Global Information Assurance Certification Paper

Securing Office/Home Power-Line Network

Igor Paic

March 26, 2002

Introduction

One of the first ways or methods used for communication over the distance was the scream. Soon, the fire was discovered and smoke signals were carrying messages. Then, written letters did the same, and so forth. The problem was always the security of these communications, because it was always there an intruder trying to get the message. At the dawn of the industrial age, the communication was getting more extensive and there were more security holes. In addition, in the newest societies, computer communications inherited the same problems. The success of our modern communication systems is now based on security, ´Security of the Communications.´

History

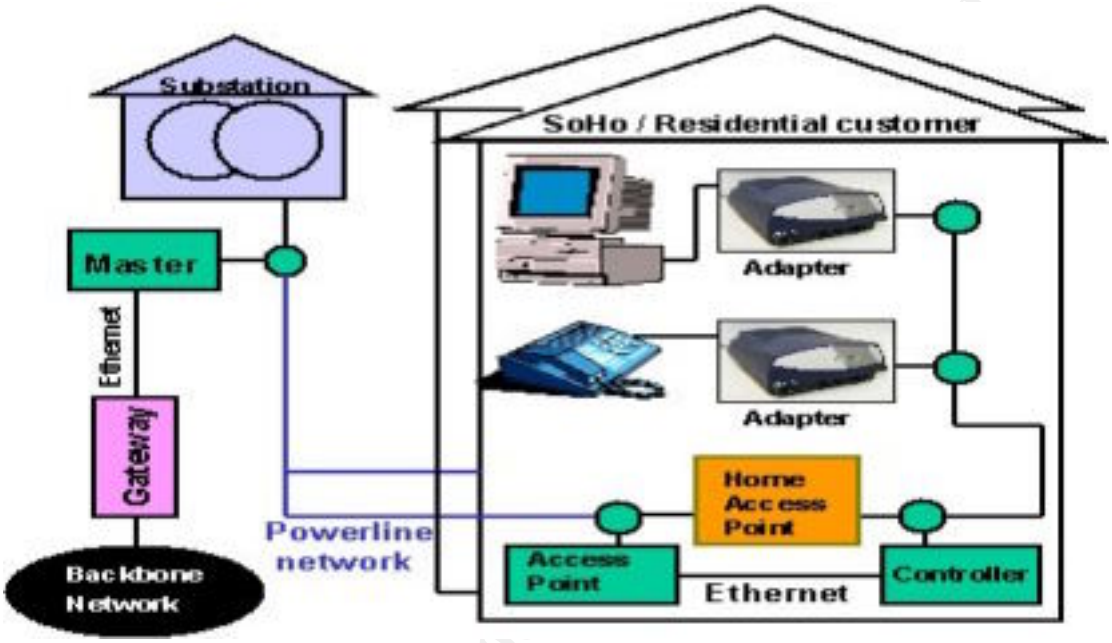
At the beginning of the computers age there were not networks at all. The giant computers were working alone, using input devices like punch cards, serial terminals and so on. Starting from 40 years ago or more, there were some research studies regarding to connect computers with other similar computers with the objective to share data, and to receive and send information in the format of electronic mails using serial communications and modems. That was the revolution of the cheap store and share data. Then, with the ARPA-Net and, lately, with Internet, the new revolution on communication was born using a TCP/IP protocol which was designed to be strong and hard to lose communication. One of the first commercial extended LAN (Local Area Network) was created using coaxial cables as the rest of the equipment like repeaters, hubs and similar. Later the new technology was UTP Cabling system using CAT-3 up to 10Mb and later CAT-5 up to 100Mb bandwidth. The problem with all these networks was -and actually is- that we must have separated networks for computer equipments and another separated network for our electrical equipment using Power-Line Network. This problem implies prices and two costs; one for power-line and another for data networks. Today, a new technology is trying to use one network, the Power-Line Network Technology.

How Power-line Networking Works

Power-line networking is one of the several ways to connect computers in your home or small office. It uses an existing electrical wiring in your house or office to create a network, the same wiring we use for power outlet. On the Chilean Technical University Santa Maria's internal sysadmins discussion list we can find tailored simple definition of How Power-line Networking Works :

Wherever exists a pair of wires (for example; Power-Line Cables) there is a possibility to transmits signals (in this case digital information). If that cable has

already another use, in case, -for instance- to empower the house/office electrical equipment, we must try to induce electric signals in the cable in such form that these do not interfere with the primary function of the cable. This is obtained by using a principle of modulation, like modulation for Internet on TV-Cable and ADSL or, to giving other examples; it is used for IP on "Power-Line-Carrier" (PLC, that is the technical name of this kind of modulation).



Source: ASCOM Web Site
http://www.ascom.com/apps/WebObjects/ecore.woa/de/showNode/siteNodeID_36717_contentID_107621_languageID_1.html [2]

In these cases, the primary function of the cable is still the electrical distribution of electrical energy, plus distribution of the TV-Cable and the telephonic signal respectively.

In the case of electrical energy cables, we should know that, one has an alternating current with a frequency of 60 Hertz, and the other has 110 Volts in the layer of low voltage. 110 Volt -even if 'low voltage is called to it'- is comparatively high for electronic equipments that work less, generally with 5 Volt or lesser. For this reason we must completely isolate the equipment we use for communication.

For this task, we must use a circuit filter with a transformer. Here, we block signals of the LF (Low Frequency, that is to say, 60 Hertz) completely, but it is still transparent for signals of the HF (high frequency, 60,000 Hertz = 60 kHz) or higher. Now, we simply need some kind of apparatus or machine that "modulates" our signal of data in high frequency (it is possible to use them until some MHz). Then, we connect it to one side of the filter. At the other side of it, we make the connection to the network of highly ready voltage and we do the data transmission or -in other words- establishes communication at this time. [1]

We place a signal of data modulated in cables of high voltage. Of course, it is needed a transmitter and a receiver at each end of the communication connection, something like modems (Modulator – Demodulator, means MODEM). The ADSL and Cable-Modem connections work using the same form or modulating and demodulating. Actually, several companies work and sale the wall-outlet-parallel, wall-outlet-serial and the wall-outlet-Ethernet communication port devices.

The following picture shows the computer PCI card with, into a wall outlet to create a power-line network. (See more on: http://www.intellon.com/products/powerpacket/int5130_evalkit.html) [3]

Source: Intellon Web Site http://www.intellon.com/products/powerpacket/int5130_evalkit.html

For a detailed graphical, and understandable presentation about how the power line Network works, please go to the following link at the Howstuffworks web site: http://www.howstuffworks.com/power-network.htm [4]

Old and New Security Risks (Well-Known Risks, Future Risks and Threats)

Security risks are the common methods used by intruders to gain control or access to host or to the computer without owner's permission, using any method accessible to them, like physical access, network access, Internet access or combinations of them. There are a wide range of security risks and threats in these areas, but the must well-known types of security risks, basically, are:

- Network Based
- Operating System Based

Network Based

Some of these well-known examples are:

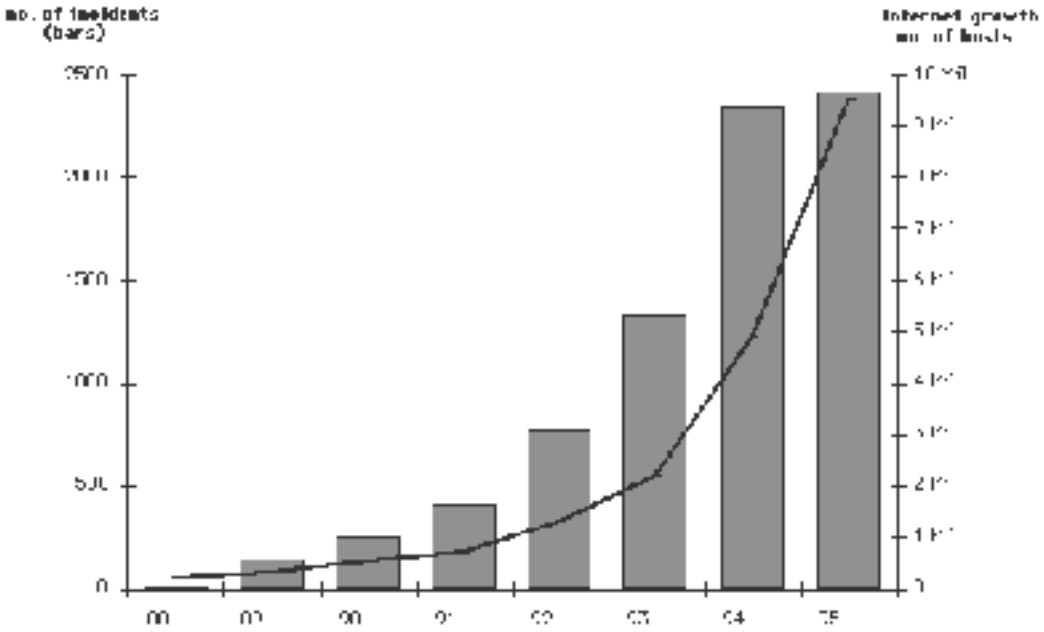
- Port Scanning
- Trojan horse programs
- Back doors
- Unprotected Windows shares
- Mobile code (Java, JavaScript, and ActiveX)
- Cross-site scripting
- Email spoofing
- Chat clients
- Remote administration programs
- Packet Sniffering
- Denial of Service
- Malicious Code
- Internet Infrastructure Attacks

Operating System Based

- Account Security, including:
    - Passwords guessing due to short or very easy passwords
    - Password aging, password remains the same all time
    - Renaming accounts
    - Weak account policies if they exist

- File System Security, including:
    - File system wide permissions
    - Weak remote file or folders access control
    - Wide share permissions
    - Weak control of combined local and remote permissions
    - Operating system security risks
    - Weak registry security in case on Windows
    - No system nor security policy for application of Patches and Fixes

Growth in Security Incidents



Source:
CERT Coordination Center Reports http://www.cert.org/encyc_article/tocencyc.html

CERT Coordination Center Reports gives the following conclusions on the Security Incidents:

In this graph issued by CERT Coordination Center, the number of security incidents reported has grown dramatically, from less than 100 in 1988 to almost 2,500 in 1995. Through 1994, the increase in incident reports roughly parallels the growth of the size of the Internet during that time. Figure shows the growth of the Internet and the corresponding growth of reported security incidents. The data for 1995 and partial data for 1996 show a slowing of the rate at which incidents are reported to the CERT/CC (perhaps because of sites' increased security efforts or the significant increase in other response teams formed to handle incidents). However, the rate continues to increase for serious incidents, such as root compromises, services outages, and packet sniffers. [5]

As we can notice, in the previous figure, the proliferation of the security risks and threats are closely related with the growth almost parallel of the growth of the Internet. Therefore, we are forced to use the devices and applications to repel these incidents, security risks and threats. These devices and applications are: NIDS's (Network Intrusion Detection System), HIDS's (Host Intrusion Detection System), Desktop Firewalls, Perimeter Security Firewalls, VPN and Antivirus systems.

NIDS (Network Intrusion Detection System)
Network Intrusion Detection System is system designed for detection and for prevention of damage caused by external or internal attacker.

The two main types are:

- Misuse detection where NIDS analyzes the information. It gathers and compares it to databases of attack signatures. Essentially, the IDS look for a specific attack that has already been documented. Like a virus detection system, misuse detection software is only as good as the database of attack signatures that it uses to compare packets against. [6]

- Anomaly detection where the system administrator clearly defines normal state of the network's traffic load, protocols, and of the typical packet size. The anomaly detector monitors network segments to compare their state to the normal baseline and look for anomalies. [7]

HIDS (Host Intrusion Detection System)
The main difference between NIDS and a host-based system (HIDS) is that the HIDS examines internal activity on each host and also they can analyze the logs files or event logs in some cases.

Desktop Firewall
Applications designed for protection on individual computer or host using the principles of the packet filtering firewalls.

Perimeter Security Firewall

Webopedia Internet site gives the following definitions of the Perimeter Security Firewall:

Application designed to block and prevent unauthorized access to or from a private network generally from Internet. This application can be implemented in software or hardware versions (appliances). Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

There are several types of firewall techniques:

- Packet filter: Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.

- Application gateway: Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose performance degradation.
- Circuit-level gateway: Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.
- Proxy server: Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

In practice, many firewalls use two or more of these techniques in concert. A firewall is considered a first line of defense in protecting private information. For greater security, data can be encrypted using VPN.[8]

VPN
Virtual Private Network, a network that is constructed by using public wires or public network to connect two or more private network or node. For example, there are number of systems that enable you to create networks using the Internet as the medium for transport data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted. [9]

Antivirus
Utility that searches hard disks, diskettes, electronic mails, shared folders for viruses and removes any that are found. Most antivirus programs include an auto-update feature that enables the program to download profiles of new viruses so that it can check for the new viruses as soon as they are discovered. [10]

Future Threats or Future Security Risks in the new power-line networking technology are the sum of up to date, well known threats and the number of new ones until now in nothing related between networks and power. For better understanding, we must think that in the up to date, the only signals that drive across the electrical wiring are electrical signals of low frequency. From now on, the electrical wiring must carry also the high frequency signals with TCP/IP packets and information. Therefore, the new risks and threats are the result of a mixture of the old and new ones.

We can distinguish some of these new ones:

- Power-line failures or out gage
- Power-line interferences on high frequencies
- Quality of the power-line wiring (Older wiring can affect performance)
- Intrusion of our neighborhood power-line networks
- Power Buss malfunction

As we can see, the totally of new, actual and never seen threats are now being considered as sources of security risks. The new world of security is opening up behind our eyes.

So, it is our responsibility to consider these new threats as soon as possible, as it is the seriously study for being prepared for them.

The New Process of Securing of Power-Line Networks

The process of securing of the Power Line Networks radically differs from the conventional securing because of introductions of new elements, like power outlets, power switches, plug fuse, the quality of power-line installation and similar up to day components nothing linked with computer sciences.

Therefore, the new elements or equipments, or modified old ones must be (at least):

- Electric Measurer with Firewall or Stand Alone Firewall for Power Line Networks
- Electric frequency filters
- Plugs with outlet and Ethernet/Parallel Port connection with or without encryption (as in the figure 2)

Source: Intelogis http://www.howstuffworks.com/power-network3.htm [11]

- New Security Policies considering the new elements and Best Practices

As in the case of ADSL or Ethernet networks, the future Electrical Company ISP provider must manage, and, it can assign a set of static or dynamic IP addresses out to Perimeter Security Firewall. Due to this reason, we must consider it.

In brief, the new process of securing must involve these new and old elements

In the case of a house use, at least:

- Perimeter Security Firewall for power line network or Electric Measurer with Firewall, for protecting the house indoor network

- Wall plug connectors with encryption
- Desktop Firewall, for protection of individual computers indoor
- Antivirus system, for protection of individual computers indoor

In the case of an office use, the above mentioned elements, plus:

- NIDS, for protection of indoor office network of the intrusions
- HIDS, for protection of indoor host computers
- VPN, for communication with other outdoor company networks

Implications on the security industry

As it is shows in this document, the security area, now, will be wider than ever The actual and future Security Engineers must have the knowledge of the basics as also the advanced knowledge of the Electrical Engineering to be at the proper, successful level in securing the new network technologies.

This is not the end of the conventional networks like UTP or Fiber Optic networks, this is the new technology, which is complementary with the existing one.

Implications of the new technology

This new technology may imply the whole new re-engineering of the security, home equipment standards, re-engineering of the studying programmes for the future Security Engineers at High Schools, Universities or Certifications like SANS or CISSP.

Conclusions

The future of Power-Line Networks will basically resides at a small office/home networks area (called SOHO) because of its natural limitations, such as: low bandwidths, home power limitations when using the home power line, low level of reliability, lack of redundancy, and so forth. On the other side, big companies need very broad bandwidths, redundancy, high availability and high performance so, today, this new technology is not appreciated within them. However, these companies are interested in providing products and services for this raising industry. The other good point is that the Internet will grow again due to the Power Line Networks.

Finally, we must be well prepared and well informed about this new technology and his potential on the growing of Internet and Security industry because we are also part of it.

Acknowledgments

Reviewers

Thanks very much, to the following people, for their patience and their time revising this work.

Leopoldo Rodriguez Rubke, Professor Ph.D.
Universidad Catolica de Valparaiso (Catholic University of Valparaiso), Chile
http://www.ucv.cl/

Julio Cella, Systems Engineer
Symantec Corporation
http://www.symantec.com/

Ricardo Silva, Electrical Engineer
Universidad Catolica de Valparaiso (Catholic University of Valparaiso), Chile
http://www.ucv.cl/

Sources and references

[1] Systems Administrators List (sysadmins), Universidad Tecnica Federico Santa Maria – CHILE

Discussion topic: Tendencias tecnologicas - IP sobre Tendido Electrico (Technologic Tendencies: Power-Line Networks)
http://www.utfsm.cl/

[2] ASCOM, Broadband Powerline Communication
http://www.ascom.com/apps/WebObjects/ecore.woa/de/showNode/siteNodeID_36718_contentID_150882_languageID_1.html

[3] Intellon: PowerPacket
http://www.intellon.com/products/powerpacket/index.html and
http://www.intellon.com/products/powerpacket/int5130_evalkit.html

[4] Howstuffworks, How Power-line Networking Works
http://www.howstuffworks.com/power-network.htm

(Continued from previous page)

[5] Carnegie Mellon University, CERT Coordination Center Reports
http://www.cert.org/encyc_article/tocencyc.html

[6][7]Webopedia: Online Dictionary for Computer and Internet Terms
http://www.pcwebopedia.com/TERM/i/intrusion_detection_system.html

[8] Webopedia: Online Dictionary for Computer and Internet Terms
http://www.pcwebopedia.com/TERM/f/firewall.html

[9] Webopedia: Online Dictionary for Computer and Internet Terms
http://www.pcwebopedia.com/TERM/V/VPN.html

[10] Webopedia: Online Dictionary for Computer and Internet Terms
http://www.pcwebopedia.com/TERM/a/antivirus_program.html

[11] Intelogis web site
http://www.intelogis.com/

Other Sources, Ideas and Information

Symantec Corporation (Symantec Enterprise Solutions)
http://enterprisesecurity.symantec.com/

Cisco – Connecting Your Home
http://www.cisco.com/warp/public/779/consumer/

HomePlug Powerline Alliance
http://www.homeplug.org/

National Semiconductor,National P/N IC/SS - Power Line Carrier Local Area Network
http://www.national.com/pf/IC/IC_SS.html

Carnegie Mellon University, CERT Web Site, Home Network Security
http://www.cert.org/tech_tips/home_networks.html