Chapter 15

COUNTERING OR NOT COUNTERING THE EAVESDROPPER: THAT'S THE QUESTION?

INTRODUCTION

Countering or not countering the eavesdropper: that's the question? It all depends on who it is – the FBI, NSA, CIA, etc. ... or is it the wily hacker or terrorist? This chapter will answer that question, and provide recommendations to counter or provide support for the eavesdropper either way.

Wiretaps have been used since the invention of the telegraph and have been a legal element of the US law enforcement arsenal for more than a quarter century. In keeping with law enforcement's efforts to keep laws current with changing technologies, in 1994 the US Congress passed the Communications Assistance for Law Enforcement Act (CALEA). The law proved to be controversial because it mandated that digitally switched telephone networks must be built wiretap enabled, with the US Department of Justice in charge of determining the appropriate technology standards [1].

The law provided a specific exclusion for information services. Despite that explicit exemption, in response to a request from the US Federal Bureau of Investigation (FBI), in August 2005, the Federal Communications Commission (FCC) ruled that broadband voice over IP (VoIP) must comply with CALEA. Civil-liberties groups and the industry immediately objected, fearing the ruling's impact on privacy and innovation. There is another community that should be very concerned. Applying CALEA to VoIP requires embedding surveillance technology deeply into the protocol stack. The FCC ruling undermines network security and, because the Internet and private networks using Internet protocols support critical as well as noncritical infrastructure, national security as well. The FCC ruling is a step backward in securing the Internet, a national (and international) priority [1].

CALEA'S HISTORY

In 1992, the FBI was struggling. What had been a boon for telephony (the split-up of AT&T (Ma Bell), which previously had a monopoly of the US market), was a serious problem for the bureau. Instead of implementing wiretaps by working with a single service provider and phone company, the FBI found itself facing a plethora of suppliers of services and telephones. Even worse from the FBI's perspective were the new telecommunications technologies: cell phones, call forwarding, call waiting, and speed dialing. That same year, the FBI put forth the Digital Telephony proposal, which would have required wiretapping standards to be included as part of the design of digital-switching telephone equipment [1].

The FBI claimed that the advanced calling features impeded court-authorized wiretaps. However, The Washington Post investigated and discovered that, FBI officials have not yet fumbled a criminal probe due to the inability to tap a phone. At this news, Computer Professionals for Social Responsibility, a public – interest group, initiated Freedom of Information Act litigation; in response, the FBI released a four-page list of impeded cases in which, citing national security, all information was blacked out [1].

Digital Telephony Proposal

The FBI's Digital Telephony proposal represented a sharp change in the government's approach to wiretapping. Instead of letting service providers determine how to configure their systems to accommodate wiretaps, the proposal put government in the middle of telephone-equipment design. In fact, this bill placed the US Attorney General, a position not generally known for technical expertise, into the process of standards design of equipment used by the general public. Industry and civil-liberties groups opposed the FBI proposal, and no one in Congress would sponsor it [1].

In 1994, the FBI reintroduced the bill, and this time, events played out differently. Over the course of the Congressional session, the bill's scope changed, narrowing down to common carriers (rather than all electronic communication service providers), adding some protections for transactional information (the first time such information was afforded protection in wiretapping law) and eliminating a clause requiring telephone companies to decrypt encrypted conversations [2], regardless of whether they had an encryption key. There was also a sweetener for the telecommunications companies: a US$500 million authorization to help carriers update their networks to comply with the law's requirements. Although other civil-liberties groups had continued to oppose the bill, the Electronic Frontier Foundation's support of the final version (now renamed CALEA) helped persuade the telephone companies to support it. This time, the bill passed. Though the law governed just the US, its impact was far broader. The FBI pressed other nations to adopt similar laws. In any case, because the law applied to the US telecom market, much of the rest of the world was forced to adopt the standards that CALEA dictated [1].

Implementing CALEA

The law ran into trouble almost immediately. The telephone companies believed that negotiations on the bill had left them in a position in which standards would be determined