Conceptual security system design for mobile platforms based on human nervous system

Nanda Kumar Thanigaivelan, Ethiopia Nigussie, Seppo Virtanen, and Jouni Isoaho

Department of Future Technologies, University of Turku, Turku, Finland
{nakuth, ethnig, seppo.virtanen, jisoaho}@utu.fi

Abstract. We present the conceptual security system design for mobile platform based on the human nervous system in order to achieve security resilience against threats. The reason for imitation of the human nervous system is to achieve distributed decision making and instinctive reaction against threats by observing the entire device activities. The system is adapted to have the functionalities of the nervous system through the creation of event detection and controlling mechanisms. The two main subsystems, brain and spinal cord, are created through sharing of security related operations in order to act independently without contradicting each other's decisions. The brain comprises of modules that handles the incidents and learning of behaviours to realise holistic view of security against ongoing activities. The spinal cord is responsible for spawning receptor and effector pairs against application activities to establish a medium to communicate and exercise control over them. Some of the factors that influence the method of implementation are usability, acceptability and the type of learning algorithms.

Keywords: Bio-inspired system design · Mobile device security · Human nervous system based security.

1 Introduction

The usage and dependency of smart devices, such as mobiles and tablets, are ever increasing in day-to-day activities as they offer numerous benefits through the applications. The applications can be obtained either free or purchasable from their respective official channels. Mobile devices established itself as a primary focal point of contact by offering different medium for communication, e.g., Wi-Fi, data networks and Bluetooth. In future, the usage of smart devices are predicted to outpace desktops and laptops usage [1, 2]. The amount of data traffic through smart devices are predicted to exceed 77 Exabyte per month [3, 4] and internet accessibility of mobile users is estimated to reach more than 5.7 billion by 2022 [4]. The fact that smart device applications access users personal information and engages in information exchange with external networks stresses on securing communication medium is an essential task.

Smart devices are also forms a part of IoT ecosystem which has been deployed extensively in multiple fields over different identities such as smart cities [5–7],

smart health[10, 11] and smart transport [8, 9]. Mobile devices plays crucial role in IoT, for instance, in smart health applications, mobile devices acts either as a controller or coordinator, and also acts as information accumulator and exchanger. From these factors, it can be concluded that

- communication medium will be used extensively
- data generation and handling through smart devices will increase exponentially
- may attract threats to applications which in turn causes potential monetary losses and human lives in worst case.

Several security mechanism are available to strengthen the communication medium from being exploited by the attackers. Existing solutions, such as firewall, can handle threats efficiently provided they are used together. For example, firewall coupled with intrusion detection/prevention system (IDS/IPS) are efficient in protecting systems against threats spreads through communication medium. In smart devices scenario, firewall coupled with IDS/IPS may enforce additional overhead in terms of energy usage and operations. These solution cannot be applied without modification since they designed as a closed system. Changes are required in the existing security mechanisms at architectural level in order to use across different application scenarios. Thus, a requirement exists for a security mechanism based on completely new architecture that can cooperate with other subsystems, react to threats instinctively and have holistic view of security related events encountered through communication medium and application activities.

In this work, a conceptual design of security mechanism derived from human bio-mechanism is presented. The newly proposed security mechanism will apply measures against threats without human or other (sub) system intervention. Since the mechanism based on human bio-mechanism, each smart devices, e.g., tablets and mobiles, will be considered as a human body, and the applications, resources and communication medium will act as body parts. The contribution of this work are as follows:

- Introduction and adaptation of human nervous system: A conceptual level system design adaptation of human nervous system in the security of mobile devices in order to handle events triggered by the applications and services.
- Advantages and implementation challenges: The advantages of the security system based on human nervous system and the factors that impose serious challenges during the system development process, different implementation possibilities in the mobile platforms are discussed.

The paper is organised as follows. In section 2, our inspiration from human nervous system are discussed. The system design, adaptation of nervous system and operations are given in section 3. In section 4 and 5, challenges in the implementation and summary are presented.

2 Human Nervous System

Human nervous system (HNS) is one the complex system in the human body. It attaches itself with every body parts of the human body and establishes communication medium, which is used to transmit and receive signals. This allows human body to react against any physical events, e.g., pressure, pain and touch, and non-physical events, such as heat, warm and cold. Sensory, integration and motor are 3 main functions of nervous system.

Sensory is carried out by the sensory nerves system. It gather signals from receptors which are responsible for observing internal and external environment activities. The gathered signals will be forwarded to central nervous system. *Integration* is handled by the spinal cord and the grey matter in the brain. During integration, the gathered signals are stored or discarded in memory, processed and used for making decisions. *Motor* functions are responsible for the execution of the instructions sent by the brain or by the dorsal horn. Motor nerves receives the brain signals and produce appropriate actions, for instance, moving a part of the body or generating hormones. The overview of human nervous system is given in Figure 1.

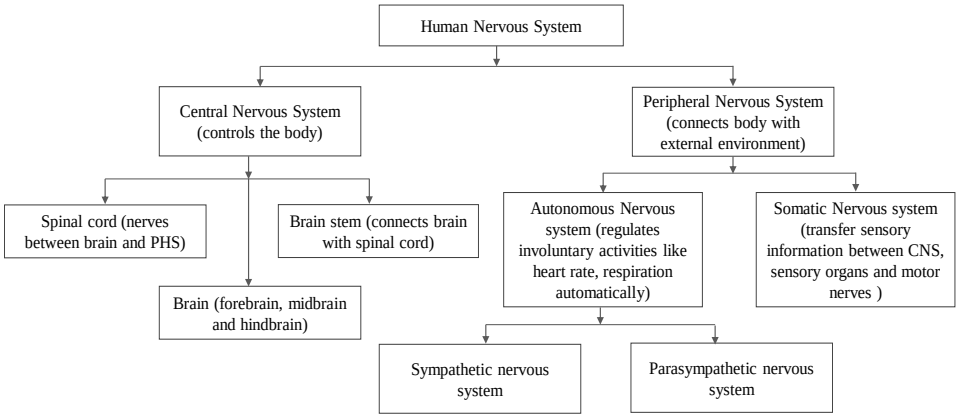

Fig. 1. Overview of human nervous system

Central nervous system (CNS) and *peripheral nervous system* (PHS) are two classification of human nervous system. CNS consists of *brain* and *spinal cord* nerves whereas PHS comprises of nerves other than CNS nerves, including motor and sensory nerves [12]. The motor nerves responsible for receiving instructions from brain while sensory nerves responsible for transmitting signals to CNS.

Sensory nerves receives signals from the receptors and forward the same to brain through spinal cord. Brain replies with instructions to the motor nerves to take appropriate actions for received signals. Brain acts as a central hub for nervous system. It stores encountered incidents, compare new incidents against

past archived incidents and makes decision. Spinal cord acts like convergence point where signals are collected and forwarded to brain. Also, it receives signals from brain and forward to nerves to act as instructed.

A special pain receptor, called *nociceptor*, responsible for handling pain signals. Nociceptor is classified into two, *A-fibre* and *C-fibre*, to facilitate signal communication that requires fast and slow sensational responses respectively [14, 15]. *Dorsal horn*, which exists in spinal cord, plays important role in handling the signals [13]. Depending upon the intensity of the pain detected by the nociceptor, decision to handle those signals will be made by brain or dorsal horn. For example, when hand came into contact with a hot utensil which would result in instantaneous withdrawal of hand away from the utensil, followed by responses such as shouting, crying and prolonged burning sensation. In this example, instantaneous withdrawal is the decision made by dorsal horn and remaining sensational reactions are handled by the brain according to the past incidents which are archived as references. C-fibre handled the slower prolonged burning sensation whereas the quick sharp pricking sensation during skins contact with hot utensil is handled by the A-fibre.

Human nervous system attracted our focus through its seamless flow execution of functionalities simultaneously. Furthermore, human nervous system operates in both centralised and de-centralised manner depending of the circumstances. Hence, a system designed based on nervous should also share its traits such as architecturally reactive, different decision makers, fast and slow communication medium.

3 Security System Design

In this section, security mechanism design including adaptation of human nervous system and potential advantages are discussed. The newly proposed mechanism control applications communication activities by planting numerous receptors and effectors on application basis in the smart device.

3.1 Adaptation of human nervous system for mobile security

To design system operations similar to human nervous system, 2 decision making engines, equal to brain and dorsal horn (spinal cord), are required. Though one decision making engine, dorsal horn, do not perform constant decision making or permanent information management, it must operate independently to a certain degree in order to take action without brain‘s intervention. To achieve this kind of system operations, system architecture should be neither centralised nor decentralised in nature.

Brain and dorsal horn (spinal cord) operations should be created, segregated and shared among 2 subsystems. Spinal cord subsystem should control the communication flow among other subsystems. It also should have the ability to create and attach receptor and receptor pairs on any application activities.

Major modification requirements are: *operation segregation*, *spawning receptor and effectors*, and *faster and slower communication medium* within the subsystems. These requirements need to be defined clearly and ingrained into the system design to achieve security mechanism functions similar to human nervous system.

- *Operation segregation*: The brain and spinal cord functions must be defined and implemented separately as two individual subsystems. These 2 subsystems can have several modules to handle different functions simultaneously. Furthermore, brain subsystem should be defined as such that it can manage and coordinate with multiple spinal cord subsystems in parallel. Spinal cord subsystem also able to function with multiple brain and coordinate with other spinal cord subsystems. This independent operability and multiple coordination ability helps to achieve minimum resilience against threats at any given point of time.
- *Spawning receptors and effectors:* Receptors operate as sensory organs in spinal cord and react to any events. Effectors play crucial role, as primary control points through brain and spinal cord controls and regulate the events sensed by the receptors. Effectors, in the nervous system, are plain as such that they can increase or decrease the intensity of a response based on the received signals. Similarly, security mechanism should able to create plain effectors whose actions can be determined by the instructions of brain and spinal cord subsystem.
- *Fast and slow communication:* Similar to human nervous systems A-fiber and C-fiber, security mechanism should have 2 separate medium for exchanging information between the subsystems and receptor and effector pairs. It is essential because A-fiber type of communication will be used during distress times and C-fiber used under normal circumstances. Hence, system know that if they receive A-fiber signals, they should react quickly by pausing other tasks which are under execution in subsystems.

3.2 Conceptual Design

Security mechanism should consists of all the subsystems discussed in section III-A. Inclusion of those subsystem will completely change the architecture which would result in architecturally reactive mechanism. The system design adapted from human nervous system is given in Figure 2.

Brain subsystem: Brain act as a core of the security mechanism. It comprises of artificial intelligence (AI) block and 2 handler blocks: incident handler and repository handler. *AI block* will perform operations such as establishing behavioural patterns, assist in decision making process for the incidents reported by the receptors through spinal cord subsystem. Behavioural pattern establishment is crucial for the entire security mechanism. It will help incident handler to make decisions from the past learned incidents along with the user configuration settings. *Incident handler* receive the events detected by the receptors and

determines any actions need to be executed depending on the settings. Incident handler also archive the incidents through repository handler. *Repository handler* is responsible for handling entire transmission targeted towards repository. Repository holds the encountered event information by the spawned receptors. It will store the learned outcomes of AI for future references if same incidents are encountered.

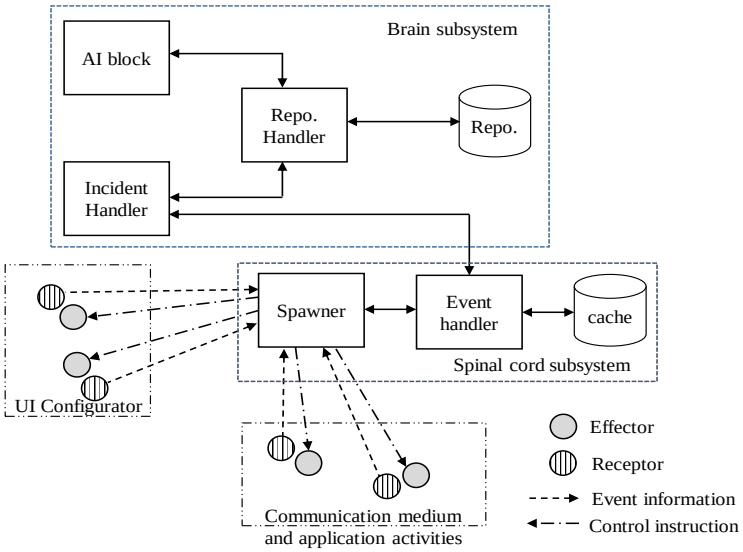

Fig. 2. Adapted system design based on human nervous system

Spinal cord subsystem: It comprises of 2 modules: spawner and event handler, and a cache for quick access to incidents. *Spawner* is responsible for the entire life cycle management of receptor and effector pairs. Through spawner, spinal cord will possess the ability to spawn the receptor and effector pair on every detected events from the application activities. Spawning receptor and effector pairs are crucial for the entire system operations as every event detection and its appropriate responses are based on them. Spawner also maintain information such as number of spawned receptor and effector pairs, active duration of the pairs employment and the activities performed by the application within the employed duration. These information will be sent to brain and stored in repository until they are required. Spawner also handles the UI configurator subsystem through the receptor and effector pairs, and employs low speed communication to handle events triggered by the pairs.

Event handler receives event information from spawner and determine its status, i.e., event or incident. If the decision falls under latter case, event handler will take appropriate counter measures by sending instructions through the established receptor and effector pairs. It will also forward the same incident to the brain for further instructions. In *cache*, spinal cord stores the receptor and

effector pair details and critical incident responses. This will help spinal cord to react quickly and independently before brain gets notified. Spinal cord spawns receptor and effector pair to communication mediums, e.g., Wi-Fi, to monitor and control the activities in those medium.

UI configurator: UI configurator allow users to configure the security mechanism by providing easy-to-use interface. It also provides information related to spawned receptor and effector pair, detected activities and appropriate response made by the security mechanism.

Table 1. Challenges in the implementation

	Platform customisation	Application
Features implementation	All features are implementable by following recommended programming practices	It is not possible to implement all features by following recommended programming practices.
Execution implications	Security mechanism will function normally even after platform version upgrades.	Application may crash, i.e., fail to execute properly, after platform upgrades if disapproved programming practices are employed.
Ease of install	Quite complex for non technical users. Requires flashing of mobile operating system (OS).	Easy to install from application repository, e.g., Google play and Play store.
Multiple device support	Quite tedious to support across multiple mobile devices as it requires libraries from corresponding manufacturers.	Easy to develop as an application for multiple mobile devices, e.g, Samsung, Pixel, Nexus.
Ease of acceptance	Users may hesitate to accept and may become suspicious due to the usage of customised platform. It is not possible to uninstall the application, entire OS should be reflashed.	Users can accept easily as they can install and use the application. Application can be uninstalled, if user feels uncomfortable.
Version upgrades	Entire platform has to be modified and released to upgrade the versions.	Only application need to be changed to release upgrades.
Device warranty implications	Warranty may become void due to flashing of custom OS and unlocking boot loader.	Do not break the warranty of the mobile devices.

3.3 Potential advantages

Nervous system controls the entire activities of the human body, e.g., gentle and forceful movements. It regulates the active and passive activities, such as voluntary movement of legs and rate of heart beat, which in turn helps to protect the body internally and externally. Therefore, a system that follows the same approach as nervous system and implemented based on the above adaptation, will have numerous advantages and some of them are listed below:

- Independent decision making, subsystems can make decisions individually and enforce them against threats.
- Guaranteed minimum resilience, even after disabling the brain subsystem, spinal cord can alone handle the threats through the spawned receptor and effector pairs.
- Hybrid architecture, since brain is designed to operate with multiple spinal cord subsystems and vice versa, the system can further expanded to manage multiple devices and each device can make decisions on its own during critical time.

4 Challenges and future directions

Implementing security mechanism based on human nervous system requires greater caution as the entire system architecture need to be modified in order to accommodate the nervous system functions, particularly spawning receptor and effector pairs and learning engine. In mobile platforms, implementation layer determines the reachability and acceptance of the security mechanism. Usage of kernel or middle-ware layer provides numerous possibilities to observe and restrict application activities. This would result in platform customisation. For example, restricting access to (active and passive) sensors and informational assets, can be achieved easily in platform customization. Furthermore, controlling communication medium can be implemented by directly modifying their corresponding libraries.

Implementing the same as an application will be harder and should follow programming practices that are not recommended for application development by platform providers, e.g., Android and Apple. An application that uses disapproved practices possess a very high possibility of crashing when considerable changes in platform implementation during version upgrades. It is possible to implement communication medium as an application using recommended programming practices but not the entire security mechanism. When compared to kernel or middle-ware layer customisation, it is easier for user to use an application rather than flashing their mobile devices with customised platform. The list of differences in implementation as platform customisation and as an application are listed in Table 1.

Selection of learning algorithm has critical role in the implementation as learning is one of the primary activities of brain. Learning outcome helps to redefine the operational criteria which influences the future learning outcomes and the operations of other subsystems. Hence, learning algorithm should have high detection accuracy and small in size as it will reside permanently in the mobile devices.

5 Summary

In this paper, we presented the conceptual security system design of our ongoing work inspired by the operations of human bio-mechanism. The presented system

is based on human nervous system and has subsystems, brain and spinal cord, to establish similar operations in the security context. The security functions are shared among the brain and spinal cord subsystems to enable cooperation between the subsystems and distributed decision making abilities. The brain and spinal cord subsystems can engage in decision making process independently and execute countermeasures against perceived incidents individually without contradicting each other decisions. The existence of receptor and effector pairs allow brain and spinal cord subsystems to restrict the application activities by sending appropriate instructions. UI configurator provides configuration settings and creates awareness by enabling users to track the activities of security mechanism and the installed applications. The presented conceptual design can be implemented either as platform customization or an application depending on the requirements and user preference.

References

1. Laptop, PC, tablet sales 2010-2022. Statista, https://www.statista.com/statistics/272595/global-shipments-forecast-for-tablets-laptops-and-desktop-pcs/. Last accessed 25 Feb 2019
2. Global smartphone shipments 2010-2022. Statista, https://www.statista.com/statistics/263441/global-smartphone-shipments-forecast/. Last accessed 25 Feb 2019
3. Global mobile data traffic. Statista, https://www.statista.com/statistics/271405/global-mobile-data-traffic-forecast/. Last accessed 25 Feb 2019
4. Cisco VNI: Global Mobile Data Traffic Forecast Update (2017-2022), https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-738429.pdf. Last accessed 25 Feb 2019
5. Zanella, A., Bui, N., Castellani, A., Vangelista, L., Zorzi, M.: Internet of things for smart cities. IEEE Internet of Things Journal vol. 1(1), 22–32 (2014)
6. Sotres, P., Santana, J. R., Sánchez, L., Lanza, J., Muñoz, L.: Practical Lessons From the Deployment and Management of a Smart City Internet-of-Things Infrastructure: The SmartSantander Testbed Case. IEEE Access (5), 14309–14322 (2017)
7. Tsai, K.-L. and Leu, F.-Y. and You, I.:Residence energy control system based on wireless smart socket and IoT. IEEE Access (4), 2885–2894 (2016)
8. Guerrero-ibanez, J. A., Zeadally, S., Contreras-Castillo, J.: Integration challenges of intelligent transportation systems with connected vehicle, cloud computing, and internet of things technologies. IEEE Wireless Communications, vol. 22(6), 122–128 (2015)
9. Siegel, J. E., Erb, D. C., Sarma, S. E.: A Survey of the Connected Vehicle Landscape–Architectures, Enabling Technologies, Applications, and Development Areas. IEEE Transactions on Intelligent Transportation Systems (2017)
10. Catarinucci, L., De Donno, D., Mainetti, L., Palano, L., Patrono, L., Stefanizzi, M. L., Tarricone, L.: An IoT-aware architecture for smart healthcare systems. IEEE Internet of Things Journal, vol. 2(6), 515–526 (2015)
11. Farahani, B., Firouzi, F., Chang, V., Badaroglu, M., Constant, N., Mankodiya, K.: Towards fog-driven IoT eHealth: promises and challenges of IoT in medicine and healthcare. Future Generation Computer Systems (2017)

12. How does the nerves system work? PubMed Health, https://www.ncbi.nlm.nih.gov/books/NBK279390. Last accessed 21 Jan 2019
13. Brown, A. G.: Review article the dorsal horn of the Spinal Cord. Quarterly Journal of Experimental Physiology, vol. 67(2), 193–212 (1982)
14. Westlund, K. N., Willis Jr, W. D.: The Human Nervous System, 3rd Edition. Springer, 1144–1186 (2012). http://www.sciencedirect.com/science/book/9780123742360. Last accessed 21 Jan 2019
15. Stucky, C. L., Gold, M. S., Zhang, X.: Mechanisms of pain. National Academy of Sciences of the United States of America, vol. 98(21), 11845–11846 (2001).