A Home Firewall Solution for Securing Smart Spaces

Pho Duc Giang, Le Xuan Hung, Yonil Zhung,

Sungyoung Lee, and Young-Koo Lee

Computer Engineering Department, Kyung Hee University, Korea
{pdgiang, lxhung, zhungs, sylee}@oslab.khu.ac.kr, yklee@khu.ac.kr

In Ubiquitous Computing environments, service servers play a central role of actively gathering situation information to detect changes in context to provide appropriate functions for users. However, they also raise concerns related to security and privacy. It is the dynamism and mobility absolutely necessary for smart spaces that can yield extra chances for attackers to exploit vulnerabilities in the system invisibly. From a server-centric viewpoint, researchers must find techniques to reduce the security risks as much as possible from these servers. Firewall technology is a logical approach that can help them accomplish this troublesome task. In this paper, we propose a new concept of context-aware host-based firewall called *Home Firewall*[1], to protect the central server deploying our current context-aware middleware, namely Context-Aware Middleware for Ubiquitous computing Systems (CAMUS), from suspicious actions. The idea is established on host-based firewalls to filter off malicious context-aware and command packets in/out the service server.

Threats to the Central Server: One of the most severe security threats to the server coming from wireless sensor networks is base station spoofing. The wireless sensor networks often collect and relay data to the server via a gateway or base station. An attacker gain unauthorized access to the environment by making it appear that a malicious message has come from the base station by spoofing the IP and/or the MAC address of that machine. Therefore, instead of sending the control packets to the base station, i.e., to turn the surveillance camera and alarm system on, to alert strangers breaking into the house, the server delivered messages to the hacker's machine. Moreover, dangers to the main server coming from wireless networks are wireless device compromise. We can take a visual example by supposing that the home owner joins his laptop into an unprotected network already infected with viruses, worms, or Trojan horses at his office, his laptop is then infected with the kind of plague. Later, he brings the laptop into his home network, a protected environment, and connecting to the central server through the Wireless Access Point (WAP). In this case, packets from his laptop are sent to the servers without any verification and they are thus free to corrupt the entire system. Also, risk to the principle server resulting from applications or services implemented on the system can be exploited by attackers because they miss crucial security patches. Once these programs are compromised,

[1] This work is financially supported by the Ministry of Education and Human Resource Development (MODE), the Ministry of Commerce, Industry and Energy (MOCIE), and the Ministry of Labor (MOLAB) through the fostering project of the Lab of Excellency. Dr. Sungyoung Lee is the corresponding author.

the system control right will be taken over by hackers. Our server may be planted viruses, opened back doors for serving the intruder's remote control demands.

Our Proposed Methodology: We present our basic design of the Home Firewall in the smart home infrastructure described in Fig.1.

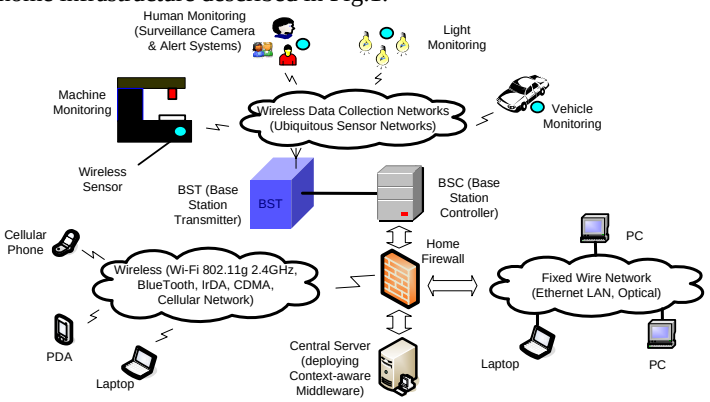

Fig. 1. A smart space with Home Firewall support

In our approach, the Home Firewall contains MAC Address Refining (MAR) module. This module is responsible for real-time selecting trusted MAC addresses of available confident base stations in the space for preventing base station spoofing attack. The selected addresses are maintained in an admission list. The MAR module periodically sends a RARP (Reverse Address Resolution Protocol) packet to each address in the list. The function of RARP is mapping a MAC address into an IP address. Following this, Reverse ARP should reply one IP address for one network device. If multiple IP addresses return, it means that the MAC address is being exploited by more than one device.

The firewall manages all the transactions between the user's mobile devices and the central server. If the WAP and/or user's mobile device are compromised, attackers still have no way to change the behavior of our server since they don't know the username/password to change the firewall policies. Our policy, i.e., was set to turn the camera system on from 11P.M to 6A.M. Therefore, malicious control packets that want to improperly turn the system off at that time will be dropped by the firewall.

The Home Firewall also helps preventing other server's programs from being compromised by stopping common hacker's reconnaissance port scanning techniques. In order to defend our server from these kinds of potential threats, such as ICMP scanning, TCP scanning, UDP scanning, we deploy an anti-scanning security policy. Our firewall will prohibit the ICMP replying packets for preventing ICMP scanning technique and deny the ICMP Port Unreachable packets transmitted back to an attacker for protecting UDP scanning probe. For detecting the TCP scanning signature, we might say that if there are more than 5 SYN packet attempts to non-listening ports in one minute, an alarm SMS message should be automatically triggered to the user's cell phone.