Conquering the Last Frontier in the Digital Invasion: The Home Front

25

25.1 Introduction

As digital technology conquers new territory and there is ubiquitous use of technology, the last frontier has fallen in the digital invasion and the digital activity hub has come home. It is almost a paradox that as more technological activities have come home to make the lives of millions of people easier and more enjoyable, the threat to their core personal security is directly under attack. Since the early 1950s as digital technology become pervious, the main activity and locus of technological activities invaded the workplace first as the need for improvement in production become paramount. Millions of people took on the task of learning the new technologies as a way to prevent job losses as these new technologies entered the workplace to improve production and hence improve profitability. There were cries of "computers invading the workplace and eating jobs." After a while, we all got used to these new invaders and we became comfortable to work with the job skills they provided. Production skyrocketed and new jobs were created as old olds disappeared and the fear of job losses was overcome and confidence increased among young workers as they entered the workplace with ever-increasing new skills promising enormous fortunes. We saw new technology giants springing up every other day and making millions. With little fanfare and unknowingly, we become members of social networks as we linked up with colleagues and relatives and a million other people we never and we will never know.

We become the netizens and we become connected and linked to the world. We unknowingly became part of the foci of technology we carried in little ever powerful digital devices. Technology now had moved out of the workplace. We carried it whenever and wherever we went. We become unknowing carriers as we couldn't live without those devices. Noticing that as workers carried the little powerful gizmos, they remained productive, employers allowed us to bring the gizmos back to the workplace. Now technology was everywhere.

While all these activities and the silent digital crusade were going on, there is clear demarcation between the home and the workplace. The workplace was a place

J.M. Kizza, *Guide to Computer Network Security*, Computer Communications and Networks, DOI 10.1007/978-3-319-55606-2_25

of production, of making a living, of discovery, and of personal development. The home on the other hand was a place of sanity, serenity, rest, and personal entertainment. The kind of technology that entered the home from was designed to do just that. For example, television, video, and audio technologies directed to the home front were meant to entertain—and they were stand-alone. Instead of becoming small like their production technologies, these homebound technologies became big to enhance realism in entertainment.

These divisions in the two technologies help up for a while. But in the early 2000s, things started to change; an invasion of sorts started to encroach on both technologies—the smartness and intelligence of digital devices whether big or small. Smartness in digital devices started to create a kind of relationship and courtship between the two divergent technologies. As the courtship grows, it started leading to a convergence of telecommunication, computing, and broadcasting technologies—a marriage that was unstoppable. The marriage took place without fanfare and the home front will never be the same. It became, in addition to entertainment, a production front.

More and more people are now working from home for convenience or otherwise. Employers are finding benefits for some kind of employees to work from home. More and more professions are discovering that working from home is more beneficial and profitable that the workplace outside the home. There is now a growing list of production activities that are better done home. In the following sections, we will discuss the enablers of home production.

25.2 The Changing Home Network and Hotspots

The growing and evolving entertainment technology in the home, the advent of the Internet, and the new monitoring home technologies have all turned the home place into the "new wild west" as far as the security and integrity of the home, including house data and individuals in the home, are concerned. Before we look at the data in the home, let us take a look at the way the home network has evolved over the years and the specific entry points into the home. There are several avenues that intruders and hackers can penetrate and access house data at will. Some of the most known of these avenues are:

25.2.1 Cable LAN

For a long time, homes used to have devices offering different functions like entertainment and communication, but these devices were never connected. As more digital devices started to enter the homes, there was a need to interconnect them with cables for easy use, better services, and experience. A central component to connect such devices was needed and it came to be the *router*. Using cables and wires, each house digital device plugs into a designated entry point into the router called a *port*. With this kind of cascading of home devices, a *local area network*

(LAN) is formed in the home, with the router as the central connecting device. A router can have several ports, called RJ45s, which can connect several devices in the house.

A router has two sets of ports, internal ports that connect all devices in the home onto a LAN and one special port, usually designated by a different color or with a word *Uplink*, known as the *wide-area network (WAN) port* [1]. This port, also known as the *Internet port*, connects the router, and hence the hone LAN, to an Internet source, such as a *broadband modem*. The WAN allows the router to connect to the Internet and share that connection with all the Ethernet-ready devices connected to it [1].

25.2.2 Wireless Home Networks

The development and the perverseness of wireless technology in the last few years have created great freedoms for and more mobility of users with mobile devices. This has also increased the use of mobile devices at home leading to the birth of wireless networks in homes. There are several types of wireless networks that can be found in homes:

25.2.2.1 Wireless Personal Area Network (WPANs)

These networks, based on IEEE standard 802.15.4 of 2004, interconnect home devices within a range of between 10 and 100 m with a transfer rate of 250 kbit/s. WPANs networks focus on low-cost, low-speed ubiquitous communication between devices within the range. Devices using this standard, like mobile phones, computers, GPS receivers, digital cameras, and video game consoles, can exchange data and information using the network layers based on the OSI model, although only the lower layers, the physical and MAC layers, are defined in the standard.

According Lou Frenzel [2], the 802.15.4 category is probably the largest standard for low-data-rate WPANs. It has many subcategories including the 802.15.4a/802.15.4c for China, 802.15.4d for Japan, 802.15.4e for industrial applications, 802.15.4f for active (battery powered) radio-frequency identification (RFID) uses, and 802.15.4g for smart utility networks for monitoring the smart grid. All of these special versions use the same base radio technology and protocol as defined in 802.15.4a/b.

The 802.15.4 standard defines the physical layer (PHY) and media access control (MAC) layer of the Open Systems Interconnection (OSI) model of network operation (Fig. 25.1). The PHY layer defines frequency, power, modulation, and other wireless conditions of the link. The MAC layer defines the format of the data handling. The remaining layers define other measures for handing the data and related protocol enhancements including the final application [2]. We will see more of these networks in Chap. 18.

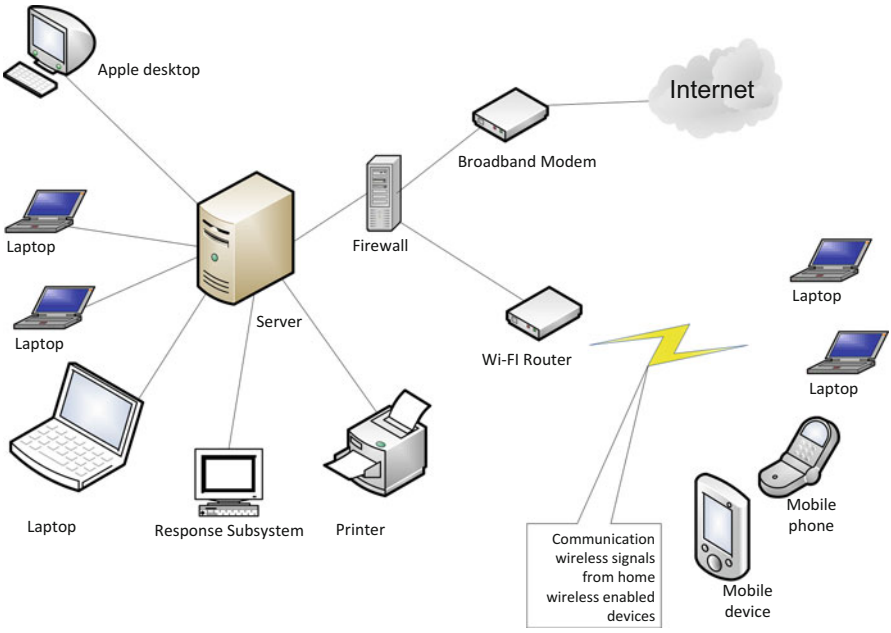

Fig. 25.1 The home LAN

25.2.2.2 Wireless Local Area Networks (WLAN (WI-FI))

This is another short-range, up to 500 m, local area wireless technology that allows an electronic device to exchange data or connect to the Internet using 2.4 GHz UHF and 5 GHz SHF radio waves. Wi-Fi is probably the premier local area network (LAN) technology for high-speed Internet access for mobile devices like laptops, smart phones, tablets, and smart TV sets for video transfer. Wi-Fi-enabled devices, like those we have given, can connect to the Internet when within range of a wireless router which connects to the *broadband modem (access point)*. A broadband modem is a device that bridges the Internet connection from a service provider to the LAN router or a computer, making the Internet available to the home devices [1]. With wireless technology, wireless-enabled devices can connect to one another in the same LAN or outside the LAN without being connected by cables as it used to be. See Fig. 25.1.

Although Wi-Fi ranges are limited, they can be extended with use of several overlapping coverage of access points to cover a large area as large as many square miles. Wi-Fi technology is increasingly being used in private homes, businesses, as well as in public spaces called hotspots usually set up by businesses or public authorities for free-of-charge use. Wi-Fi technology has been standardized as IEEE 802.11. We will see more of this in Chap. 18.

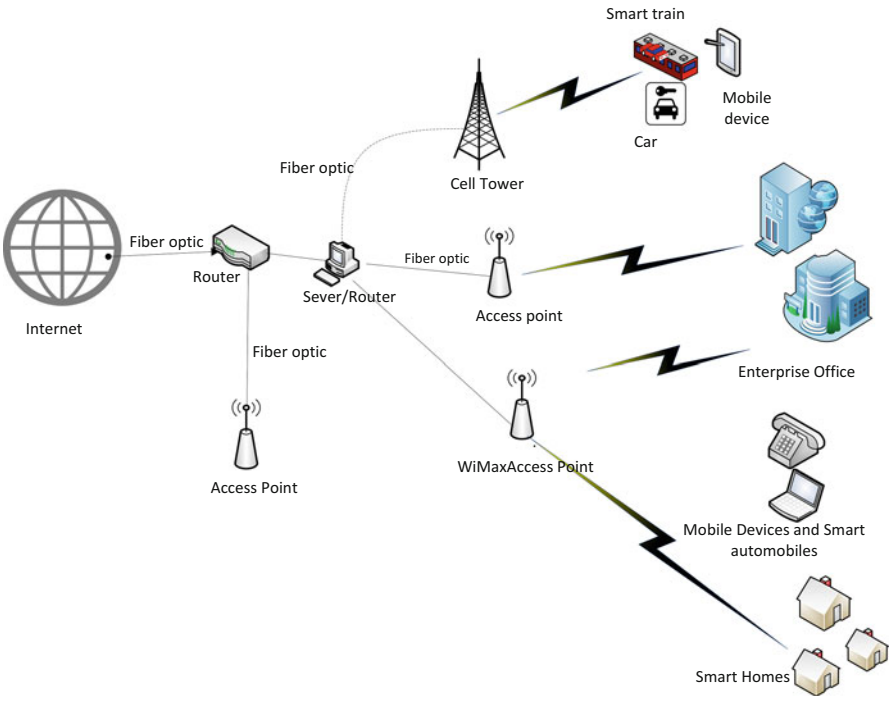

Fig. 25.2 WiMax coverage

25.2.2.3 WiMax LAN

WiMAX (Worldwide Interoperability for Microwave Access) is another limited area wireless communications technology based on IEEE 802–16 standard, designed to extend the range and functionalities of Wi-Fi technology. It provides data rates reaching up to 75 megabits per second (Mb/s) and a number of wireless signaling options ranging anywhere from the 2 GHz range up to 66 GHz, with up to 1 Gbit/s for fixed stations. It can also provide a service range of up to 10 miles. Because of that range, WiMAX can be installed either by a survive provider as base stations or as small receivers installed by clients to connect to the base station. The WiMAX base station then sends and receives data to and from a WiMAX-enabled router, which would then send the data to the different devices in the home LAN. It is possible to combine Wi-Fi with WiMAX by having the router send the data to the devices via Wi-Fi server. See Fig. 25.2.

As a step above DSL and cable modem, WiMAX protocol accommodates a whole range of data transmission protocols that both cable modems and DSL cannot, so far, like Voice Over Internet Protocol (VoIP). VoIP allows making local, long-distance, and even international calls through a broadband Internet connection possible. As we look forward, we will scale up city size *metropolitan area network* (MAN). See more in Chap. 18.

25.2.2.4 4G and LTE LAN

The last of the extension of the home LAN is the current 4G technology and its enhancement by LTE (Long-Term Evolution) LAN. The combo has created a wireless broadband technology designed to support roaming Internet access via cell phones and handheld devices. Nearly all devices running 4G and LTE technologies can also be part of the home inventory, and we will consider this technology as home-based technology to join the other three we have so far discussed. LTE, as a newer technology, its communication protocols are based on Internet Protocol (IP). Because of this, it offers a variety of communication protocols that the older technologies could not offer including VoIP- and other IP-based services. LTE can theoretically support downloads at 300 Mbps or more based on experimental trials. Finally, because it is still a new technology, it is only available in limited geographic areas, but it is growing after getting early support from telecommunications providers.

25.2.2.5 5G Wireless Technology

In Sect. 18.2.4 we briefly discussed 4G and associated LTE technology and the anticipated rollout of 5G technologies. These technologies are indeed enhancing mobile broadband, adding new exciting feature and increasing speed and footprint.

25.2.3 Types of Broadband Internet Connections

Doug Ngo [1] gives three types of broadband Internet connections as:

- *Wired Internet (residential broadband)*: In this category, the home LAN is connected to the Internet via a physical cable such as a telephone line (DSL) or a cable line (cable), or a fiber optic line (FIOS). This is one of the good options for a home LAN because with it, there are no data caps or at least very high caps, so users don't need to worry about how much they download or upload.
- *Satellite Internet (satellite broadband)*: With satellite broadband, the home LAN connection to the Internet is via a satellite disk, probably on the roof, which communicates with satellites to provide the LAN with Internet access. Although satellite Internet is slower and more expensive, it is a great, probably the only, option for remote areas with no cable, DSL, or FIOS services.
- *Cellular Internet (wireless broadband)*: With this option, the LAN Internet connection is made possible via a cell phone signal to carry data and connect the supported device directly to the Internet. There are several cellular data standards, and starting with 3G, it's fast enough to be called "broadband." The latest standard, 4G LTE, offers the speed equivalent to that of a midrange residential broadband connection (somewhere between 5 Mbps and 20 Mbps download speed).

25.2.4 Smart Home Devices

For generation, the home has been a source of entertainment for the family and guest to the family. Throughout history, the family as an entertainment center has seen a growing number of gadgets to enhance entertainment. As technology started invading the home, it came via the entertainment devices. With changing technologies, the evolving entertainment menu, and the need to enhance the integrity and security of the family, a new role of technology in the home, beyond entertainment, of monitoring the home was born. This new role brought to the home a new breed of digital devices that will later turn into a security problem as we will soon discuss.

25.3 Data and Activities in the Home LAN

With the miniaturization of digital devices, there is a new breed of medical monitoring and wearable devices are in people's home. More and more people are wearing health supporting and monitoring devices that are actually connected or are able to connect to the Internet. There are now devices that are remotely regulating or delivering medicines to patients in their homes via the Internet. These kinds of devices are increasing. Also there are an increasing number and caliber of digital devices that are meant to monitor the integrity and security of the home letting the owner from afar know in real time or near real time, or through alerts, the status of the home. It used to be that the types of data that were most common in the home network were pictures, usually from family vacations and valued occasions of family like weddings and family get together, videos of family events, and various personal data files usually stored on the family computer hard drive. Given the changing nature and utility of the family network, although these data are still being stored in the family LAN, a lot more data types have come home too.

25.3.1 Work Data

The growth of work at home movement that started in the late 1980s has changed the home LAN, not only by bringing in new technologies but also bringing in the home enterprise data. Home workers routinely download and upload and consequently store enterprise data on the home LAN in their routine work. Also the new movement of bring your own device (BYOD) to the enterprise premises is creating avenues where employees are bringing enterprise data on their devices knowingly or otherwise. Mobile devices have a way of collecting and sometimes storing data either from the enterprise spaces or public commons.

25.3.2 Social Media Data

The increasing use of smart and more powerful mobile devices are increasing the amount of both personal and public data brought into the home LAN by these mobile devices from social media and from public commons.

25.3.3 Banking and Investment Data

Long lines in banks are numbered as more and more bank customers are running home to do their banking in the comfort of their homes. The banks themselves are encouraging this through advertising of online banking. Most people that do online banking do it either after work or on weekends, most at home. Doing any online banking activity on the home LAN transfers sensitive data back and forth between the family LAN and the banker servers. It is not only banking that invades the home LAN but also investment activities are not far behind. Again most people who have investments check invest and trade mostly after work or on weekends, again using the home LAN. Doing these activities, like in banking, a considerable amount of data is exchanged between the home LAN and the investment house servers. Some of this data and the trail of activities are stored in histories on the home LAN.

25.3.4 Health Devices

It has taken a while, but at last medical technology has become of age. In fact among all the sectors, the medical sector has seen the fastest growing and more promising technologies in the last several years. As providers, hospitals, and health insurance companies are fighting for consumer dollars, technology is coming in to the rescue. Health insurance providers in order to cut on long and expensive hospital stays are encouraging health providers to embrace and use technologies that enable patients to have operations and leave hospitals in a day or two. These patients and many other healthcare types are increasingly getting follow-up care at home. Medications, monitoring signals, and patient data information are usually and commonly uploaded on the family LAN, and many times this data stay stored either on the family LAN or LAN histories.

25.3.5 Home Monitoring and Security Devices

The growth in monitoring technology in the last few years has opened a flood gate in home monitoring. The usual movement sensor monitoring that home security providers like ADT used to offer is now archaic. All types of sensors are now packaged in minute, well-hidden devices that can be remotely controlled via the family LAN. We have already discussed the use of the family LAN to penetrate and take control of the family electronic devices through the electric meter. The

marriage between the electric and cyber signals in the family LAN has made the remote control of most family devices and family electronic data a reality and has created a security quagmire in the home. No home, no home LAN is secure anymore.

25.4 Threats to the Home and Home LAN

As we pointed out before, the home front, as the last frontier of invasion to personal security and privacy, has become the "new wild west." What is more worrying is that the individuals in the home front, unlike their counterparts in the workplace, are less knowledgeable and far less prepared to deal with the intruders. In a way, they are helpless in a sense that they may not know what is or may happen to their home, data and home devices, and, more frightening, their personal lives because hackers can now use physical harm to individuals in the home. Even if they come to know, they may not be able to do anything to stop it. In "Hacking Home Automation Systems Through Your Power Lines," Kim Zetter [3] details how hackers can attack a home or even a business automation and security systems though power lines. Using this conduit, the hackers can, through remote commands, take control of a multitude of devices, such as lights, electronic locks, heating and air conditioning systems, and security alarms and cameras. The systems operate on Ethernet networks that communicate over the existing power lines in a home, sending signals back and forth to control devices. Beyond taking control of your devices, hackers can also introduce sniffers to the broadband power network through an electrical outlet and sniff the signals in the home to know what is going on in the home using already installed security and monitoring devices such motion sensors and image cameras.

What is worrying is that these cheap systems are running on open-source tools to conduct the hacks. Although most of the current tools are more successful on home systems running non-encrypted protocols, very soon, even systems supporting encryptions may be attacked as encryptions are increasingly being broken by hackers.

The tools and attacks to the home are varied and are on the increase. Attack types are also changing. With attackers now able to remotely enter the home, they are now able to reprogram the house devices to do things unimaginable including opening doors, jamming home security, and monitoring signals thus able to prevent security signals from ever reaching home security and monitoring companies, the police, and even the home owner.

As we have seen above, growth in medical and monitoring technologies are increasingly allowing an increasing number of patients to receiver care from their homes. With this kind of increasing potential attacks on home systems, the future of health home care is also in jeopardy.

Let us discuss a few of the major steps individuals can do to mitigate, if not stop, a home invasion by hackers for whatever reason. First, we will look at the most common threats to the home and home LAN.

25.4.1 Most Common Threats to Homes and Home LANs

The most common methods used by intruders to gain control of home computers are briefly described by CERT in "Home Network Security" [4]:

- Trojan horse programs—Trojan horse programs are social engineering programs sent by introducers and designed to make you trust them as they introduce access traps for easy access into the home LAN.
- Back door and remote administration programs—common on Windows computers, there are three tools used by intruders to gain remote access to the house LAN. The tools are BackOrifice, Netbus, and SubSeven. These tools allow access and control house LAN.
- Denial of service—this attack, common in the 1990s, causes digital devices on the home LAN to crash or to become so busy processing data that you are unable to use it.
- Mobile code (Java/JavaScript/ActiveX)—code from these Web programming languages is executed by most computer Web browser. This code can be used by intruders to gather or to run malicious code on any computer on the family LAN. Read more about this at http://www.cert.org/archive/pdf/activeX_report.pdf
- Cross-site scripting—this is malicious script moved around the Internet by computers visiting servers sitting these scripts. There are several ways a LAN computer can expose the family LAN to these types of code [4]:
  - Following links in Web pages, e-mail messages, or newsgroup postings without knowing what they link to
  - Using interactive forms on an untrustworthy site
  - Viewing online discussion groups, forums, or other dynamically generated pages where users can post text containing HTML tags
- E-mail spoofing—E-mail "spoofing" is a way to trick a user to believe an e-mail is coming from a specific source when it is actually coming from another. Spoofed e-mail can range from harmless pranks to social engineering ploys.
- E-mail-borne viruses—transporting and spreading viruses via e-mails. Most viruses are actually transported and spread using e-mails attachments.
- Hidden file extensions—Windows operating systems "file extension hiding," if not disabled, can be exploited by e-mail-borne viruses. So these file extension hiding options, whether in Windows systems or other products, which are usually defaults, must be disabled.
- Packet sniffing—these are programs deposited at strategic points of the Internet to capture data from information packets as they travel over the network. They can attach any designated network including the family LAN.

25.4.2 Actions to Safeguard the Family LAN

The most recommended steps a home owner and home LAN user can take are again CERT [4]:

- Consult your system support personnel if you work from home.
- Use virus protection software.
- Use a firewall.
- Don't open unknown e-mail attachments.
- Don't run programs of unknown origin.
- Disable hidden filename extensions.
- Keep all applications (including your operating system) patched.
- Turn off your computer or disconnect from the network when not in use.
- Disable Java, JavaScript, and ActiveX if possible.
- Disable scripting features in e-mail programs.
- Make regular backups of critical data.
- Make a boot disk in case your computer is damaged or compromised.

For more details of each one of these, the reader is referred to [4].

25.4.3 Using Encryption to Protect the Family LAN

The wireless family LAN has not only brought convenience in the use of home devices but has also brought ease of use and a far greater exposure and outreach of the family computer and other devices via the Internet. However, wireless technology has also brought more problems to the family with a wireless LAN. While wired home networks are confined by their connected wires, to send and receive data from specified points of the network, wireless networks, on the other hand, broadcast data in every direction to every device that happens to be listening, within a limited range [5]. Because of this, the security and integrity of the devices and the wireless LAN in the family is at risk. More directed steps, therefore, are called for to mitigate these risks.

As more advanced wireless communication technologies are developed, there is a need for stronger and more focused encryption protocols. Along the way, therefore, various wireless security protocols have been developed to protect home wireless networks. These wireless security protocols include WEP, WPA, and WPA2, each with their own strengths and weaknesses. These new wireless encryption protocols have improved the prevention of uninvited guests from connecting to the family LAN and have further helped to harden private data by encrypting it as it leaves and enters the family LAN. Lawrence C. Miller in "The Essentials of Setting Up a Wireless Network: Wireless Security Protocols: WEP, WPA, and WPA2" [5] discusses the three most popular protocols as follows [5]:

- *Wired Equivalent Privacy (WEP)*: The original encryption protocol developed for wireless networks. It was designed to provide the same level of security as wired networks, but WEP suffers from many well-known security flaws, it is difficult to configure, and it is easily broken.
- *Wi-Fi-Protected Access (WPA)*: To further harden the wireless network, a newer protocol, WPA, was developed as an interim security enhancement over WEP,

while the 802.11i wireless security standard was being developed. Most current WPA implementations use a pre-shared key (PSK), commonly referred to as *WPA Personal*, and the Temporal Key Integrity Protocol (TKIP, pronounced *tee-kip*) for encryption. *WPA Enterprise* uses an authentication server to generate keys or certificates.
- *Wi-Fi-Protected Access version 2 (WPA2)*: Based on the 802.11i wireless security standard, which was finalized in 2004. It enhanced WPA by introducing the use of the Advanced Encryption Standard (AES) for encryption. The security provided by AES is far superior to that of WPA. The US government uses it to encrypt information classified as top secret.

25.4.4 Protecting the Family LAN with Known Protocols

Although Wi-Fi LANs provide many benefits to a family using it, but as we pointed out earlier, WI-FI LANs broadcast data in every direction to every device that happens to be listening, within a limited range. Unprotected WI-FI LANs can result in unauthorized use and potential harm to the family LAN and those in the family. Family WI-FI LANs, therefore, need to be protected with the most efficient encryption protocols available to the user. In "Protecting Your Wireless Network," the US Federal Communications Commissions—Consumer Task Force [6] suggests the following security steps should be taken:

- *Turn encryption on*—Turn on the WI-FI LAN router's encryption setting right after installing the router. As the router comes out of the box, the encryption feature is usually disabled. Use "WPA2" the most current and most effective. When turning on WPA2, choose a longer password that utilizes a combination of letters, numbers, and symbols for better security.
- *Turn the firewall on*—In addition to turning on WPA2 at installation, also turn on the firewall to protect the LAN from harmful intrusions. Firewalls can be hardware based or software based. Wireless routers generally contain built-in firewalls, but are sometimes shipped with the firewall turned off. So it is important and recommended to check and see if the wireless router's firewall is turned on.
- *Change default passwords*—Most wireless routers come with preset passwords for administering the devices settings (this is different from the password used to access the wireless network itself). Unauthorized users may be familiar with the default passwords, so it is important to change the router device's password as soon as it is installed. Again, longer passwords made up of a combination of letters, numbers, and symbols are more secure.
- *Change the default name of the network*—A network's name is known as its "SSID" (service set identifier). When a computer with a wireless connection searches for and displays the wireless networks nearby, it lists each network that publicly broadcasts its SSID. Manufacturers usually give all of their wireless routers a default SSID, which is often the company's name. It is a good practice

to change the LAN's SSID. Never use personal information such as the names of family members.

- *Turn network name broadcasting off*—Wireless routers may broadcast the name of the network (the "SSID") to the general public. This feature is often useful for businesses and institutions offering free WI-FI to the public. For personal or family Wi-Fi networks, turn this feature off.
- *Use the MAC address filter*—Every device that can connect to a Wi-Fi network has a unique ID called the "physical address" or "MAC" (media access control) address. Wireless routers can screen the MAC addresses of all devices that connect to them, and users can set their wireless network to accept connections only from devices with MAC addresses that the router is set to recognize. In order to create another obstacle to unauthorized access, change the family LAN's router settings to activate its MAC address filter to include only the LAN authorized devices.

Exercises

1. Discuss why the home front is the last digital frontier of the digital invasion.
2. Discuss with evidence why the home front is the "new wild west" in personal privacy and security.
3. Why is the home LAN user in a more precarious state than an enterprise LAN user.
4. Discuss the growing hacker invasion and the pending potential threat to the home devices and home LAN security.
5. What are the security imperative of a home LAN user not knowing or ignoring putting security measures in the family LAN.
6. Based on your current knowledge, what must be done to stop or mitigate this pending Armageddon?
7. Do you think this is a mere small threat or a pending catastrophe?
8. How should the home LAN user be alerted or trained to meet the pending threat?
9. Given what you know, should working from home be discouraged?
10. Should corporations and businesses be responsible for the security of the family LAN for those working from home?

Advanced Exercises

1. Develop an application that can be used to run a security assessment of a family LAN.
2. Develop an application that can intercept and prevent a home-based medical device to be hacked in to save a life.
3. Develop an application that alerts a home LAN user of a penetration attempt and suggest quick remedies to mitigate prevent the intrusion.
4. Develop a series of remedies for a home LAN intrusion and develop applications for each.

5. Develop a menu of security applications for a family LAN capable of intercepting an intrusion into a family LAN and generating a corresponding alert.

References

1. Ngo D. CNET, Home networking explained, Part 4: Wi-Fi vs. Internet. http://www.cnet.com/how-to/home-networking-explained-part-4-wi-fi-vs-internet/
2. Frenzel L. What's the difference between IEEE 802.15.4 and ZigBee wireless? March 22, 2013, Electronic Design. http://electronicdesign.com/what-s-difference-between/what-s-difference-between-ieee-802154-and-zigbee-wireless
3. Zetter K. Hacking home automation systems through your power lines. Wired. http://www.wired.com/2011/08/hacking-home-automation/
4. CERT. Home network security. http://www.cert.org/historical/tech_tips/home_networks.cfm?#IV-A-1
5. Miller LC. The essentials of setting up a wireless network: wireless security protocols: WEP, WPA, and WPA2. Home Networking Do-It-Yourself For Dummies. http://www.dummies.com/how-to/content/wireless-security-protocols-wep-wpa-and-wpa2.html
6. Protecting your wireless network. Federal Communications Commissions – Consumer Task Force. http://www.fcc.gov/guides/protecting-your-wireless-network