Protecting IMS Networks From Attack

Krishna Kurapati

Application-level attacks and fuzzing are on the rise. Can IMS cope?

Krishna Kurapati is the founder and CTO of Sipera Systems (www.sipera.com), a company that specializes in security for VOIP, mobile and multimedia communications. He can be reached at 214/206-3210 or krishna@sipera.com.

Just as the ecommerce companies have learned that they must go to great lengths to protect their core servers from hackers, malware and service abuses, so too must network operators who plan to offer Internet-based services using IMS (IP Multimedia Subsystem) technologies.

Because the Internet is an "open" system, any user can freely connect to it at any time from any place with little effort, making it a fertile breeding ground for a wide variety of malicious and unauthorized activities. With both ecommerce and IMS, security is a necessary requirement, as any down time of the site or service means lost revenue for the company.

Ecommerce sites typically protect their infrastructure and services with a variety of security devices and techniques. These range from denial of service (DoS)/distributed DoS (DDoS) protection for HTTP request traffic to intrusion detection/prevention systems IDS/IPS) that do deep packet inspection for vulnerabilities in application traffic. Many ecommerce sites also deploy application-specific firewalls and implement SSL/HTTPS access for ecommerce transactions (see this issue, pp. 34–39).

While the IMS network attacks bear similarities to those on ecommerce sites, both the attacks and required devices with IMS are unique to this network. This article explains why IMS is so vulnerable, and then describes several potential IMS

FIGURE 1 How To Hack An IMS Network

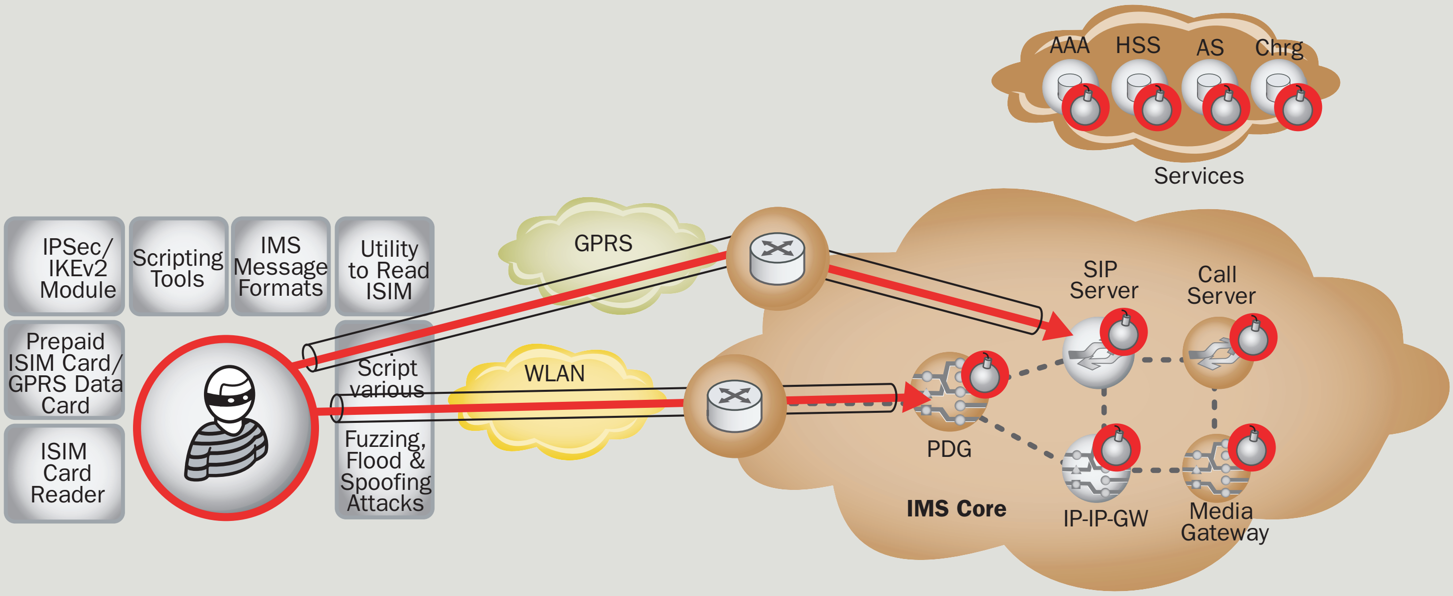
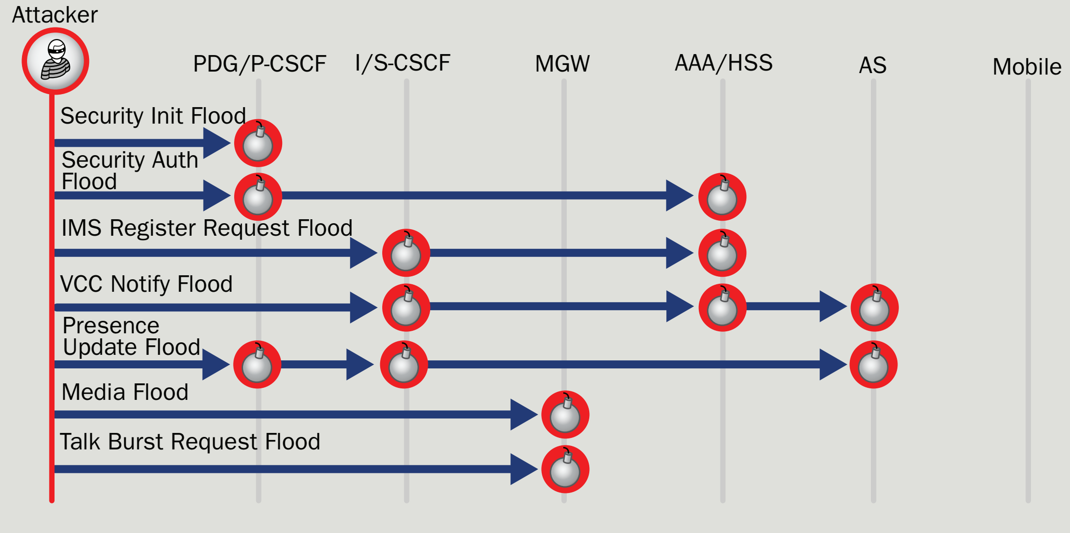


FIGURE 2 Examples Of Floods And The Components Attacked



Building an attack vector to exploit an IMS network takes very little time or money

attacks and the different security requirements that need to be addressed. It also briefly explores possible solutions that can complement current authentication and encryption, to protect against all these attacks.

While the article focuses on IMS, many of the same problems and solutions apply equally to unlicensed mobile access (UMA) networks, which some view as mobile precursors to IMS. Let's first explore why IMS is such an easy target for malicious users, and then take a close look at the major application-layer weaknesses and how to address them.

Building An Attack Tool Is Easy

IMS and one of its chief components, the Session Initiation Protocol (SIP), enable a rich set of converged services, but they also open up the network to a host of known IP-based vulnerabilities. Some of these can be addressed by firewalls and some by the packet data gateway (PDG), while other application-layer attacks are completely new.

At the same time, building an attack vector to exploit an IMS network takes very little investment in terms of time or money. The components are available for free as open-source software, and all the IMS specifications are publicly available at the 3GPP website. After simply purchasing a Universal or IP multimedia Services/Subscriber Identity Modules (U/I-SIM) card, a competent hacker could, in just a few days, easily write scripts to read the cards. Once the SIM cards are hacked, the perpetrator is easily "inside" the IMS network, as shown in Figure 1.

Because IMS specifies IPSec as the preferred form of core-level, network-layer security, once tunnels are established with the packet data gateway, the clever hacker can readily launch huge floods of traffic—up to 10,000 messages per second, which is equivalent to the traffic from 10 million subscribers, bringing down multiple nodes in the network, including the PDG itself.

Flooding is just one of many IMS vulnerabilities. In fact, our lab has identified more than 90 major classes of unique vulnerabilities and more than 20,100 attacks that can be launched against IMS networks.

Some IMS attacks can be launched even before the user authenticates (necessary each time the user initiates a request to gain access to system capabilities and services), while others can be used to attack the core infrastructure and take down the service, or they can be used to attack the end users. Here are some specific examples:

Glossary Of Terms

■ **PDG: Packet Data Gateway** is the security gateway that terminates and aggregates the IPSec tunnels.

■ **CSCF: Call Server Control Function** provides registration of the endpoints and routing of the SIP signaling messages. The various CSCF components include the Proxy-CSCF (P-CSCF), the Interrogating-CSCF (I-CSCF); and the Serving-CSCF (S-CSCF).

■ **MGW: Media Gateway** interfaces with the media plane of the circuit switched network, by converting between RTP and PCM.

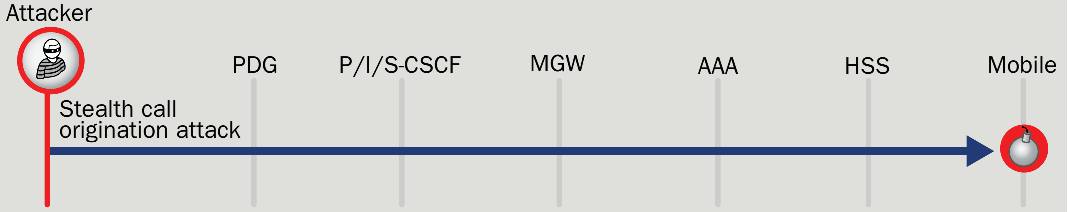
■ **HSS: Home Subscriber Server** is the main data storage for all subscriber and service related data.

■ **AAA: Authentication Authorization Accounting Server** controls the database concerning who can access the network, and tracks billing data for each user.

■ **AS: Application Server** is responsible for the execution of service-specific logic and delivering value-added services.

Some flood attacks can be launched before the IPSec tunnels are set up

FIGURE 3 Stealth Attack Example



Floods, Distributed Floods And Stealth Attacks

As just described, DoS attacks, as shown in Figure 2, basically flood the IMS network with a tremendously large number of random messages. Whether sent from a single location or from multiple locations (DDoS), the flood of messages is well beyond the processing capacity of the target system, thereby quickly exhausting its resources and denying services to its legitimate users.

The nature of these flood attacks is very similar to what can be launched at other networks, but the impact could be much more devastating. Floods that are extremely damaging to IMS networks include those based on the Internet Key Exchange (IKE), such as IKE_SA_INIT floods and IKE_SA_AUTH floods, both of which are possible even before setting up the IPSec tunnel. Application-specific floods such as Register Request Floods and Presence Update Floods are also possible. These attacks are easily created using publicly available tools.

In a stealth attack, one or more specific endpoints are deliberately attacked from one (DoS) or more (DDoS) sources, although at a much lower call volume than is characteristic of flood type attacks, as shown in Figure 3.

What makes IMS particularly vulnerable to these floods is the fact that the IKE messages in IMS, for the first time, expose the key IMS infrastructure components to attack, including the home subscriber server (HSS), which stores and provides real-time customer data. Any of these flooding attacks would be devastating if the IMS network is used to offer emergency services and/or connectivity to other non-IMS networks. If IMS is assumed to be the architecture for wireless and wired public networks, then any attack on an IMS network could potentially affect the more than 2 billion users connecting to wireless and wireline networks today.

The key challenge is to stop all these attacks (i.e., no false negatives) while allowing legitimate traffic to still pass through (i.e., no false positives). There is no standard mechanism in the IMS specifications to handle these types of attacks, so vendors need to develop their own techniques to provide this protection. Rate limiting is sometimes used to prevent floods and distributed floods, but it does not selectively block only the attack traffic.

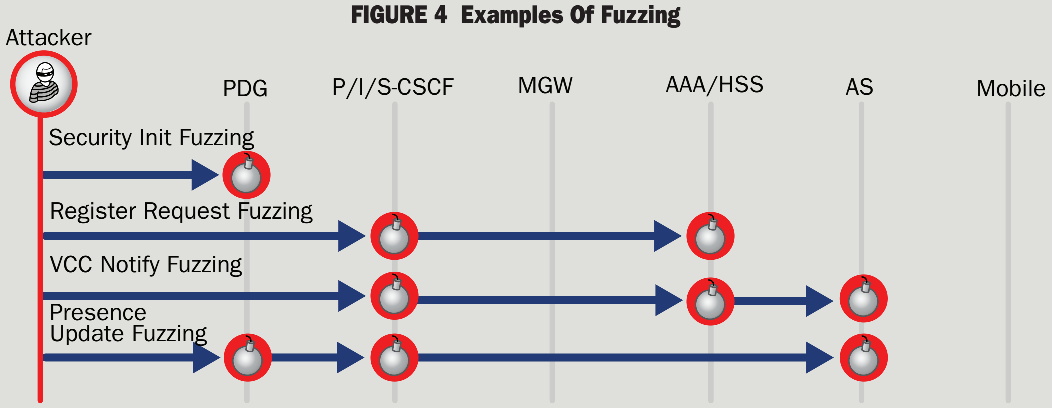
Protocol Fuzzing

Fuzzing is a legitimate method of testing software systems, in which semi-valid input is provided to an application to see how it reacts. Then appropriate fixes can be implemented, if necessary.

Malicious users, however, employ this same methodology to exploit vulnerabilities in a target system. They do this by sending messages whose content is good enough that the target will assume it's valid. In reality, the message is "broken" or "fuzzed" enough that, when the target system attempts to parse or process it, various failures result. These can include application delays, information leaks, or even catastrophic system crashes.

Fuzzing attacks are nearly impossible in the PSTN and on 2G cellular networks because the

FIGURE 4 Examples Of Fuzzing



signaling traffic is encoded (not text-based like SIP) and the OSes and protocols are proprietary, so hackers don't have access to the details.

However, in the IMS network and on the public Internet, fuzzed messages can easily be used to launch attacks. They can even be transmitted using encrypted and authenticated traffic all the way to the IMS core, as shown in Figure 4.

IMS also may be more vulnerable to fuzzed messages because it is the product of hundreds of IETF drafts and RFCs, combined with some 3GPP specs, and none of these are very mature or robust. In addition, each message is handled by multiple subsystems, offering many points of potential vulnerability.

Again, IMS specifications do not spell out how these fuzzing vulnerabilities are to be addressed. A deep-packet-inspecting security device needs to decrypt and examine the traffic at wire speed to prevent these fuzzing attacks, by either fixing the malformed part of the message or dropping the call. Otherwise the mobile devices or infrastructure will be overwhelmed and reboot, since they don't know how to handle the fuzzed messages.

VOIP Spam

VOIP spam, or Spam-over-Internet Telephony (SPIT), is unsolicited and unwanted bulk messages that can be easily generated and broadcast over the IMS network. The origins of such bulk calls routed over IP are often very difficult to trace because of the portability and mobility of devices and soft clients, as well as the IP layer's open invitation to fraud, unauthorized resource use and privacy violations.

Similar problems exist on the Internet, too, and solutions, such as email spam filters, have been developed to address them. However, these solutions do not address VOIP behavior and VOIP call states (such as call forwarding, transfer and caller ID spoofing detection), so these will not work for IMS networks.

Fraud

Fraud can happen in IMS networks in many ways. As mentioned above, the fraudulent user can easily gain access to the IMS network by hacking the U/I SIM cards. Once s/he has access, s/he can commence toll fraud by acting as a gateway between the local PSTN and the IMS network. The attack and result could be quite similar to the recently publicized million-dollar toll fraud on a VOIP network (see, for example, www.theregister.co.uk/2006/06/08/voip_fraudsters_nabbed/).

Although IMS is ostensibly to be secured by IPSec, the fraudulent user can easily become an authenticated subscriber and once inside, can access the entire IMS network and servers. Hackers already have many techniques—such as password cracking, buffer overflows, exploits for OS vulnerabilities and installing rootkits—to get access to the servers, routers, firewalls and operating systems in the network once they get connected. These attacks expose subscriber records and call records to the hackers.

To protect against fraud, the behavior of all subscribers needs to be monitored in real time, and misbehaving subscribers need to be blocked. In PSTN networks, you have fraud protection systems that monitor SS7 and billing traffic for potential anomalies. Today, IMS specifications count only on authentication and authorization systems, both of which are easily hacked, to address fraud.

Rogue Devices

New, smart devices and new access capabilities (such as USB, Bluetooth and downloadable software) can pose a great risk to IMS networks, even inadvertently. Since most of these devices have soft clients, they are easy targets for worms and viruses. These devices also can be recruited as bots on the Internet by hackers to attack the IMS networks and applications.

Current Approaches To IMS Security

The probability of damaging attacks against the IMS network is obviously greater than network operators and IMS equipment suppliers and standards bodies have recognized. If operators are to succeed with IMS, they will need to protect subscribers, software, servers and other infrastructure nodes from the attacks described above.

In IMS networks and on the public Internet, fuzzed messages can easily be used to launch attacks

TABLE 1 Today's IMS Security

PDG/P-CSSF	Firewall Functionality	Not Addressed
User authentication	Layer 3 IP access control	IMS application information-based access control
Signaling and/or media encryption	Layer 3 IP flow control	IMS application information-based flow control
	NAT functions	IMS message fuzzing prevention
	Layer 4 TCP/UDP stateful packet inspection	IMS message spoofing prevention
		IMS message and media misuse prevention
	HTTP/FTP application protection	IMS service misuse prevention
	Application layer gateway (ALG)	IMS subscriber protection
		IMS spam prevention

Thus far, IMS security in 3GPP/3GPP2 refers to various encryption techniques and authentication mechanisms (TS 33-203 and TS 33-110), plus IPSec and security gateways (TS 33-210). Although these techniques are well understood and standardized in 3GPP/3GPP2 specifications, and some already have been integrated into a variety of wireless infrastructure products, they provide only privacy and authentication.

So far, IMS standards provide only privacy and authentication

Therefore, most operators approach the issue by implementing firewalls and/or packet data gateways (PDGs) in front of their Proxy-Call Server Control Function (P-CSCF) that provide the following functions:

- Authentication and encryption methods to prove the identity of IMS users and ensure the privacy of their communications.
- Stateful firewall capabilities that offer Layer 3 (IP) and Layer 4 (TCP/UDP) access control and flow control, network address translation (NAT) traversal with topology hiding and dynamic opening/closing of media ports.

While these services are important, they do not protect against attacks launched by authenticated users, attacks embedded in the encrypted traffic and application layer attacks, as shown in Table 1 and discussed above.

Conclusion

We have seen how easy it is to become an authenticated subscriber on the IMS network through the purchase (or hacking) of a prepaid SIM card. As we discussed, it is hard to determine which authenticated subscribers can be trusted.

We also have seen that traditional security mechanisms are insufficient, and that IMS security specifications are lacking. We note that the encryption and authentication that have been specified are only part of the solution.

The probability of malicious attacks and service abuse of VOIP and other real-time IP communications applications continues to increase, together with the increase in attack sophistication. All these developments are creating a new level of security requirements for the operator that go beyond anything they have deployed thus far.

The best way to provide the required level of protection is to comply with the 3GPP standards and rigorously apply all authentication and encryption mechanisms; deploy the very best existing data security techniques, such as firewall, IDS/IPS and spam filters; and deploy an IMS application-level security device that takes the best existing security techniques but also incorporates a variety of sophisticated IMS-specific security methodologies that include behavior learning, filtering and anomaly detection and verification.

Together, these practices will proactively protect the IMS network from attacks, misuse and service abuse which networks and end-users could face today and in the future□