

Summary for security session

17 July, 2008

Heung-youl Youm, Session chair

Overview of three presentations(1/3)

- VoIP security issues by KISA
 - Various threats to current VoIP system, such as eavesdropping, DDoS, VoIP SPAM, and abuse.
 - Countermeasures to these threats, such as secure VoIP terminal by encrypting communication, Secure SBC, SPAM response system using domain authentication, and Intrusion Protection.
 - Work item including two subjects for collaboration proposed;
 - Spam response for VoIP by providing domain authentication, Attacker trace for spammer
 - Possible subject (Location information protection)

Overview of three presentations(2/3)

- Mega Communications TRAP: Trust and Privacy
 - Concept of future of the Internet, Internet of things
 - Projects such MAGNET (Secure Personal Network), ASPIRE (secure middlew are of RFID based application)
 - Ingredients for Telehomecare
 - wireless communication, context awareness, mobility/management/Governance, S ecurity/Trust/Privacy, Policy/Identity management, security, privacy, trust and identi ty
 - Especially, trust and identity requirements presented
 - Provisioning, identification, authentication, authorization, accountability/ moitoring, user management
- Challenges
 - Protecting identity, Securing CI, Securing the interactions and interfaces
 - Designing scalable, sependable and resilient open system and composite servi ces, Contaxt-aware security architecture, security for small devices, new crypto schemes

Overview of three presentations(3/3)

- Developing cooperative defense mechanisms for DDoS Attacks
 - Concept of DDoS attacks
 - Various countermeasures to DDoS attacks were presented;
 - Visualization techniques, Defending VoIP DDoS
 - BOTNET attacks
 - BOTNET detection techniques by DNS traffic
- Work item for collaboration including the following subjects;
 - BOTNET detection/response
 - Systematic DDoS defense with information sharing protocol,

Conclusion

- Three presentations were given and useful discussion was made in the session.
- Several work items were proposed or identified:
 - SPAM response system/Traceback of attacker for VoIP system;
 - Identity management and security policy management for ubiquitous applications (Good response);
 - Countering BOTNET attacks (Very good response).
- It is recognized that further steps for substantial progress have been made.