# McGraw-Hill - Hacking Exposed VoIP Voice Over IP Security Secrets & Solutions

Block debilitating VoIP attacks by learning how to look at your network and devices through the eyes of the malicious intruder. Hacking Exposed VoIP shows you, step-by-step, how online criminals perform reconnaissance, gain access, steal data, and penetrate vulnerable systems. All hardware-specific and network-centered security issues are covered alongside detailed countermeasures, in-depth examples, and hands-on implementation techniques. Inside, you'll learn how to defend against the latest DoS, man-in-the-middle, call flooding, eavesdropping, VoIP fuzzing, signaling and audio manipulation, Voice SPAM/SPIT, and voice phishing attacks.

- Find out how hackers footprint, scan, enumerate, and pilfer VoIP networks and hardware
- Fortify Cisco, Avaya, and Asterisk systems
- Prevent DNS poisoning, DHCP exhaustion, and ARP table manipulation
- Thwart number harvesting, call pattern tracking, and conversation eavesdropping
- Measure and maintain VoIP network quality of service and VoIP conversation quality
- Stop DoS and packet flood-based attacks from disrupting SIP proxies and phones
- Counter REGISTER hijacking, INVITE flooding, and BYE call teardown attacks
- Avoid insertion/mixing of malicious audio
- Learn about voice SPAM/SPIT and how to prevent it
- Defend against voice phishing and identity theft scams

Download | **Size:** 16.33 MB |