Automatic Defense Mechanisms against Malicious Intruders and Attackers on Cyber Society

Keisuke Takemori
KDDI R&D Laboratories Inc.

Over the last few years, the risks of using network services have been growing day by day because many kinds of communication terminals, which have vulnerabilities, have been released. The terminals can access to the risky Internet at anytime and anywhere by using various wireless and wired services. On the other hand, ubiquitous terminals, such as cellular phones, now have many kinds of personal information, for example address book, scheduler, and credit card identification. Therefore, the risks of losses from terminals increase. How do you defend the terminals against malicious intruders or computer viruses? It is hard for inexperienced Internet users to protect them completely.
We have proposed automatic defense schemes for user terminals, which monitor attack activities on the Internet and protect the terminals by using an access controller or simple authentication mechanisms. A security operation center (SOC) monitors incidents on the Internet and handles them between network operators and users. When security incidents are detected, the SOC analyzes them and considers a strategy for protecting backbone networks and user terminals to restrain their impact. The network infrastructure includes defense appliances, such as an intrusion detection system, an anti-virus system, and an access controller. The SOC controls the appliances automatically to defend the terminals that access via home networks or wireless networks on public space from various attacks.
Moreover, we have proposed a simple and easy biometrics authentication scheme that can prevent personal data leakage from a lost cellar phone. This scheme distinguishes key typing habits between an original holder and a malicious finder, and suspends the terminal immediately when any anomalies are detected.
The automatic defense mechanisms are important mechanisms for next generation network services. The schemes should be considered from a user perspective, i.e., easy and simple to use.

Keywords:
Distributed Denial of Service (DDoS) Attack: Many infected terminals attack a victim site simultaneously and affect network services.

Biometrics Authentication: Authentication technologies that measure and analyze human physical and behavioral characteristics for authentication purpose.