

News

Alliance Addresses VoIP Security

BENJAMIN ALFONSI

The Voice over IP Security Alliance (VOIPSA; www.voipsa.org), created in February 2005 to combat security and privacy threats to VoIP, is hoping that strength indeed comes from numbers—in just a few months, the organization has more than doubled its membership.

“Before VOIPSA, no single group had strongly emerged to help organizations understand and mitigate VoIP security risks,” says David Endler, VOIPSA chair and director of security research for 3Com’s security division, Tipping Point.

According to Andrew Graydon, VOIPSA Security Requirements Committee chair and a vice president at BorderWare Technologies, this isn’t a surprise considering the technology’s relative newness.

“History shows us that advances and trends in information technology typically outpace the corresponding realistic security requirements, which are often tackled only after these technologies are widely deployed,” Graydon says. “VoIP is no different.”

Nature of threats

No published attacks have occurred against mainstream or commercial VoIP deployments thus far, but it’s probably just a matter of time.

Like other Internet-based applications, a given VoIP deployment’s level of risk can be a function of its operating system’s vulnerability. According

to Endler, no matter how secure a VoIP application is, it’s a moot point if the underlying operating system can be compromised.

“The most prevalent threats to VoIP deployments are many of the same security threats that plague traditional data networks today,” he says, citing Cisco’s Call Manager, which is typically installed on Windows, as an example.

Graydon says that although threats to VoIP aren’t necessarily more severe than other Web-based applications face, the effort required to safeguard against them might be.

“VoIP implementations typically require more connections than Web browsing or email, for example,” Graydon explains. “Since these streaming connections are dynamic ...there is more complexity to [VoIP] security requirements.”

VoIP also faces different threats than other Internet applications, triggering unique security and privacy concerns.

Ofir Arkin, director and chair of VOIPSA’s Security Research Committee and CTO of Insightix, lists call tracking, call hijacking, and eavesdropping among the most serious threats.

“The targets of these attacks are the information exchanged between call participants, the identities of the caller and callee, the IP telephony-based elements, the IP telephony-based functionality, and other network elements such as servers and hosts.”

Regulation and standards

In terms of promoting VoIP security, the alliance favors adopting standards within the industry rather than lobbying for regulation outside of it.

The technology “traverses international boundaries, and, as such, regulations are hard to consistently enforce across the globe,” Endler says. The alliance is committed to developing best practices needed to help guide VoIP security, he says.

Graydon echoes Endler’s views, but he also presents a practical consideration regarding the regulatory issue. “The ease of exploiting vulnerabilities in reality has no correlation to any regulatory or legislative body, but with the implementation and deployment of the particular technology,” he says.

The young alliance has already set its agenda and formed various committees—on awareness, community outreach, security requirements, best practices, testing, and research—to carry it out. But it recognizes that mobilizing industry forces, not to mention public recognition of VoIP security and privacy concerns, is vital to realizing its goals.

“VoIP is a voice technology—as such, keeping privacy and security is a must,” Arkin says. “Just because the technology is using IP, does not mean it does not have to be, or cannot be, secured.” □

Benjamin Alfonsi is a freelance writer based in New York.