NETWORK SECURITY ARCHITECTURE AND APPLICATIONS BASED ON CONTEXT-AWARE SECURITY

Hoon Ko[1], Chang Choi[2], Pankoo Kim[3] and Junho Choi[4]

[1]IT Research Institute, Chosun University, Gwangju, South Korea
[2]IT Research Institute, Chosun University, Gwangju, South Korea
[3]Department of Computer Engineering, Chosun University, Gwangju, South Korea
[4]Division of Undeclared Majors, Chosun University, Gwangju, South Korea

ABSTRACT

The number of services and smart devices which require context is increasing, and there is a clear need for new security policies which provide security that is convenient and flexible for the user. In particular, there is an urgent need for new security policies regarding IT vulnerability layers for children, the elderly, and the disabled who experience many difficulties using current security technology. For a convenient and flexible security policy, it is necessary to collect and analyze data such as user service use patterns, locations, etc., which can be used to distinguish attack contexts and define a security service provision technology which is suitable to the user. This study has designed a user context-aware network security architecture which reflects the aforementioned requirements, collected user context-aware data, studied a user context analysis platform, and studied and analyzed context-aware security applications.

KEYWORDS

Context-aware Security, Network Security Policy, Malicious Code Detection

1. INTRODUCTION

As the internet of things develops and becomes commercialized, security threats targeting a variety of mobile smart devices are increasing. Among the threats currently being introduced are attacks which can install malicious code on washing machines and refrigerators, attacks which allow hackers to illegally control automobiles remotely, and security vulnerabilities in medical devices such as pacemakers. However, the security solutions for responding to these threats have not taken user convenience into account, and users are inconvenienced by them as a result. It is believed that in the future all devices will connect to networks at high speeds, and the problem of network security will become more important. Children, the elderly, and the disabled in particular must be considered, as they experience difficulties in understanding and using current security solutions. Current security studies are being conducted toward the end of increasing user convenience while maintaining system security. The goal is to resolve the underlying problem by accurately understanding the principles related to security threats and providing the security factors which current solutions omit or fail to satisfy. The user context-aware network security

Dhinaharan Nagamalai et al. (Eds) : ACSIT, SIPM, ICITE, ITCA - 2019
pp. 79–90, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90308

solution proposed in this study is a security framework which can simultaneously provide convenience and security to the normal user. It collects information which can determine the user's context such as user location information, service use patterns, etc., and it automatically provides the most appropriate security service to the user. This paper describes the user context-aware technology that is needed to collect data from the user device's sensors and nearby communications devices and becomes aware of the user context through machine learning and real-time big data analysis technology in order to provide optimized security services.

2. USER CONTEXT-AWARE NETWORK SECURITY TECHNOLOGY TRENDS

2. 1 CONTEXT DEFINITION

Context describes the situation that an entity is experiencing, and context can be collected to analyze a scenario. There are various kinds of context such as people, places, and things. Context is categorized as physical or logical according to its nature, as shown in Table 1.

Table 1. Context Categories.

Category	Physical Context Data	Logical Context Data
Acquisition Method	Acquired through sensors; sensors observe status through measurements	Acquired through record data and activity situation
Processing	For example, magnetic sensors measure a magnetic field's strength and direction, and inertia sensors measure angular displacement and changes in angular displacement	For example, the data indicates whether a person is performing an activity or resting, or whether the person is talking on the phone or sending a message, etc.

2.2 DATA COLLECTION

The types of data which can be collected by a device are very diverse, but the problems with collected data such as integrity, availability, user privacy, etc. are also very diverse. Table 2 shows recent studies related to data collection.

Table 2. Data Collection.

Category	People-centric Opportunistic Sensing [1]	The algorithmic foundations of differential privacy [2]	Continuous user authentication on mobile devices [3]	Soft authentication with low-cost signatures [4].	Joint segmentation and activity discovery using semantic and temporal priors [5]
Feature	When the results of devices performing sensing are accessed by Wi-Fi, they	Device's own security and user privacy	Use of wrist motion sensor's accelerometer (hallmark usage)	Comparison of behavior patterns of registered smartphone owner and illegal user	Uses non-parametric integrated model, divides time into specific segments and

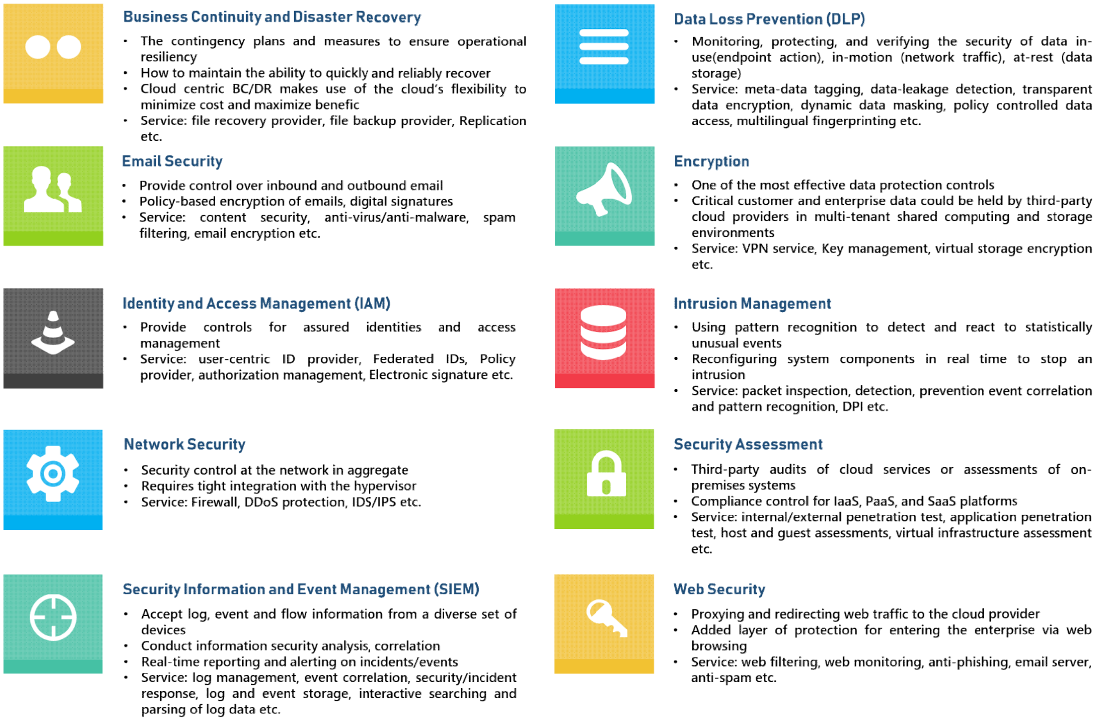
	are sent to the database server and data is collected				uses time points where activities are changing
Advantages	Data collection is possible even though separate infrastructure is not allocated	Strengthens security of Android market	No need for passwords, fingerprints or RFID tags	Higher accuracy than existing methods when noise of sensor results is below a fixed level	Flexible segment size possible by specifying one super sample
Disadvantages	Problems related to participants' privacy, data integrity, and usability	User information leaks when requesting permission to access specific information on the devices during app installation	Accuracy increases only if the time when the user uses the object and the time when the wrist motion sensor collects the data are the same	There is still battery consumption, and usage range (coverage) is limited	Higher accuracy than existing methods when noise of sensor results is below a fixed level

A. SECURITY INFORMATION / EVENT MANAGEMENT

Systematic measures are necessary to perform early detection and respond to the various security threats that use advanced/large-scale network infrastructure. It is also necessary to have a security control system which collects large amounts of event data such as logs, packets, etc. generated by various security devices, network infrastructure, server/storage devices, and service applications, and which uses big data solutions to perform security analysis. Security Information and Event Management (SIEM) is a commercially-oriented solution which collects virtual/actual networks, service applications, system logs and event data. It then categorizes these and analyzes them to create quick reports, and it gives warnings if an additional intervention or altered response is needed [6][7][8][9]. The security tools provided by SIEM perform the core role of a security operations center (SOC) which performs central duties related to security in an organization or business' IT structure. It is also used to record security logs and generate compliance reports [9].

B. TRENDS IN SECURITY COLLECTION/ANALYSIS TECHNOLOGY USING THE CLOUD

In Security as a Service (SESaaS), the security service provider takes responsibility, and services are provided for authentication, anti-virus, anti-malware/spy-ware, intrusion detection, and security event management [10]. In cloud computing, this is defined as Cloud Security as a Service or SECaaS in which the cloud provider (CP) provides security in the form of SESaaS. The services are categorized as shown in Figure 1. The provided services include identity and access management, data loss prevention, web security, email security, security assessments, intrusion management, security information and event management, encryption, business continuity and disaster recovery, and network security.



Business Continuity and Disaster Recovery

- The contingency plans and measures to ensure operational resiliency
- How to maintain the ability to quickly and reliably recover
- Cloud centric BC/DR makes use of the cloud's flexibility to minimize cost and maximize benefic
- Service: file recovery provider, file backup provider, Replication etc.

Data Loss Prevention (DLP)

- Monitoring, protecting, and verifying the security of data in-use(endpoint action), in-motion (network traffic), at-rest (data storage)
- Service: meta-data tagging, data-leakage detection, transparent data encryption, dynamic data masking, policy controlled data access, multilingual fingerprinting etc.

Email Security

- Provide control over inbound and outbound email
- Policy-based encryption of emails, digital signatures
- Service: content security, anti-virus/anti-malware, spam filtering, email encryption etc.

Encryption

- One of the most effective data protection controls
- Critical customer and enterprise data could be held by third-party cloud providers in multi-tenant shared computing and storage environments
- Service: VPN service, Key management, virtual storage encryption etc.

Identity and Access Management (IAM)

- Provide controls for assured identities and access management
- Service: user-centric ID provider, Federated IDs, Policy provider, authorization management, Electronic signature etc.

Intrusion Management

- Using pattern recognition to detect and react to statistically unusual events
- Reconfiguring system components in real time to stop an intrusion
- Service: packet inspection, detection, prevention event correlation and pattern recognition, DPI etc.

Network Security

- Security control at the network in aggregate
- Requires tight integration with the hypervisor
- Service: Firewall, DDoS protection, IDS/IPS etc.

Security Assessment

- Third-party audits of cloud services or assessments of on-premises systems
- Compliance control for IaaS, PaaS, and SaaS platforms
- Service: internal/external penetration test, application penetration test, host and guest assessments, virtual infrastructure assessment etc.

Security Information and Event Management (SIEM)

- Accept log, event and flow information from a diverse set of devices
- Conduct information security analysis, correlation
- Real-time reporting and alerting on incidents/events
- Service: log management, event correlation, security/incident response, log and event storage, interactive searching and parsing of log data etc.

Web Security

- Proxying and redirecting web traffic to the cloud provider
- Added layer of protection for entering the enterprise via web browsing
- Service: web filtering, web monitoring, anti-phishing, email server, anti-spam etc.

Figure 1. SECaaS WG defined 10 categories

3. User Context-Aware Network Security Structure Design

3.1. Considerations During Architecture Design

Recently, there has been an increase in the device networks which need authentication in the IoT environment as well as the range of performance and usage environments for these devices. Because of this, it must be possible to use existing authentication methods in the proposed user context-aware network structure. The network security structure design considerations are shown in Table 3.

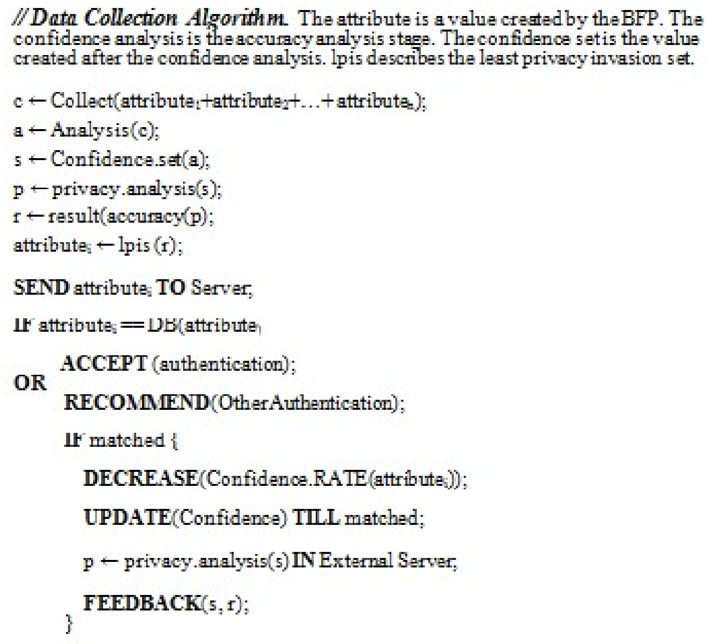
Table 3. User context-aware network structure design considerations.

Considerations	Features
User usability Issue	Because smart devices are always carried by the user as they move around, usability must be considered more for cases in which authentication occurs often [11] In practice, user accessibility is decreased if errors such as false positives and false negatives occur often or if it takes a long time to perform authentication and use the device
Capacity issue of Mobile devices	If there is no interface which provides knowledge-based or biometric-based authentication methods due to the device characteristics: It is necessary to entrust security related features to an external server such as a hub, gateway, or cloud There can be a problem with having to completely trust the entity which performs this role, and higher security such as additional authentication is required

Privacy issue	There is a possibility that GPS information which user data gives can expose the user’s location[12] User call logs describe the user’s personal relationships. It is necessary to consider the privacy of users which have information

3.2. DATA COLLECTION ARCHITECTURE

The device’s sensors are used, and logs such as the user’s contact information and text information are collected, and a behavior fingerprint is defined for each. For example, if the user is a student, the student’s movement pattern may take a regular form such as moving between home and school. If the user accepts a phone call from an unregistered number, the probability that the number will be accepted in the future increases. If the user does not accept the call, the probability that it will not be accepted in the future increases. These user behavior patterns are used in the creation of a behavior fingerprint (BFP). BFPs which are created this way are called attributes. The accurate creation of attributes is more important than anything in increasing the accuracy of user authentication. This is because external factors such as the smartphone’s location, user’s behavior, current weather, temperature/humidity, etc. create noise, and this reduces accuracy when distinguishing the user. Therefore, in order to distinguish users by using attributes, confidence must be increased continually by combining nearby attributes and renewing them.



```
// Data Collection Algorithm. The attribute is a value created by the BFP. The
confidence analysis is the accuracy analysis stage. The confidence set is the value
created after the confidence analysis. lpis describes the least privacy invasion set.

c ← Collect(attribute$_1$+attribute$_2$+…+attribute$_n$);
a ← Analysis(c);
s ← Confidence.set(a);
p ← privacy.analysis(s);
r ← result(accuracy(p);
attribute$_i$ ← lpis (r);

SEND attribute$_i$ TO Server;

IF attribute$_i$ == DB(attribute$_i$

    ACCEPT (authentication);
OR
    RECOMMEND(OtherAuthentication);

    IF matched {
        DECREASE(Confidence.RATE(attribute$_i$));
        UPDATE(Confidence) TILL matched;
        p ← privacy.analysis(s) IN External Server;
        FEEDBACK(s, r);
    }
```

In the proposed architecture’s processing order, the data is first collected according to the attribute, and then the confidence analysis is performed. The confidence analysis is a module which calculates whether a certain combination of attributes is necessary to guarantee confidence over a certain threshold value. Based on these calculations, the confidence set is created and analyzed. The privacy analysis analyzes the degree of privacy invasion for each attribute. The least privacy invasion set is selected, and the set’s attributes are transmitted to an external server.

The external server provides feedback on the confidence analysis and the privacy analysis based on the analyzed results. If the comparison with the fingerprint that the user has already saved does not produce a match, a different authentication method is proposed. If the different authentication method succeeds, the attribute's confidence is lowered, and the confidence is continually updated (FEEDBACK Step). In FEEDBACK, if privacy continually brings in the same result, similar attributes are continually sent out. However, because it is easy to violate privacy, the external server's feedback results are reflected in the privacy analysis to prevent transmission of the same attribute.

3.3. CONTEXT-AWARE MULTI-FACTOR AUTHENTICATION

Multi-factor authentication requires different types of information on the authentication target in order to control access to a resource, such as information that the user knows and a possession that the user has [13]. This authentication method is already widely used. For example, a transaction with a bank's ATM card requires both knowledge (password -- information the user knows) and the ATM card (possession -- thing the user has) to confirm the user. Because 2 pieces of information are required, this corresponds to a type of multi-factor authentication known as two-factor authentication. If the user's context is used as one piece of authentication information in multi-factor authentication, the level of security can be maintained while also ensuring convenience. Information acquired as the result of soft sensing is used to determine the user context information. This method can confirm whether or not the device or environment which is to be authenticated matches the context experienced by the user, and the complexity of the authentication stage is only alleviated if it does match. If this method is used, an additional two-factor or three-factor authentication stage is required if the user context information does not match. By providing such a stage, a higher level of authentication security can be achieved. If the user context information does match, the authentication stages can be simplified to increase user convenience.

4. USER CONTEXT-AWARE NETWORK SECURITY STRUCTURE DESIGN

4.1. Definition of Data

A. COLLECTION DEVICES

In the IoT era, the number of sensor types and the places where they are used have both increased. Devices that users carry and connected sensors can extract features from the user's activities, behavior, etc. There are convenient and effective authentication methods which calculate a risk score and make requests for a suitable authentication approach according to the risk. Types of collection devices include smart phones, PCs, tablet PCs, wearable devices, smart sensors / hubs, smart door locks, smart TVs with IoT hubs, and other connected devices.

B. COLLECTABLE DATA

Table 4 shows the collectable data. For example, a smartphone that a user carries or a wearable device can detect the user's location, activities, and characteristics through physical sensors (hard sensing) such as accelerometers, magnetometers, and gyroscopes. Effective authentication methods which are suitable for the user context can be requested through logical sensors (soft sensing) which detect screen state of devices, battery consumption, phone records, data usage, etc.

Table 4. Collectable data.

Device	Sensors (Physical/ Logical)	Features
Smartphone, PC and tablets/ Wearables	- Phone Info/Calls - Location, Accelerometer - Magnetometer	User's current location and activities
Smart Sensors/ Hub	- Motion, Light	User's environments and activities
Smart Door Lock	- Location	User at home or not
Smart TV with IoT Hub	-Usage time -User channel properties, etc.	Duration, User's personal interest

4.2. SECURITY/PRIVACY ISSUES

Context- aware opportunistic user authentication systems collect biometric contexts through the user's smart device and are able to understand the user's current context. By doing so, they have the compelling benefit of providing appropriate security solutions. However, by collecting this data, problems can occur which are related to user privacy and collected data integrity and usability. Also, as the use of smart devices increases, malicious apps may be offered on app markets. Even when an app is not malicious, mistakes by a developer who does not take security into account may cause problems in which users accidentally encounter other malicious programs through advertisements, etc. and expose their personal information [10]. If context- aware opportunistic user authentication is being used, there is a risk that the device may become a privacy vulnerability point (privacy hole) and even personal information stored on other connected devices could be leaked [14].

4.3. COLLECTION TECHNOLOGY

Data collection for user context- awareness is categorized as physical sensor data which can be directly obtained from the devices that the user is operating, logical sensor data which changes according to the user's habits and device usage patterns, and soft sensing data in which new data is derived by using the data of several sensors [15][16]. Each type of sensor data can be collected continuously like GPS data or collected intermittently like phone conversation data. In short, there are many types of data for context awareness, and they have characteristics that make it difficult to integrate collection methods. As such, context-aware data requires analysis and processing before inferences which utilize the data can be made. Depending who is in charge of processing, this analysis includes (a) methods which directly process sensed data on the user device and (b) methods in which the user device sends data to a server and it is processed. The features of each method are shown in Table 5.

Table 5. Collection technology types.

Type	Advantages	Disadvantages
(a) Data is processed directly on the user device	After processing, the size of the data is reduced so that storing it is easy and sending it to the server is easy.	The user device cannot guarantee sufficient performance and it is difficult to update the algorithms needed for data processing
(b) Data is sent to a server and processed	It is possible to guarantee sufficient performance to process the collected data. It is easy to change the data characteristics or analysis standards and update the algorithm.	The collected data must all be sent to the server, which may put a burden on the user device or server depending on the situation.

4.4. Collection Technology

Figure 2 shows the proposed data collection architecture. Confidence analysis analyzes the user fingerprint accuracy for each attribute. It can analyze 1 attribute or analyze the accuracy of a set of several attributes simultaneously. The accuracy analysis is first done on the basis of reference data, and later machine learning is used to continue learning about accuracy analysis. At first, an accuracy above a fixed level is seen. However, because the accuracy for each attribute can vary due to flaws in the sensors themselves or changes in user patterns, the accuracy is updated by setting a score for the accuracy based on the authentication results.

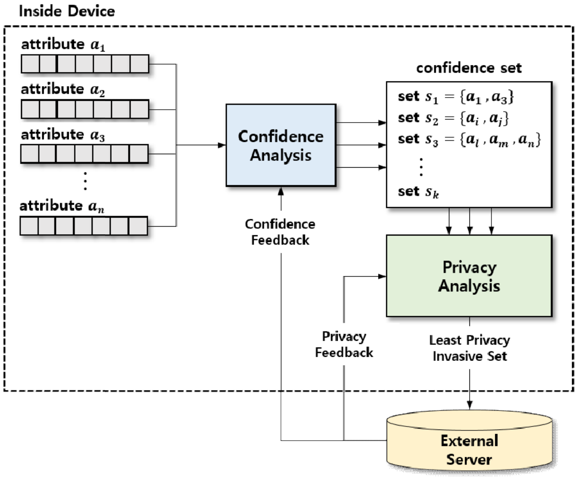


Figure 2. Data collection architecture

When confidence analysis is finished, a set of attributes which has an accuracy above a fixed threshold value is produced. The threshold value can be selected experimentally, and it can be updated later based on the authentication results. The set of attributes which is above the threshold value is called the confidence set. Privacy analysis is performed for a total of k confidence sets.

Privacy analysis shows the privacy given by the attributes in the confidence set. The user's sensitivity to the privacy of each attribute varies. Because the analysis of sensitivity to privacy varies by each user, different levels of sensitivity are used for each user. Providing high accuracy means distinguishing the user more easily, and this ultimately means showing the user's personal information more accurately. When the privacy analysis is finished, one set with the lowest sensitivity, i.e. the set with the least user privacy leaking, is selected. The selected set is defined as the least privacy invasive set, and it is transmitted to the external server for the next stage.

5. Applications

This section defines 5 context-aware applications based on the previously defined context-aware network security architecture and context-aware data collection method. These applications are context-aware authentication technology, context-aware access control technology, a context-aware personalized warning system, context-aware security settings, and a malicious code detection system. Table 6 describes each application.

Table 6. Applications.

Category	Goal	Processing	Features
Context-aware authentication technology	Provides a suitable user context authentication process in which the service user is pre-enrolled to provide context-aware service to the user	- Collects data from acceleration sensor, microphone, GPS location service, and touch screen for authentication - The acceleration sensor measures the user's movement state and speed. The microphone receives the user's voice. - The GPS can accurately know the user's location. The touch screen collects the user's touch behavior. The collected information is used to perform authentication	- Authentication using the user's movement state - Authentication using the user's voice - Authentication using the user's GPS - Authentication using the user's touch records
Context-aware access control technology	Determines the access control which is suitable for the context based on context data acquired by using a variety of sensors, GPS, etc.	- The Profiler module extracts features from collected raw data and defines objects related to context models and profiles - The Classifier module uses the extracted features to train the context classification model - Transmits the "classification" and the "confidence value" which shows the degree of risk in the context model to the Access Control Layer - The Access Control Layer module determines access control based on the received data	- Knows outdoor places that the user visits often - Knows indoor places that the user visits often - Integrates GPS data with interactions between the user and the device UI and performs user location analysis and current user status analysis
Context-aware personalized warning system	Provides custom warnings according to the user context and effectively conveys the warning content to the user	- Creates different warnings to transmit to the user depending on the context analysis results - Creates customized warnings which can effectively convey warning content to the user based on each context such as the level of specialized knowledge possessed by the user, the user's current status (working, sleeping, resting, etc.), level of risk for abnormal contexts, etc.	- Warnings according to the user's system specialty - Warnings according to the user's status - Warnings according to the warning context's risk level - Bot detection warning: If the user is not a person, distinguishes the user as a bot and creates a captcha
Context-aware security settings	Uses the user's context-aware data to resolve the hassle of having to go through a complex security settings process and provides a dynamic and simple security settings method	- Collects the user's context-aware data and uses it to dynamically set the security settings level of the devices used by the user according to the situation - The security settings levels are defined as normal, high, and user-specified - The context that is used to change the security settings utilizes information such as the degree to which the user understands security-related information, the user's current status, the user's activity data, and the user's location data	- Security settings using user status data - Security settings using user location data - Security settings using user activity data
Malicious code detection system	Provides malicious code detection system which is customized according to the user status to establish measures for systematically responding to and preventing malicious code attacks	- Goes through static analysis, dynamic analysis, and trace analysis and categorizes the features which show the execution file as classes - Determines groups which are estimated by the relationship with the target execution file via class categorization stage - Categorizes the developer's classes based on the data extracted from the execution file and infers the developed and circulated execution file from the specific structure	- Malicious code detection through static analysis - Malicious code detection through dynamic analysis - Malicious code detection through usage tracking

6. CONCLUSIONS

To implement user context-aware network security technology, it must be possible to determine contexts by utilizing user usage patterns and movement patterns which are based on user position data. To utilize safe user context awareness, data must be collected from the user device's sensors and nearby network devices, and the user's nearby context must be recognized by using machine learning and real-time big data analysis technology to provide optimized security service. In order to implement a safe user context-aware service, this study examined trends in context-aware network security technology and designed a user context-aware network security architecture. The trends in user context-aware network security technology were organized into data collection in which the collected data's integrity, usability, and user privacy are processed, context analysis which is an analysis stage for performing various analyses on the collected data, and context-based applications which are for safely using the analyzed contexts. In the user context-aware network security architecture design, the context information analysis and the user's nearby context, which have been collected by the cloud server, were judged together to measure risk, and based on these results, security services which can deliver both user satisfaction and security were provided. In the results of the study, five kinds of applications were introduced, and the safety of the user context-aware applications were analyzed. Based on the results of this study, a variety of safe user context-aware applications are expected in the future.

ACKNOWLEDGEMENTS

This research was supported by Korea Electric Power Corporation (Grant number: R18XA06-12) and the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIP)(No.NRF-2016R1A2B4012638).

REFERENCES

[1] Berker Agir, Jean-Paul Calbimonte and Karl Aberer, "Semantic and Sensitivity Aware Location Privacy Protection for the Internet of Things," PrivOn'14 Proceedings of the 2nd International Conference on Society, Privacy and the Semantic Web - Policy and Technology, Vol. 1316, pp. 58-63.

[2] Dwork, Cynthia, and Aaron Roth. "The algorithmic foundations of differential privacy," Foundations and Trends in Theoretical Computer Science 9.3-4 (2014): 211-407.

[3] Vishal M. Patel, Rama Chellappa, Deepak Chandra, and Brandon Barbello, "Continuous user authentication on mobile devices: Recent progress and remaining challenges," IEEE Signal Processing Magazine 33.4 (2016): 49-61.

[4] Buthpitiya, Senaka, Anind K. Dey, and Martin Griss. "Soft authentication with low-cost signatures," Pervasive Computing and Communications (PerCom), 2014 IEEE International Conference on. IEEE, 2014.

[5] Seiter, Julia, et al. "Joint segmentation and activity discovery using semantic and temporal priors," Pervasive Computing and Communications (PerCom), 2015 IEEE International Conference on. IEEE, 2015.

[6] "SIEM: A Market Snapshot,"Dr. Dobb's Journal, Feb. 2007.

[7] J. Hayes, "Cybersecurity and the Big Yellow Elephant," Cloudera Vision Blog, May 2015.

[8] K. M. Kavanagh, O. Rochford, and T. Bussa, “Magic Quadrant for Security Information and Event Management,” Gartner, Aug. 2016.

[9] Bhatt, P. K. Manadhata, and L. Zomlot, “The operational role of security information and event management systems,” IEEE Security & Privacy, vol. 12, no. 5, 2014.

[10] Mosaic Security Research, “Log Management & Security Information and Event Management (SIEM) Software Guide,” Mosaic Security Research, (accessed May 2014).

[11] G. Abowd and A. Dey, "Towards a better understanding of context and context-Awareness," In International Symposium on Handheld and Ubiquitous Computing, pp. 304-307, 1999.

[12] H. Witte, C. Rathgeb and C. Busch, "Context-Aware Mobile Biometric Authentication based on Support Vector Machines," 2013 Fourth International Conference on Emerging Security Technologies, Cambridge, 2013, pp. 29-32.

[13] William E. Burr, Donna F. Dodson, Elaine M. Newton, Ray A. Perlner, W. Timothy Polk, Sarbari Gupta, and Emad A. Nabbus, “Electronic Authentication Guide,” Special Publication 800-63-2, NIST, 2013.

[14] Kapadia, Apu, David Kotz, and Nikos Triandopoulos. "Opportunistic sensing: Security challenges for the new paradigm." 2009 First International Communication Systems and Networks and Workshops. IEEE, 2009.

[15] H. Witte, C. Rathgeb and C. Busch, "Context-Aware Mobile Biometric Authentication based on Support Vector Machines," 2013 Fourth International Conference on Emerging Security Technologies, Cambridge, 2013, pp. 29-32.

[16] T. Gisby, “”Soft” Sensors Are Breaking Into Four Major Industries,” Aug 2015.

[17] Harbach, Marian, et al. "Sorry, I don’t get it: An analysis of warning message texts." International Conference on Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2013.

[18] Anderson, Bonnie Brinton, et al. "How polymorphic warnings reduce habituation in the brain: Insights from an fMRI study." Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems. ACM, 2015.

AUTHORS

Hoon Ko received B.S. at Howon University in 1998, and M.S. in 2000, Ph.D. in 2004 at Soongsil University, S. Korea. He had worked at GECAD/ISEP/IPP in Portugal as a Post-Doc from 2008 to 2013, and at J. E. Purkinje University, Czech Republic as a research professor from June 2013 to July 2015. Now he been working at IT Research Institute, Chosun University, S. Korea as a research professor since Oct 2017. His research area is CPS Security, Cyber-Security, context-aware, multicast, IoT, Bio-information security.

Chang Choi received his Ph.D. degree in Computer Engineering from Chosun University in 2012, and is now working as a research professor at the Chosun University, South Korea, and is a Senior member of the IEEE. His research interests include Intelligent Information Processing, Semantic Web, Smart IoT System and Intelligent System Security.

Pankoo Kim received his B.E. degree from the Chosun University in 1988 and M.S. and Ph.D. degrees in Ccomputer Engineering from Seoul National University in 1990 and 1994. Currently, He is now working as a full professor at Chosun University. He is an EIC of IT CoNvergence PRActice Journal. His specific interests include semantic web techniques, semantic information processing and retrieval, multimedia processing, semantic web and system security.

JunHo Choi received the PhD degree from Chosun University, Gwangju, Korea in 2004. He is currently an Assistant Professor with the Department of Undeclared Majors, Chosun University, Gwangju, Korea. His research interests include Security, Cloud Computing, Semantic Analysis, Ontology Modeling.