mancalanetworks
making networks manageable

Security one pager

VoIP attacks

SIP has been subject to a number of vulnerabilities. Most VoIP products have protection against protocol-layer attacks, but only the Network Controller uses realtime tracing and correlation to protect your organization from more complex attacks.

The Session Initiation Protocol (SIP) is the signaling layer behind Voice over IP (VoIP) connections. It is used by VoIP clients to log in to the VoIP server, and to signal outgoing and incoming calls.

> Stolen credentials

Most organizations have publicly accessible VoIP servers. This configuration allows employees to make or receive calls using their internal extensions, even when traveling outside of the office. Employees are usually also allowed to make long-distance calls. However, many employees create poor or easily guessable passwords. The combination of the above items can have catastrophic effects on a company.[1]

Once a users SIP login and password are stolen, attackers can use those credentials to make unlimited long distance calls. Even worse, they can give those credentials to their friends, who can also make unlimited long distance calls. In some cases, the company can be on the hook for hundreds of thousands of dollars of long distance calls, before the problem is discovered.

> Mishandled Credentials

Most VoIP phones configure themselves via TFTP when they boot. However, TFTP servers do not perform any security checks when a VoIP configuration is requested, which enables anyone to obtain SIP credentials for any VoIP phone on the network. This vulnerability allows an attacker to monitor or impersonate anyones telephone extension, including the CEO.

An attacker can use the credentials of “internal” corporate devices to make VoIP calls while located outside of the corporate network. He can then make calls as if he were internal to the company, bypassing many security restrictions. This vulnerability arises because VoIP servers do not maintain a location-aware database of devices, so they have no way of knowing that a login is from the wrong device or location.

> Dictionary Attacks

Attackers regularly use Amazon Cloud instances to brute-force passwords via dictionary attacks.[2] They can try thousands of SIP registrations per second, and quickly discover common accounts and passwords. Once those credentials are discovered, they are used to make fraudulent long distance calls, as described above. Existing VoIP servers do not monitor failed authentications, and will not flag these login attempts.

> Summary

VoIP products offer SIP service. and they excel in their area of expertise. However, they do not provide higher layer network policies which enhance corporate security. Even a simple policy such as limiting the number of simultaneous calls, or call duration may be difficult to achieve.

Similarly, firewalls protect against protocol-layer attacks such as. malformed packets. However, they do not track user accounts or VoIP accounting data. As a result, they are also vulnerable to these attacks.

The Mancala Network Controller offers an additional layer of security which is not available in existing devices. It both detects and protects against all of these attacks, lowering the risk and expense of corporate security.

[1] http://www.zdnet.com.au/thousands-lost-in-rising-voip-attacks-339306478.htm
[2] http://www.voiptechchat.com/voip/538/sip-attacks-from-amazon-ec2-cloud-continue/