Security and Legal Implications of Wireless Networks, Protocols, and Devices

Jeff Bilger, Holly Cosand, Noor-E-Gagan Singh, Joe Xavier

Overview

The last decade has seen an explosive growth of wireless networks. Due to the cheap cost of equipment compared to wired networks and relative ease of deployment, the adoption rate of wireless will soon exceed that of wired networks. Initially, many companies predicted that wireless networks would only be used by the military, government, and the very rich. However, the commercial success of analog cellular telephony networks in the 1980's, followed by the digital cellular telephony networks based on GSM and I-mode in the early 90's and finally culminating in the WiFi phenomenon of the early 2000's has proven that wireless networks are here to stay.

Although wireless networks afford users more flexibility and mobility, they also expose users to a number of new security risks inherent to wireless networks themselves. Regardless of the type of wireless technology (cordless phones, cellular communication devices, WiFi), most first attempts at security were based on obfuscation. Subsequent attempts plugged existing security holes and were based on assumptions that may not hold true. Wireless networks and devices will continue to proliferate and unless these systems are designed around security, users will continue to be vulnerable to security breaches.

From a legal point of view, wireless networks and devices present an interesting dilemma: Is using your neighbor's open wireless network a crime? What categories of activity should be illegal? What are the legal precedents? How should existing laws be changed?

Topic Coverage

We will use the topics provided in the table below as the high level sections for organizing our paper. These sections will be integrated into the body of our paper template.

Individuals on the team will take responsibility for writing sections for specific topics as shown in the table. However, all members are responsible for reviewing the submissions made by the other team members and providing feedback and edits on the document. In order to provide valuable feedback, all members should do some research and reading in all topic areas covered in the paper.

Written submissions for the paper will be sent to all members of the team. One member of the team is responsible for pasting the submissions into the paper template, versioning the paper and redistributing to all team members.

Our paper will cover the security and legal implications of wireless networks, protocols, and devices by exploring the following:

Topic	Primary Author
The evolution of wireless networks, devices, and protocols.	Holly Cosand
The future of wireless networks, devices, and protocols in terms of adoption and prevalence.	Holly Cosand
A survey of current wireless networks, devices, and protocols.	Holly Cosand Jeff Bilger
Why is wireless network security a high priority item?	Noor-E-Gagan
Vulnerabilities of wireless networks, devices, and protocols. Scope of the vulnerabilities.	Noor-E-Gagan Joe Xavier
Detection of attacks on wireless networks, devices, and protocols.	Joe Xavier
Defense options: How can wireless networks, devices, and protocols be made more secure?	Jeff Bilger
What can we learn from existing wireless networks?	Noor-E-Gagan
Legal implications of wireless networks and devices.	Jeff Bilger