia, and H.J. Podell, (ed.), *Information Security: An Integrated Collection of Essays*, pages 98-110. IEEE Computer Society Press, Los Alamitos, CA, 1995.

[5] R. Baskerville. "The threat in security for the adaptive organization". *Information Systems Security*, 2, 1993.

[6] N.S. Borenstein, J. Ferguson, J. Hall, C. Lowery, R. Mintz, M. Joanie, D. New, B. Parenti, M. Rose, S. Einar, L. Stein, C. Storm, E. Vielmetti, M. Weiser, and P-R. Wolff. "Perils and pitfalls of practical cybercommerce". *Communications of the ACM*, 39(6):36-44, 1996.

[7] D.D. Brinkley and R.R. Schell. "Concepts and terminology for computer security". In M.D. Abrams, S. Jajodia, and H.J. Podell, (ed.), *Information Security: An Integrated Collection of Essays*, pp. 98-110. IEEE Computer Society Press, Los Alamitos, CA, 1995.

[8] E.R. Buck. *Introduction to Data Security and Controls*. QED Technical Publishing Group, 2nd edition, 1991.

[9] J.M. Carroll. "A portrait of the computer criminal". In *IFIP TC11 11th International Conference of Information Systems Security*, 1995.

[10] D. Denning. "Concerning hackers who break into computer systems". In *13th National Computer Security Conference*, 1990.

[11] D. Denning. "The U.S. key escrow encryption technology". *Computer Communications*, 17(7), 1994.

[12] W. Diffie. "The impact of a secret cryptographic standard on encryption, privacy, law enforcement and technology". In L.J. Hoffman, (ed.), *Building in Big Brother: The Cryptographic Policy Debate*. Springer-Verlag, NY, 1995.

[13] D. Fiery. *Secrets of a super hacker by the Knightmare.* Loompanics Unlimited, 1994.

[14] T. Forester and P. Morrison. *Computer Ethics. Cautionary Tales and Ethical Dilemmas in Computing*. Basil Blackwell, Ltd., 1990.

[15] P. Gray. *Open Systems: A Business Strategy for 1990s*. McGraw-Hill Book Company, Berkshire, GB, 1991.

[16] A. Hartmann. "Comprehensive information technology security: A new approach to respond ethical and social issues surrounding information security in the 21st century". In *IFIP TC11 11th International Conference of Information Systems Security*, 1995.

[17] M.J. Herskovits. "Cultural relativism and cultural values". In J. Ladd, (ed.), *Ethical Relativism*, pp. 58-77. Wadsworth Publishing Company, 1973.

[18] A. Hutchinson. "gGSS-API: A group enhanced generic security service". In *Proceeedings of the IFIP TC11 13th International Conference on Information Security*, 1997.

[19] D. Icove, K. Seger, and W. VonStorch. *Computer Crime: A Crimefighter's Handbook*. O'Reilly & Assicoates, Inc., 1995.

[20] A.J.I. Jones and M. Sergot. "Formal specification of security requirements using the theory of normative positions". In *ESORICS'92*, 1992.

[21] S. Kowalski. "Computer ethics and computer abuse: A longitudinal study of Swedish university students". In *IFIP TC11 6th International Conference on Information Systems Security*, 1990.

[22] K.E. Laudon. "Ethical concepts and information technology". *Communications of the ACM*, 38(12), 1995.

[23] J. Leiwo. "Deterring computer network criminals with legislative methods: The need for international harmonization". In *Groningen International Information Technology Conference for Students*, 1995.

[24] S. Lichtenstein. "Information system security design principles for adaptive organizations". In *6th Australian Conference on Information Systems*, 1995.

[25] R.O. Mason. "Four ethical issues of the information age". *MIS Quarterly*, 10(1), 1986.

[26] G.R. Meyer. The social organization of the computer underground. Master's thesis, Northern Illinois University, Department of Sociology, 1989.

[27] J.H. Moor. "What is computer ethics". In D.G. Johnson and H.Nissenbaum, (ed.), *Computers, Ethics & Social Values*. Prentice-Hall, Inc., 1995.

[28] K. Nance and M. Strohmaier. "Ethical information security in a cross-cultural environment". In *IFIP TC11 11th International Conference on Information Systems Security*, 1995.

[29] R. Pascale. *Managing on the Edge: How the Smartest Companies Use Conflict to Stay Ahead.* Simon and Schuster, 1990.

[30] C. Piller. "Bosses with x-ray eyes". *MacWorld*, July 1993.

[31] M. Reiter. "A secure group membership protocol". In *IEEE Symposium on Research in Security and Privacy*, 1994.

[32] M. Reiter, K. Birman, and L. Gong. "Integrating security in a group-oriented distributed systems". In *IEEE Symposium on Research in Security and Privacy*, 1992.

[33] B. Russell. *History of Western Philosophy*. George Allen & Unwin Ltd., 2nd edition, 1961.

[34] J. Schopman. "Information technology's ideology makes its user risky". In *IFIP WG9.2 Working Conference on Facing the Challenge of Risk and Vulnerability in an Information Society*, 1993.

[35] R.A. Spinello. *Ethical Aspects of Information Technology*. Prentice-Hall, Inc., 1995.

[36] D.W. Straub, P.J. Carlson, and E.H. Jones. "Deterring highly motivated computer abuser: A field experiment in computer security". In *IFIP TC11 8th International Conference of Information Systems Security*, 1992.

[37] Streeter, R.E. Kraut, H.C. Lucas Jr., and L.Caby. "How open data networks influenced business performance and market structure". *Communications of the ACM*, 39(7):62-73, 1996.

[38] L.F. Young. "Utopians, cyberpunks, players and other computer criminals". In IFIP TC9/WG9.6 Working Conference on Security and Control of Information Technology in Society, 1993.