Security risks on VoIP caused by DNS server

Ge Zhang
Karlstad University

Current Voice over IP (VoIP) service is regarded less secure than the traditional Public Switched Telephone Network (PSTN). This is mainly due to two reasons: first, the VoIP services are usually deployed in a relatively open environment, so that VoIP infrastructures can be easily accessed by potential attackers. Second, VoIP services heavily relay on other public Internet infrastructures shared with other applications, for example, DNS server, web server, accounting database, etc (We define them as *external servers*). Thus, the vulnerabilities of these external servers may introduce negative impacts on VoIP services as well. Moreover, the careless designed communication interfaces between VoIP infrastructures and external servers may also be exploited by attackers.

Three concrete security risks on VoIP will be addressed from the aspects of confidentiality, integrity and availability respectively. All of these risks are caused directly or indirectly by DNS servers. For confidentiality, attackers may mount a timing attack to profile some sensitive information, such as a calling history of a VoIP domain, by taking advantage of DNS cache. Regarding the integrity of data source, a DNS spoofing attack may make VoIP calls to be redirected to unwanted users. Considering the availability, attackers may exploit the latency between DNS request and response to launch Denial of Service (DoS) attacks on VoIP services.

Although we only demonstrate some security risks caused by using DNS servers, similar attacks can be realized by using other external servers as well. Therefore, the VoIP service providers should not only pay attention on the protection of VoIP infrastructures, but also the security issues of external servers.

Key words: VoIP, SIP, security, DNS, DNS cache, DNS spoofing, DNS latency