CHARACTERISTICS AND MEASURES FOR MOBILE-MASQUERADER DETECTION

Oleksiy Mazhelis
Information Technology Research Institute
University of Jyväskylä
P.O. Box35, FIN-40014, Jyväskylä, Finland
mazhelis@titu.jyu.fi

Seppo Puuronen
Department of Computer Science and Information Systems
University of Jyväskylä
P.O. Box35, FIN-40014, Jyväskylä, Finland
sepi@it.jyu.fi

Abstract Personal mobile devices, as mobile phones, smartphones, and communicators can be easily lost or stolen. Due to the functional abilities of these devices, their use by an unintended person may result in a severe security incident concerning private or corporate data and services. Organizations develop their security policy and mobilize preventive techniques against unauthorized use. Current solutions, however, are still breakable and there still exists strong need for means to detect user substitution when it happens. A crucial issue in designing such means is to define what measures to monitor.

In this paper, an attempt is made to identify suitable characteristics and measures for mobile-user substitution detection. Our approach is based on the idea that aspects of user behavior and environment reflect user's personality in a recognizable way. The paper provides a tentative list of individual behavioral and environmental aspects, along with characteristics and measures to represent them.

Keywords: Mobile Terminal Security, User Profiling, Masquerader Detection

1. Introduction

Today, mobile devices have become a convenient and often essential component assisting us in our everyday life. These devices are becoming increasingly powerful, and the number of features and services available

to their users is growing steadily. Some of the abilities of modern mobile devices are essential also from the security perspective. Among them are i) the ability to store (private and corporate) data, ii) the ability to perform mobile e-transactions, and iii) the ability to access a corporate intranet. These abilities pose security concerns, since only the legitimate user of the device should be permitted to access the private data and the corporate intranet, or to carry out mobile e-transactions allowed to the device. While these concerns are common for laptops and networked workstations, the problem is still more severe with mobile devices because they can be more easily lost or stolen – according to [16], 24% of PDA users experienced a loss or theft of at least one of their PDAs. Currently, in order to ensure the legitimacy of a user, an authentication procedure is performed, usually consisting in entering PIN/password by a claimant (a device user whose legitimacy is not verified yet). The authentication process is usually launched when the device is being turned on, or after idle time. However, many users find such protection mechanism inconvenient and do not use it [6]. Besides, sometimes a possibility exists to bypass the authentication procedure, or the authentication password can be compromised thus enabling illegal use of the device. Therefore, there is a strong need for further security means to resist the use of a mobile device by a non-legitimate person.

This paper is aimed at addressing the issue of detective security services in the context of mobile devices. We focus on the problem of *mobile-masquerader detection*, where masquerading can be defined as the use of the device's protected resources by an individual other than the legitimate user. In the context of a mobile device, the protected resources are the device itself along with the information stored on it, and allowed services.

The detective security means are based on the assumption that both normal and malicious activities are manifested in system audit traces, and that malicious activity can be detected through the analysis of these traces. A crucial issue in designing such means is to define what measures to monitor, and what models to assign to these measures [22, 10, 19]. However, the available frameworks, models, methods and approaches for detecting security breaches are often based on various heuristics and intuition of experts (as in [2, 9, 11, 20]), or are largely data-driven (as in [18, 8, 12]). As pointed out by McHugh, many works in intrusion detection have been based on "a combination of intuition and brute-force techniques" [15, p. 14]. Furthermore, these works are targeted at networked workstations and servers, and hence do not take into account the peculiarities of personal mobile devices.

In this paper, we consider the mobile-masquerader detection problem from *user identity verification* (UIV) point of view. The fact that cognitive processes of each human are individual is utilized in the paper. This part of psychological personality is a natural choice to verify one's identity. The difficulty is that the psychological personality cannot be directly observed and measured. To solve this problem, we relate the psychological personality to one's behavior and environment, by using Bandura's social cognitive theory [3] outlined in Section 3.2. Furthermore, the decomposition of human personality into multiple factors according to the multifactor theory of personality [17] as described in Section 3.1 is projected in individual aspects of behavior (considered in Section 4) and individual aspects of environment (considered in Section 5). Thereafter, some characteristics to describe these individual aspects are hypothesized, and the measures to represent these characteristics are proposed in Section 6. While the measures to be assigned to various characteristics are hypothesized in the paper, neither statistical nor other models to be assigned to these measures are considered.

2. Masquerader detection

Intrusion detection is aimed at revealing any deliberate unauthorized attempt to access information, manipulate information, or render a system unreliable or unusable [22]. Among the attacks, which intrusion detection techniques are supposed to detect is the masquerade attack, i.e. an attack performed by an impostor who masquerades as a user with legitimate access to sensitive data.

Intrusion detection approaches may be divided into those based on anomaly detection and those based on misuse detection. Approaches based on anomaly detection track user behavior and try to determine (on the basis of users' personal profiles) whether their current activities are consistent with an established norm. Contrary, misuse detection utilizes the knowledge about unacceptable behavior and directly searches for it.

In the context of masquerader detection, the above two approaches can be described as follows:

- *Masquerader detection via user identity verification.* The first approach involves continuous verification of user identity. In other words, it verifies whether the user is present and alarms if verification fails. This is therefore following the anomaly detection approach in the sense that deviations from an established norm are searched for.

- *Masquerader detection via impostor recognition.* The second approach is complementary to the first one and involves detecting

predefined patterns associated with impostor activity or identity. Thus, it is aimed at detecting the presence of an impostor, and is following the misuse detection approach.

Most (if not all) of the masquerader detection techniques following anomaly detection approach, explicitly or implicitly assume the individuality of user behavior. For example, in the paper presenting neural network intrusion detection, the authors stated that they "believe that a user leaves a 'print' when using the system; a neural network can be used to learn this print and identify each user much like detectives use thumbprints to place people at crime scenes" [18, p. 943], and, later, "the set of commands used and their frequency, therefore, constitute a 'print' of the user, reflecting the task of the user and the choice of application programs, and it should be possible to identify the user based on this information" [18, p. 945].

Analysis of user behavior characteristics has proven fruitful in many approaches to anomaly intrusion detection, whose functioning involve detecting anomalies in user behavior. Probably the most often cited is the statistical approach used in NIDES [1]. More recently, many other approaches have been investigated as reported in [23], [19], [13], [11], [18], [24], and [20], to mention a few. In these approaches, different measures are monitored to model user behavior: frequencies and sequences of Unix shell commands or system calls, temporal parameters of user actions and temporal intervals between them, etc. The reported results indicate the feasibility of the use of these measures for masquerader detection. User behavior has not explicitly been considered. Rather, the choice of characteristics has been data and technology driven, i.e. governed by available data and processing techniques. The choice itself is based either on the intuition of researchers or other experts (as in [18]), or on the supporting knowledge discovery tools juxtaposing the data describing the behavior of different users (as in [12]).

Contemporary masquerader detection techniques may be enhanced. Namely, the set of measures currently employed in masquerader detection is limited and may be extended by taking into consideration individual behavioral and environmental aspects. Additional characteristics and measures may provide further information describing the user, and consequently, the detection accuracy may be improved. Besides, the reported techniques dealt with static hosts; i.e. masquerader detection techniques are rarely tailored to mobile computers or other mobile devices. The work of [25] and [21] taking into account mobility patterns of users for intrusion detection purposes are rather exceptional.

3. Employing personality factors for masquerader detection

Personality can be defined as "a dynamic organization, inside the person, of psychophysical systems that create a person's characteristic patterns of behavior, thoughts, and feelings" [5, p. 5]. From trait perspective, personality traits are considered as dimensions of individual differences that influence patterns of thoughts, feelings and actions [14]. According to [14], these traits represent individual difference variables. In this paper, an attempt is made to employ these individual differences for distinguishing between the user and a substitute, and personality is seen as a complex of relatively enduring aspects which make a person distinct from other individuals.

3.1 Multifactor-systems theory of individuality

Royce and Powell [17] present the theory of individuality and personality, which is "a comprehensive theory about how individuals differ from each other psychologically and how such differences give rise to differences in integrative personality, including world view, life style and self-image" [17, p. 5]. The theory hypothesizes that personality is composed of mutually interacting sensory, motor, cognition, affect, style, and value systems. The total psychological system is defined to be "a hierarchical organization of systems, subsystems, and traits that transduce, transform, and integrate psychological information" [17, p. 10].

According to the theory, personality is hierarchically organized. The six systems comprising personality can be divided into high-, middle- and low-level systems (Figure 1). The higher level systems in comparison with lower level systems "are concerned with longer units of time"; "have a higher priority of action", "are more closely related to the deeper (in the sense of significant) levels or aspects of personality" [17, p. 12]. Each system itself is further considered to include several subsystems. Moreover, each system is decomposed into a hierarchy of factors at several levels, from the lowest-level factors (first-order factors) to highest-level factors indicating the systems and subsystems of personality.

Factor values determine processes within various personality systems, e.g. values of the factors of the value system describe goal-seeking processes. At the same time, the goals established are not processes any more but rather "records in memory", i.e. storages. Such storages include goals established, the knowledge (operators, invariants) obtained, and the motor programs constructed. Due to individual differences and due to differences in learning environments, the content of the storages

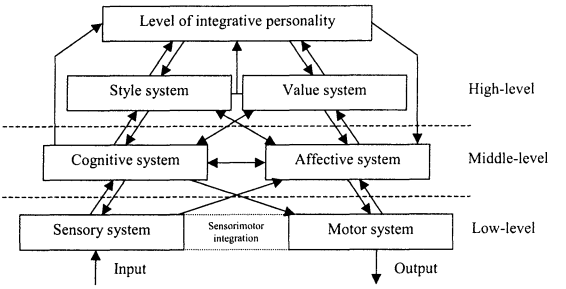

Figure 1. Integrative personality model [17, p. 12]

may also be individual. Thus, in addition to the variety of factors, the content of these storages comprise the personality of a human.

Taken together, the values of the personality factors along with the storage content can be thought of as an array of values describing, or encoding, one's identity. It is reasonable to assume that such identity description is peculiar for each human being. A superposition of the factor values is assumed to "identify a processor" [17, p. 47]. Therefore, an evident approach to the user identity verification would be to match a claimant's factor values against the previously acquired factor values of the legitimate user. The problem with such an approach is that it is highly difficult to obtain factor values automatically not to speak about user-friendliness. As referred by [7, p. 9], the traits "are not directly observable; they are inferred (as any kind of determining tendency is inferred)". The process of factor inference may involve for example answering specific questions or interview. In the context of UIV, such method would not be appropriate. Therefore, instead of inferring factor values, an alternative approach based on Social Cognitive Theory is adopted in this paper.

3.2 Social Cognitive Theory

Social Cognitive Theory considers psychological and biological personality of a human, his/her behavior, and environment as mutually interfered. According to the theory, a complex network of reciprocal influences between personality, behavior, and environment frames the being of human. The theory considers behavior of an individual being uniquely determined by personality, behavioral, and environmental factors, and largely regulated through cognitive processes. This suggests

that the mind has an active role when an individual constructs his/her own reality [4].

In treating mobile-masquerader detection as user's identity verification, the fact that inherent constituents of human personality – cognitive structures and processes – are individual for each user can be employed. Due to the reciprocal determinism described in the Social Cognitive Theory, this individuality affects one's behavior and environment. Consequently, it is possible to assume that some aspects of behavior and environment are individual as well. The superposition of these individual behavioral and environmental aspects constitutes the reflection of one's personality, and thus it may be used to differentiate individuals. In two subsequent sections, some of these individual aspects of behavior and environment are hypothesized.

4. Individual behavioral aspects

While psychological personality is latent, it influences the individual's behavior and individual's environment, which can be observed more easily. The personality can be considered as reflected in some *aspects* of one's behavior and environment. In turn, the characteristics describing these behavioral and environmental aspects can be thought of as functions of multiple variables; some of these variables are personality factors. Since the superposition of factor values is individual, it is possible to hypothesize that the superposition of values of characteristics describing one's behavior and environment is also individual. Therefore, the behavioral and environmental characteristics reflecting personality can be used to verify the identity of a person.

To consider individual aspects of user behavior, we have categorized various behavioral aspects into three hierarchical levels: high, middle, and low levels corresponding to the division of personality systems into three levels (Section 3.1). The high-level aspects are hypothesized to reflect/manifest the peculiarities of high-level personality systems, i.e. the style and the value systems. Accordingly, these aspects are supposed to describe behavior that occurs over long time periods, involves selection of particular mode of action, requires high-level coordination, etc. In turn, middle- and low-level aspects of behavior manifest the peculiarities of respectively middle- and low-level personality systems.

For each of the three hierarchical levels, we consider the personality factors as well as the content of storages (goals, operators, invariants, and motor programs). As a result, a set of individual aspects of observed behavior have been recognized; these aspects are discussed below.

- High-level behavioral aspects reveal the peculiarities of values and styles of a user. The values determine what goals are selected, while styles determine how the stated goals are to be achieved. The following high-level aspects are recognized:
  - *Way of obtaining information (e.g. through communication with people, web-browsing, services).* This aspect is assumed to reflect the individuality of operators and goals, which in turn are influenced by factors of the value system, the affective system, etc.
  - *Way of communication with others (calls, email, SMS, etc.).* It is hypothesized that difference in operators is reflected in this aspect.
  - *Way of performing tasks.* It is assumed that sequences of actions employed, frequency of different sequences of actions, and other characteristics describing how the user carries out his/her tasks reflect the individuality of user operators and goals.
  - *Movements (routes, speed of movements, etc.).* As above, this aspect is assumed to manifest individuality of user operators and goals.
  - *Time/efforts devoted to work/businesses.* Need for endurance (a factor of the value system) is supposed to partly determine this aspect of behavior.
  - *Time/efforts devoted to entertainment.* Need for play (a factor of the value system) is supposed to be reflected in this aspect.
  - *Changes in behavior.* Need for change (a factor of the value system) is supposed to be reflected in this aspect. Behavioral changes implied here concern the behavior that is intentionally coordinated and regulated by a human, i.e. they concern high-level aspects of behavior.
- Middle-level behavior reflects the transformational processes within the cognitive system where the external information is processed in order to identify environmental invariants, and within the affective system where the cognitive information is processed in order to achieve the optimal internal arousal states. The peculiarity of these systems is manifested in the following behavioral aspects:
  - *Concepts used* are assumed to reflect individual differences in invariants.

  - *(Speed of) comprehension* is assumed individual as it is determined by multiple factors of the cognitive system (perceptual speed, verbal comprehension, memory span, associative memory, etc.).
  - *Decision making (e.g. time to respond).* Individuality of this aspect may be attributed to multiple factors of the cognitive system (perceptual speed, verbal comprehension, memory span, associative memory, memory for design, induction, deduction, spontaneous flexibility, etc.), but also to factors of the style system (e.g. reflection/impulsivity).
  - *Accuracy.* Personality factors of the cognitive system (deductive reasoning and spontaneous flexibility) and the affective system (surgency, autonomic balance, etc.) are hypothesized to influence this behavioral aspect.
  - *Disposition towards communication.* This aspect is assumed to be partly regulated by factors of the affective system (e.g. self-sufficiency, self-sentiment), but also by factors of the value system (e.g. need for exhibition).

- Low-level behavior is mainly regulated by the sensory and the motor personality systems responsible for transforming the environmental information into psychological information and back respectively. The individual behavioral aspects at this level are:

  - *Way of writing.* Individuality of this aspect may be explained by individuality of motor system factors (e.g. the dexterity and speed of small movements), motor programs (a dictionary of letters, rules to produce words, etc.), but also by the individuality of control-decision processes within the cognitive and the affective systems.
  - *Way of typing.* As above.
  - *Voice.* This aspect may be attributed to factors of the motor system (articulation, phonation, respiration), but also to factors of the cognitive and the affective system.

The above list of individual behavioral aspects does not pretend to be complete. These behavioral aspects were identified deductively by analyzing the factors suggested by [17]. While they recognize around 200 factors, for many of them we have not managed to reveal a linkage with observable behavioral aspects. Some aspects corresponding to other or the same factors may have been overlooked, and further analysis might reveal other aspects to be added to the list.

5. Individual environmental aspects

Above, it was hypothesized that due to the influence of personality on behavior, some aspects of human behavior are individual; furthermore, due to the influence of user personality through user behavior on his or her environment, some environmental aspects may also be individual (a person selects environment that fits his/her own personality). Individual aspects of behavior were considered in the previous section. In turn, this section is devoted to individual environmental aspects.

In the process of inferring individual environmental aspects, they are classified into high-, middle-, and low-level aspects. Similarly to the division of behavioral aspects, the division of environmental aspects is aimed at making the process of inference more structural. High-, middle-, and low-level environmental aspects are supposed to reflect respectively high-, middle-, and low-level personality systems. For each level, it is analyzed what aspects of environment could reflect the individuality of factors and storages of this level. As a result of this analysis, the following individual aspects of environment are hypothesized.[1]

- High-level environmental aspects are regulated by the factors and storages of the value and style systems determining the goals of a user and the ways to attain them. The individual environmental aspects of high level are:
  - *Choice of people to contact with.* This aspect is hypothesized to reflect the individuality of user goals and to a certain degree operators, but also the individuality of factors of the value system (e.g. need for affiliation, and need for nurturance).
  - *Choice of places to visit.* Individuality of places a user visits can be attributed to the individuality of goals, but also to the individuality of factors. Goals and operators partly determine the places a user has to visit, while needs and interests partly determine the places a user wants to visit.
  - *Choice of (software) tools.* Individual tools are supposed to be chosen according to individual goals, but also according to individual factors of the cognitive system (memory span, associative memory, etc.) and individual cognitive styles.
  - *Changes in the choice of environment.* Similarly to the above-mentioned aspect of changes in behavior, changes in the choice

[1] We limit the environmental aspects to those that may interact or otherwise contact with the device.

of environment are supposed to reflect the need for change (a factor of the value system). These changes correspond to changes in high-level environmental aspects, e.g. changes in places visited.

- Middle-level aspects of environment reveal the peculiarity of user's cognitive and affective systems involved in the processes of identifying invariants and attaining emotional activation needed. So far, only one aspect is recognized:
  - *Tendency of "being on-line"* is assumed to reveal the individuality of factors of the cognitive system (perceptual speed, verbal comprehension, extraversion, etc.), but also the need for exhibition (a factor of the value system).
- Low-level environmental aspects are determined by the factors from the low-level personality systems (sensory and motor) implementing the transformation between psychological information and physical energy. Among these aspects are:
  - *Choice of screen resolution.* It is hypothesized that the choice of screen resolution is partly determined by the visual acuity (a factor of the sensory system).
  - *Choice of volume level.* The choice of volume level is partly determined by the auditory acuity factor of the sensory system.

As well as the list of behavioral aspects proposed in previous section, the list of environmental aspects is unlikely to be complete. Further analysis may reveal other aspects reflecting personality factors and storages. The list therefore should be treated as initial and it should serve as a basis for further refinement.

6. Characteristics and measures

The personality factors and storages are latent and hence cannot be directly observed and measured. However, according to the Social Cognitive Theory (Section 3.2), they are reflected in different *aspects* of *behavior* and *environment*; some of these aspects are hypothesized in previous sections. Each of these behavioral and environmental aspects, in turn, may be described by one or several *characteristics*. For example, the accuracy in typing can be taken as a characteristic describing "accuracy" (middle level aspect of behavior). Tentative characteristics to describe various individual behavioral and environmental aspects hypothesized in previous sections are presented in Figure 2.

Personality reflected in behavior			Personality reflected in environment		
Level	Aspect	Characteristics	Level	Aspect	Characteristics
High	Way of communication with people, and performing other actions	• Device's facilities usage • Sequences of actions followed • Temporal lengths of actions • Temporal intervals between actions in a sequence • Use of shortcuts vs. use of menu	High	Choice of people to contact with	• People contacted with, conditioned on type of communication, time, etc.
	Paths of movements	• Routes taken • Speed of move conditioned on route/time		Choice of places to visit	• Places visited, conditioned on time of day, week, etc.
	Endurance	• Length of work day		Choice of tools	• Set of software installed
	Changes	• Changes in behavior		Changes	• Changes in environment
Middle	Comprehension	• Time of reading a unit of textual information	Middle	"Being online"	• Time, when the user (or device) are online
	Decision making	• Time between incoming event and response			
	Concepts used	• Words or phrases used more often			
	Accuracy	• Accuracy in typing, in menu item selection, etc.			
	Disposition towards communication	• Time devoted to communication			
Low	Voice	• Statistical characteristics of voice	Low	Choice of screen resolution	• Current screen resolution
	Way of typing	• Temporal characteristics of keystrokes		Choice of volume level	• Volume level
	Way of writing	• Pressure, direction, acceleration, and length of strokes			

Figure 2. List of distinctive characteristics

For the purposes of automatically distinguishing the user and impostors, the behavior and environment, as reflecting the personality of a user, should be described by quantitative measurements. The model describing the regularities of these measurements should be created and stored for further reference during the verification process. Finally, the verification process is based on the comparison of current measurements against the information in the reference model. If the comparison reveals significant dissimilarity, it may indicate that a user substitution has taken place.

Table 1. Tentative measures to be employed in mobile-user masquerader detection

Characteristic	Measures (observable variables)
Device's facilities usage	Temporal interval between two consecutive evocations of a program or service of a same type
Device's facilities usage	Type of program or service evoked
Sequences of actions followed	Sequences of n actions
Temporal lengths of actions	Temporal lengths of actions
Temporal intervals between actions in a sequence	Temporal intervals between subsequent actions
Use of shortcuts vs. use of menu	For each menu command with shortcut, the chosen option
People contacted with, conditioned on type of communication, time, etc.	Phone number, e-mail address, or other address information of the contacted people
Routes taken	Sequence of cells traversed between two consecutive prolonged stops
Speed of move conditioned on route and time	Speed of move conditioned on route and time
Places visited, conditioned on time of day, day of week, etc.	Locations where prolonged stops were made
Length of work day	Time that the terminal is in the place affiliated with the user's workplace(s)
Changes in behaviour and environment	Changes in behavioural and environmental characteristics
Time of reading a unit of textual information	Time during which a document is open for reading
Time between an incoming event and response	Temporal interval between an incoming message (e.g. e-mail or SMS) is read and the response is written
Words or phrases used more often	Frequency of different words used in a piece of handwriting (with stylus) or typing
Accuracy in typing, in menu item selection, etc.	The ratio of errors (mistyped keystrokes, errors in menu item selection, etc.) to the overall number of actions
Time devoted to communication	Time during a day spent for communication (using terminal) including different types of communication (calls, e-mails, etc.)
Time, when the user is online	Time, during which the communication facilities of the terminal are not deliberately restricted
Statistical characteristics of voice	Cepstrum coefficients of the signal power
Temporal characteristics of keystrokes	Key duration time, inter-key latency time
Pressure, direction, acceleration, and length of stylus strokes	Pressure, direction, acceleration, and length of strokes
Set of installed software, current screen resolution, volume level	Changes of device configuration

In order to be able to measure quantitatively the characteristics of user behavior and environment, one or more appropriate *observable variables*, or *measures* should be assigned to each of them. These variables can be directly measured, and the results of the measurements can be stored as numerical or categorical values. Possible measures to be assigned to the distinctive characteristics are proposed in Table 1. For example, the ra-

tio of mistyped keystrokes to the overall number of typed keystrokes may be employed as a measure to represent the characteristic of "accuracy in typing". Three characteristics – set of installed software, current screen resolution, and volume level – can be represented by a same measure indicating whether a change of configuration has been made. Therefore, these three characteristics were united in the table into a single characteristic.

7. Conclusions

Traditionally, the problem of deterring the use of lost or stolen mobile devices is addressed by the means of authentication at the preventive stage, and by the means of masquerader detection at the detective stage. The masquerader detection is usually approached through the detection of anomalous changes in user behavior and environment, or through the recognition of behavior and environment, which is common for impostors. The proposed solutions to the detection problem including frameworks, models, techniques, etc. are often based on heuristics, the experience or intuition of experts, or are data-driven. Such adhocness is likely to be one of the reasons making the development of new and improved solutions with high detection accuracy difficult.

Theories from the domain of psychology offer an opportunity to extend the viewpoint of a research dealing with masquerader detection. Using these theories, it is possible to explain the differences in human behavior and environment by differences of cognitive processes and psychological/biological factors. Applied in the security context, such theories shift the focus of research from the heavily technological aspects of the problem to the social and individual aspects concerning the human being interacting with the device. Such shift in focus may be useful for deepening the theoretical background of the masquerader detection, for determining the limitations of the contemporary research and thereafter for the development of improved solutions to the problem.

In this paper the mobile-masquerader detection problem is seen as a problem of verifying user identity. The behavior and environment are considered as reflecting the personality traits of a user. Accordingly, by analyzing certain aspects of behavior and environment, the user identity claim can be accepted or denied. A set of characteristics and measures potentially useful for mobile-masquerader detection has been proposed in the paper; however, further empirical research is needed in order to evaluate their suitability.

References

[1] D. Anderson, T. Lunt, H. Javitz, A. Tamaru, and A. Valdes. Detecting unusual program behavior using the statistical components of NIDES. SRI Technical Report SRI-CRL-95-06, Computer Science Laboratory, SRI International, Menlo Park, California, May 1995.

[2] Debra Anderson, Thane Frivold, and Alfonso Valdes. Next-generation intrusion detection expert system (NIDES): A summary. Technical Report SRI-CSL-95-07, Computer Science Laboratory, SRI International, Menlo Park, California, May 1995.

[3] A. Bandura. *Social Foundations of Thought and Action: A Social Cognitive Theory.* Englewood Cliffs, NJ: Prentice Hall, 1986.

[4] Albert Bandura. Social cognitive theory. *Annals of Child Development*, 6:1–60, 1989.

[5] C.S. Carver and M.F. Scheier. *Perspectives on personality.* Allyn and Bacon, Boston, 4 edition, 2000.

[6] Nathan L. Clarke, Steven M. Furnell, Philip M. Rodwell, and Paul L. Reynolds. Acceptance of subscriber authentication methods for mobile telephony devices. *Computers & Security*, 21(3):220–228, 2002.

[7] H. J. Eysenck. *The structure of human personality.* Methuen, London, 3 edition, 1970.

[8] Anup K. Ghosh, Aaron Schwartzbard, and Michael Schatz. Learning program behavior profiles for intrusion detection. In *1 st USENIX Workshop on Intrusion Detection and Network Monitoring*, pages 51–62, Berkeley, CA, USA, April 1999. USENIX Association.

[9] Steven A. Hofmeyr, Stephanie Forrest, and Anil Somayaji. Intrusion detection using sequences of system calls. *Journal of Computer Security*, 6(3):151–180, 1998.

[10] Terran Lane. *Machine Learning Techniques for the Computer Security Domain of Anomaly Detection.* Ph.D. thesis, Purdue University, W. Lafayette, IN, 2000.

[11] Terran Lane and Carla E. Brodley. Temporal sequence learning and data reduction for anomaly detection. *ACM Transactions on Information and System Security*, 2(3):295–331, 1999.

[12] Wenke Lee and Salvatore Stolfo. A framework for constructing features and models for intrusion detection systems. *ACM Transactions on Information and System Security (TISSEC)*, 3(4):227–261, 2000.

[13] Roy A. Maxion and Tahlia N. Townsend. Masquerade detection using truncated command lines. In *Proceedings of the International Conference on Dependable Systems and Networks*, pages 219–228, Los Alamitos, California, June 2002. IEEE Computer Society Press.

[14] R. R. McCrae and Jr. Costa, P. T. *Handbook of personality: Theory and research*, chapter A five-factor theory of personality, pages 139–154. Guilford, New York, 2nd edition, 1999.

[15] John McHugh. Intrusion and intrusion detection. *International Journal of Information Security*, 1(1):14–35, 2001.

[16] Pointsec Mobile Technologies. Half of all corporate PDAs unprotected despite employer risk. Pointsec News Letter 2, Available from http://www.pointsec.com/news/news_pressroom.asp (read 25.04.2005), June 2004.

[17] Joseph R. Royce and Arnold Powell. *Theory of personality and individual differences: factors, systems and processes.* Englewood Cliffs, NJ: Prentice Hall, 1983.

[18] Jake Ryan, Meng-Jang Lin, and Risto Miikkulainen. Intrusion detection with neural networks. In Michael I. Jordan, Michael J. Kearns, and Sara A. Solla, editors, *Advances in Neural Information Processing Systems*, pages 943–949, Cambridge, MA, USA, 1998. The MIT Press.

[19] Karlton Sequeira and Mohammed Zaki. ADMIT: anomaly-based data mining for intrusions. In David Hand, Daniel Keim, and Raymond Ng, editors, *Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 386–395, Edmonton, Alberta, Canada, 2002. ACM Press.

[20] Jude Shavlik and Mark Shavlik. Selection, combination, and evaluation of effective software sensors for detecting abnormal computer usage. In *Proceedings of the 2004 ACM SIGKDD international conference on Knowledge discovery and data mining*, pages 276–285. ACM Press, 2004.

[21] Bo Sun, Fei Yu, Kui Wu, and Victor C. M. Leung. Mobility-based anomaly detection in cellular mobile networks. In Markus Jakobsson and Adrian Perrig, editors, *Proceedings of the 2004 ACM workshop on Wireless security*, pages 61–69. ACM Press, 2004.

[22] A. Sundaram. An introduction to intrusion detection. *ACM Crossroads*, 2(4):3–7, 1996.

[23] S. Upadhyaya, R. Chinchani, and K. Kwiat. An analytical framework for reasoning about intrusions. In *20th IEEE Symposium on Reliable Distributed Systems*, pages 99–108, New Orleans, LA, October 2001.

[24] Dit-Yan Yeung and Yuxin Ding. Host-based intrusion detection using dynamic and static behavioral models. *Pattern Recognition*, 36(1):229–243, 2003.

[25] Yongguang Zhang and Wenke Lee. Intrusion detection techniques for mobile wireless networks. *Wireless Networks*, 9(5):545–556, 2003.